MALVIDENCE - A COGNITIVE MALWARE CHARACTERIZATION FRAMEWORK

by

Muhammad Salman Khan

A Thesis submitted to the Faculty of Graduate Studies of

The University of Manitoba

in partial fulfilment of the requirements of the degree of

Doctor of Philosophy

Department of Electrical and Computer Engineering,

University of Manitoba, Winnipeg, MB, Canada

THIS PAGE INTENTIONALLY LEFT BLANK

Abstract

The challenges of cyber security have outpaced the advantages of cyber tools and technologies. In 2018, World Economic Forum has already placed cyber security in the top five risks faced by the world. Cyber threats are evolving and can cripple economies and nations. The major tools of cyber threats are anonymity, deception and uncertainty. Current state of the art research is also evolving into addressing these challenges by applying new and proactive threat hunting approaches instead of doing reactive cyber defense, which is proving futile. Malware is an indispensable tool of cyber threat actors to accomplish malicious activities i.e. exfiltration, espionage and disruption. Using advanced obfuscation and mutation methods, malware adversaries are able to remain ahead of cyber defenders. Most malware detection technologies are based on finding a-priori known signatures of malware payload or known patterns of malware behavior. This dissertation addresses the challenge of hunting unknown behaviorally mutated malware inside a host computer by proposing a proof of concept framework named Malvidence for characterizing malware behavior within a host operating system process tree using cognitive machine intelligence. Using Malvidence framework, tools and techniques can be derived for variety of cyber security methods for threat detection. Cognitive Computing is a promising domain of machine intelligence which explores and develops new tools to incorporate human cognitive characteristics so that the performance of existing domain of artificial intelligence and machine learning can be improved. Therefore, cognitive complexity based fractal analysis is demonstrated and a methodology of extracting inherent but hidden patterns of malware dynamics using a temporal graph theoretical approach is proposed. Further, a set of graph theoretical features is analyzed and proposed for an effective characterization of malware behavior which can be subsequently used for malware hunting and detection. In addition, the proposed features are tested for their mathematical validity. Finally, using proposed cognitive complexity analysis, characterization performance of an unsupervised clustering algorithm is provided to demonstrate the validity of Malvidence framework.

Keywords:

Fractals, malware mutation, anomaly detection, clustering, unsupervised machine learning, malware characterization framework, malware mutation, endpoint threat detection, EDR, Endpoint Detection and Response, Microsoft Windows, process tree, polymorphism, metamorphism, class imbalance, class inseparability, variance fractal dimension, correlation fractal dimension, information fractal dimension, spectral fractal dimension, graph theory, time graphs, cognitive machine intelligence, Cognitive Computing, cyber kill chain, cognitive and concurrent cyber kill chain, semantic analysis, features, attributes, k-means, fBm, fractional Brownian motion process, cyber security, behavioral analytics, host anomaly detection, malware data set, semantics, threat hunting, threat model.

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgment

Throughout the progression of my research during the past few years, there are so many people who contributed and supported my research efforts that I find it very difficult where to begin with. First and foremost, I would like to thank my Ph.D. adviser Prof. Dr. Ken Ferens of Electrical and Computer engineering. I am very grateful for his support, trust, motivation, advice, careful reviewing and providing feedback to my work and his continued guidance and support to my pursuits and career goals. His unrelenting insights and patience with me is and will always be appreciated. I would like to thank Prof. Dr. Andrew Goertzen for not only providing me an opportunity to work on OpenPET project but also his guidance and instilling a confidence of pursuing doctorate level research. I am grateful to Prof. Dr. Bob McLeod for his guidance and motivation to carry on the difficult path of doctoral research. Without any exaggeration, I would like to state that I am blessed and proud to have such a wonderful and supportive advisory panel.

I would like to extend my deepest gratitude to Prof. Dr. Witold Kinsner, who convincingly inspired my research directions towards multiscale and multifractal analysis. His relentless dedication and motivation have been very instrumental in paving my way and instilling confidence in diving into the complex domain of fractals.

I am also thankful to Amy Dario as her relentless efforts in making the administrative work easier for me and all the graduate students. Her support is very commendable.

My special thanks to Cyber Intelligence, Analytics and Data Science team at Canadian Tire Corporation and Mitacs Accelerate Ph.D. fellowship program who made it possible to pursue my goals. I am grateful to Stephen Weston, Vice President IT Governance and CISO at Canadian Tire, for his confidence upon me, my research and University of Manitoba.

I would like to extend my gratitude to IMPACT Cyber Trust USA, University of Wisconsin, USA, University of Twente, Netherlands, North Carolina State University, USA, Mila Parkour and all data set repositories which are used in our publications.

I am grateful to Canada, province of Manitoba and University of Manitoba for providing me an opportunity to come, research, study and pursue my ambitious goals.

I would like to express deep gratitude to my life partner and research colleague Sana Siddiqui whose enthusiastic collaboration has been helpful in progressing our group’s contributions to the cyber security and cognitive machine learning research.

I could not have been progressed without the support of my parents, parents-in-law and friends who always remained supportive, always trusted me and stood by me through the thick and thin.

Finally, I am thankful to Almighty Allah SWT who blessed me with an opportunity to be thankful to everyone and for everything He bestowed me with.

THIS PAGE INTENTIONALLY LEFT BLANK

The malware data set for this dissertation were collected using the sandbox developed in our paper [1] *authored by several research members of our group. My major contribution to this paper is the development of the data acquisition software framework of the sandbox and the fractal based characterization algorithms which are used in this dissertation. Further, I am deeply grateful to Sana Siddiqui, a core member of our research group who supported and contributed my efforts in searching, collecting, compiling and test running the mutated malware code and executable files which are later used in this dissertation for testing and validating the cognitive characterization performance. The proposed graph algorithms, coding of fractal algorithms, proposed feature extraction and characterization techniques and the concomitant analysis are my own work.*

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

Glossary of Abbreviations

No.	Abbreviations/Notations	Full Form
1	.NET	MS Windows based free software framework
2	.PDF	Portable Document Format
3	ACCS	Australian Center for Cyber Security
4	ADFA	Australian Defense Force Academy
5	AI	Artificial Intelligence
6	ANN	Artificial Neural Network
7	API	Application Programming Interface
8	APT	Advanced Persistent Threat
9	CC	Cognitive Computing
10	CFD	Correlation Fractal Dimension
11	CFDT	Correlation Fractal Dimension Trajectory
12	CI	Cognitive Informatics
13	CLSID	Globally unique identifier for COM class object
14	CMD	Command Prompt
15	CnC	Command and Control
16	CNTS	Count of Nodes per Time Stamp
17	CPU	Central Processing Unit of a computer
18	CSOC	Cyber Security Operation Center
19	CSV	Comma Separated Value
20	CTC	Canadian Tire Corporation
21	DAG	Directed Acyclic Graph
22	DDOS	Distributed Denail of Service Attack
23	DiGraph	Directed Graph
24	DLL	Dynamic-link library
25	DNS	Domain Name System
26	DOS	Denial of Service Attack
27	E	Edges of Graph
28	E(.)	Statistical Expecation Operator
29	ECTS	Edge Count vs. Time Stamp
30	EDF	Estimated Distrbiution Function
31	EDR	Endpoint Detection and Response
32	EM	Expectation Maximization
33	EMTS	Edge Memory vs. Time Stamp
34	ETSD	Edge Time Stamp Duration
35	ETTS	Edge Thread vs. Time Stamp

36	EXE	Executable File
37	F-1 / F1	Harmonic Mean of Recall and Precision
38	fBm	Fractional Brownian Motion
39	FD	Fractal Dimension
40	FFT	Fast Fourier Transform
41	FN	False Negative
42	FP	False Positive
43	Fs	Sampling Frequency
44	GCC	GNU Compiler Collection
45	GNU	GNU's Not Unix!
46	GPL	General Public License
47	GPU	Graphics processing unit
48	HEX	Hexadecimal
49	HHMM	Hierarchical HMM
50	HMM	Hidden Markov Model
51	HTML	Hypertext Markup Language
52	HTTP	Hypertext Transfer Protocol
53	IBM	International Business Machines Corporation
54	ID	Identification
55	IDS	Intrusion Detection System
56	IFD	Information Fractal Dimension
57	IFDT	Information Fractal Dimension Trajectory
58	IMPACT	Information Marketplace for Policy and Analysis of Cyber-risk & Trust
59	IoE	Indicator of Exploits
60	IP	Internet Protocol
61	IPS	Intrusion Prevention System
62	IR	Incidence Response
63	k-NN	k-Nearest Neighbor algorithm
64	label	Label (normal = 0, malware = 1)
65	LAMP	Linux, Apache, MySQL, PHP (Linux Framework)
66	LSE	Least Square Estimate
67	modBaseSz	Module memory in bytes
68	modCTm	Module create time in MS Windows timestamp (100 nano second)
69	modNm	Module opened by the process
70	modPth	Module Path in Windows directory structure
71	MS	Microsoft
72	ms	milli second
73	MSDN	Microsoft Developer Network

74	Mutex	mutual exclusion object
75	MySQL	Open Source SQL - GPL 2 License by Oracle
76	N!	Factorial Combinations of N
77	NOP	No Operation / No-Op
78	NP	Nondeterministic Polynomial time
79	ns	nano second
80	NTSE	**T**ime **S**tamp vs. **E**dge **T**ime
81	Op-Code	Operation Code
82	OpenCV	Open Source Computer Vision
83	OS	Operating System
84	OS	Operating System
85	P2P	Peer-to-peer
86	PDF	Probability Distribution Function
87	PFN	Probability of False Negative
88	PFP	Probability of False Positive
89	PHP	Hypertext Preprocessor - Server Scripting Language
90	PID	Process Identifier
91	pid	Process ID
92	PoS	Point of Sale
93	PPID	Parent Process Identifier
94	ppid	Parent Process ID of the pid
95	procCTm	Process create time in MS Windows timestamp (100 nano second)
96	procMemSz	Process Memory Size in bytes
97	procNm	Process Name
98	PSD	Power Spectral Density
99	PTN	Probability of True Negative
100	PTP	Probability of True Positive
101	RBM	Restricted Boltzmann Machine
102	RegEx	Regular Expression
103	SD	Spectral Dimension
104	SFD	Spectral Fractal Dimension
105	SFDT	Spectral Fractal Dimension Trajectory
106	SIEM	Security Information and Event Management system
107	SOC	Security Operation Center
108	SP	Service Pack - MS Windows Patch
109	sup	Supremum - Least Upper Bound
110	SVD	Singular Value Decomposition
111	SVM	Support vector machine
112	threadCnt	Number of threads opened by the module

113	TI	Threat Intelligence
114	TN	True Negative
115	TP	True Positive
116	TSEM	Time Stamp vs. Edge Memory
117	TSER	Time Stamp vs. Edge Repeat
118	TSET	Time Stamp vs. Edge Thread
119	TSNC	Time Stamp vs. Node Count
120	TSNE	Time Stamp vs. Number of Edges
121	TSNN	Time Stamp vs. Node Neighbor
122	TSNR	Time Stamp vs. Node Repeat
123	TTP	Tools, Techniques, Procedures
124	UNSW	University of New South Wales
125	URL	Uniform Resource Locator
126	UUID	Universal Unique Identifier
127	V	Vertices of Graph
128	Var	Statistical Variance Operator
129	Vel	Volume Elements
130	VFD	Variance Fractal Dimension
131	VFDT	Variance Fractal Dimension Trajectory
132	VM	Virtual Machine
133	VPN	Virtual Private Network
134	XOR	Exclusive OR - Digital Logic

1. Introduction

This section provides an introduction of the proposed Malvidence cognitive framework to characterize mutated malware inside an operating system process tree using time based graph dynamics. Starting with the motivation behind this research work, a brief summary of the previous work and the publications which contributed incrementally to this dissertation is provided. Afterwards, a formal problem statement, research questions and the dissertation claims are stated. Subsequently, an organization of the dissertation is provided which is followed by brief details of the artefacts developed in this work.

1.1 Motivation

Evolution of Internet technologies and pervasive use of cloud computing has provided many benefits to humans across the globe. Emails, social networks, mobile applications and related information technologies have created an indispensable reliance of human being over Internet and evolving communication platforms. With this reliance, cyber security battlefield between threat actors and defenders has also entered into new dimensions. Now a days, traditional cyber security measures are proven defenseless due to the mutation and obfuscation technologies. Further, due to diverse geographical distances, which span continents, it is easy to launch a cyber-attack without any fear of retribution. Cyber world is changing very fast and the world of cyber security is evolving into a complex landscape and is posing unprecedented challenge which is difficult at one end due to big data issues (problem of finding a needle in the haystack!) and at other end due to increasing complexity of detecting threats with available defense tools and techniques. Specially, with the advent of state backed threats driven by advanced malware e.g. Stuxnet, Flame and Zeus, cyber world is increasingly becoming an advanced battlefield where threat actors are no more naive or easy to find, but are involved in sophisticated attacks by criminal organizations (states based and/or rogue entities) which are motivated by financial, geo-political or power control ambitions. Further, these threat actors are intelligent and launch threats with careful planning keeping them ahead of defenders.

Major tool for cyber adversaries is smart and intelligent malware which renders anonymity, deception and uncertainty to avoid being detected by antivirus tools, firewalls and/or intrusion detection and prevention systems. Malware detection systems mostly rely on signature based analysis of malware binaries or employ a-priori information about the behavior of a malware (sandboxing techniques). Now a days, malware are characterized by a family of malicious entity which shows certain attributes of similarity i.e. using same malware obfuscation generator and using similar code base. For example, Spy Eye, Gameover Zeus and Citadel malware are composed of malware families having similar behavior and syntax such as Zeus malware family.

Cyber kill chain is an analytical model of studying and analyzing the successful delivery and subsequent successful execution of malicious activity in the target system. Malware is the payload of the cyber-attack which is delivered to the victim computer and can be analyzed using cyber kill chain. Terminologies of polymorphism and metamorphism are attributed to the behavioral and functional changes in malware object (executable file) which originate from the same family or inherent characteristics of parent malware. Using various morphism tools (also called as mutation), malware writers can syntactically change a malware executable inside an operating system which appears benign to the host defenses i.e. sandbox and antivirus. From the perspective of Cyber Kill Chain, mutation is applied to both the delivery and execution of the malware to evade perimeter defenses to detect delivery (i.e. network firewall and Deep Packet Inspector) and host based defenses to detect malware execution (i.e. antivirus, sandbox and endpoint behavior analytic systems). Currently, malware detection technologies inside a host computer leverage various tools and techniques for detection which includes sandboxing methodologies to study the behavior of malware and generates unique behavioral patterns which are used to update anti malware technologies. Cyber security honeypot is another techniques that is used to trap threat activities

and analyze the pattern of attack in a systematic way to generate unique signatures, heuristics or behavioral patterns. Further, machine learning techniques are being used to process large volume of data and extract patterns of interests. However, mostly supervised or semi-supervised machine learning, which requires some prior knowledge about the threat entity (anomaly detection), are employed to tackle the pattern recognition problem in cyber security.

As discussed earlier, a fundamental challenge of today's malware is centered on anonymity, deception and uncertainty, which can be summed into a common term called mutation. By virtue of mutation, a malware can mimic the behavior of normal host activities and can remain below the radar of malware detection technologies. Further, state of the art malware are able to detect the presence of anti-malware technologies such as sandboxing and therefore, can stay quiet/inactive for long time to avoid detection. From the perspective of a cyber-security specialist, major challenge lies in how to sift through large volume of data which is also high velocity and veracity, and then find malicious patterns with high reliability. Further, this challenge is compounded by the mutation of malware which hides the true abnormal patterns among the big data and thus increases false alarms. Although automation using machine learning is able to reduce the challenge of handling big data, but false alarms (i.e. false positives and false negatives) are a major cause of security breaches.

Cyber security research is pacing up and has improved the posture of cyber defenders in the past few years by introducing new and novel techniques to analyze big data and search legitimate anomalies (i.e. true positives) but threat actors are also enhancing the techniques of obfuscation and mutation. This dissertation is motivated by the challenge of malware behavioral mutation inside an operating system and aims to characterize malware behavior such that without having any a-priori information about malware (i.e. knowledge of signature), host operating system process tree dynamics can reveal anomalies and can subsequently indicate the presence of malware. This thesis does not consider network based communication and solely relies on operating system process information to characterize malware trajectory in a temporal dynamics of operating system. Further, this thesis does not provide specific malware detection tool, rather it provides a new methodology known as Malvidence framework for malware characterization which can be used for detection in a security operation center, intrusion detection and prevention technologies and malware analysis frameworks.

Cognitive Computing deals with the complexity of objects by finding hidden patterns and relationships among those patterns to characterize the objects in multiscale dimensions. Fractal theory is a mathematical concept that is used to characterize and measure the complexity of objects. Fractal based complexity analysis provides a unique and discriminatory method to analyze an object of interest using time and/or spatial methods. This dissertation provides an empirical behavioral analysis of ten different mutating malware inside a Windows 7 host operating system using two separate instances of each malware and characterizes their temporal dynamics using thirteen graph theoretical features. Further, these features are analyzed for their mathematical validity and are used to study and analyze an unsupervised clustering algorithm to reliably cluster the corresponding samples in a normal and malicious cluster. In the field of cyber-security research, endpoint or host based activities are often analyzed using graph as a mathematical tool to represent and examine relationships between entities. For example, the relationship between

parent and child process is depicted by a graph where each process is denoted by a node and their spawning in time is represented by edges. Therefore, particularly, graph node based features are identified such that both false positives and false negatives can be reduced simultaneously. Also, this analysis is done on temporal graphs of operating system process tree and thus provides an effective threat hunting method for cyber security operation centers (CSOC) which reduces cognitive load on cyber experts and automates the analysis.

1.1.1 Previous Work

This dissertation is an evolution of my research since the time I joined University of Manitoba as Ph.D. student in the department of Electrical and Computer Engineering. Our group initiated the efforts by working on network based data set and explored the possibility of using cognitive multiscale analysis to detect threats. While working with the data science group at Cyber Intelligence and Analysis department of Canadian Tire Corporation (CTC), I came across with various state of the art technologies, including but not limited to Firewalls, Security Information and Event Management Systems (SIEM), IDS/IPS and Endpoint Detection and Response technologies (EDR). Further, during my three years research tenure with CTC, I also learned the methodologies and procedures of Cyber Security Operation Center (CSOC) which is required for Incidence Response and Threat Intelligence to keep organization safe from cyber threats. As my work is focussed on cognitive intelligence aspects, I found out that the major problem faced by CSOC is the ever increasing cognitive load impressed upon cyber security teams due to unprecedented volume of false alarms and high rate of missing new threats. Further, the problem is compounded by the lack of machine intelligence techniques because most of the configuration and analysis work is done manually. Therefore, it was natural for me to dive deep into finding methods of reducing this cognitive load using new and novel cognitive intelligence methods for the analysis of data to reinforce security posture. As every major advanced targeted threat in the cyber world targets endpoint system, therefore, working on endpoint became my choice of selecting this area for this dissertation. Further, most of the available cyber security research is focussed on Linux operating system, while Microsoft Windows based operating systems are mostly used for end users and thus poses a high risk in the context of new EDR technologies, therefore, the focus was to carry out research applying cognitive machine intelligence in detecting Microsoft Windows based cyber threats and therefore, executed twenty malware instances for the generation of data set, which is to the best of our knowledge, is the first attempt in characterizing malware behavior inside a Windows operating system. Overall, my doctoral journey evolved from working on openly available data sets to developing our own sandbox test bed for host based Windows operating system. Further, our research group tested various new machine intelligence algorithms and techniques to detect and characterize advanced cyber threats both in network and host based endpoint security systems.

We have published two book chapters [2] [3], two journals [4] [5] and ten conference papers [1] [6] [7] [8] [9] [10] [11] [12] [13] [14] providing details of our progress in the development of cognitive machine intelligence methods, network threat analysis and the development of malware testing sandbox. Some of the contributions of our already published work appears in this

dissertation. Following is a brief description of the analysis and results of these publications which are used in the development of this research work progressively.

1) Muhammad Salman Khan, Ken Ferens, & Witold Kinsner, (2014) "A chaotic measure for cognitive machine classification of Distributed Denial of Service attacks", in proceedings of IEEE 13th Intl. Conf. Cognitive Informatics & Cognitive Computing (ICCI*CC14), London, UK, 2014 (doi: 10.1109/icci-cc.2014.6921448).

2) Muhammad Salman Khan, Ken Ferens, & Witold Kinsner, (2014) "A chaotic complexity measure for cognitive machine classification of cyber-attacks on computer networks", in International Journal of Cognitive Informatics and Natural Intelligence (IJCINI), 2014 (doi: 10.4018/IJCINI.2014070104).

During the years of late 2013 and early 2014, our efforts were focussed on studying and testing the concepts of chaos theory to measure cognitive complexity of network based distributed denial of service (DDoS) attacks. In these publications, I contributed towards the development of detection techniques to transform network based IP traffic time series into a chaos based Lyapunov exponent trajectory to measure the detection performance and compare with traditional artificial neural network. These results provide better performance with increase false alarms. Through this research work, I found that sampling intervals for a time series should be mathematically validated because the detection performance depends on the retrieval of optimum statistical information from the selected time window size and having selected sub-optimum time sampling interval hampers detection performance significantly. Further, Lyapunov exponent requires manual selection of thresholds to improve the false alarm rates and therefore, as a result, I directed my efforts towards finding better alternatives for cognitive machine intelligence.

3) Muhammad Salman Khan, Ken Ferens, & Witold Kinsner, (2015) "A cognitive multifractal approach to characterize complexity of non-stationary and malicious DNS data traffic using adaptive sliding window", in proceedings of IEEE 14th Intl. Conf. Cognitive Informatics & Cognitive Computing (ICCI*CC15), Beijing, China, 2015. (doi: 10.1109/icci-cc.2015.7259368).

4) Muhammad Salman Khan, Ken Ferens, & Witold Kinsner, (2015) "A polyscale autonomous sliding window for cognitive machine classification of malicious Internet traffic", in proceedings of 14th International Conference on Security and Management (SAM'15), WorldComp 2015, Las Vegas, USA, 2015.

5) Muhammad Salman Khan, Sana Siddiqui, Ken Ferens, & Witold Kinsner, (2016) "Spectral Fractal Dimension Trajectory (SFDT) to measure complexity of malicious attacks", in

proceedings of the International Conference on Security and Management (SAM'16**),** WorldComp 2016, Las Vegas, USA, 2016.

In these papers, we advanced our research in search of finding better cognitive intelligence algorithms and studied fractal theory to measure cognitive complexity and long range correlation of DNS traffic time series. Particularly, the study focussed variance and spectrum based fractal technique to characterize complexity of cyber threat from the complexity of normal traffic. Further, I also studied the effects of statistical stationarity and varying overlapping time window size adaptively in time series to validate the mathematical basis of the analysis using fractals. This analysis contributed in the progress of this dissertation in developing stationarity and sampling frequency mechanisms of cyber data for meaningful and cognitive threat analysis.

6) Muhammad Salman Khan, Ken Ferens, & Witold Kinsner, (2015) "Multifractal singularity spectrum for cognitive cyber defence in Internet time series", in International Journal of Software Science and Computational Intelligence (IJSSCI), 2015 (doi: 10.4018/IJSSCI.2015070102).

In this journal, a generalized fractal analysis framework using more complex multifractal singularity spectrum is studied and analyzed to characterize Internet time series for the detection of cyber threats cognitively. A novel operational range based Mandelbrot singularity spectrum technique is presented to detect and differentiate complexity of cyber time series having DNS attacks. The operational range is based on the spectrum of multifractal exponents and is shown to provide a discriminatory subset of exponents for hidden cyber threats. Further, the validation is done on mathematical fractal Brownian motion (fBm) process. Wavelet methods were used to extract singularity spectrum. This dissertation does not use multifractal method which is more complex than fractal methods, however, the theoretical foundation of this journal helped shaped the algorithmic development of this dissertation. Further, fractal algorithms were validated using fBm method described in this journal.

7) Sana Siddiqui, Muhammad Salman Khan, Ken Ferens, & Witold Kinsner, "Detecting Advanced Persistent Threats using fractal dimension based machine learning classification", in proceedings of 6TH ACM Conference on Data and Application Security and Privacy, 2016, New Orleans, USA (doi: 10.1145/2875475.2875484).

This paper introduced the concept of complexity based cognitive intelligence in k-NN machine learning classification algorithm using fractal approach. Further, the data set of malware and network threats was used for the study and analysis of advanced persistent threats (APT). Better classification results in the reduction of both false positives and false negatives were found when the performance was compared with Euclidean based single scale measure. This paper contributed our group's efforts towards the study and analysis of malware behavior inside an operating system

by replacing single scale similarity metric with multiscale metric and measured the performance improvement of both false positives and false negatives simultaneously.

8) Muhammad Salman Khan, Sana Siddiqui Robert D. McLeod, Ken Ferens, & Witold Kinsner, (2016) "Fractal based adaptive boosting algorithm for cognitive detection of computer malware", in proceedings of 15th IEEE International Conference on Cognitive Informatics and Cognitive Computing (IEEE ICCI*CC 2016), Stanford University, USA. (doi: 10.1109/ICCI-CC.2016.7862074).

This paper explores the behavior of Zeus malware and its variants inside a Window 7 operating system. This paper contributes the development of our malware testing sandbox and analysis of advanced mutation based Zeus and Citadel malware. This paper provides an experimental framework of data acquisition for this dissertation. Also, through this paper, information fractal dimension (IFD) based adaptive boosting algorithm was developed and tested for threat detection. This paper encouraged me to advance my research towards the characterization of mutation of malware because boosting algorithms belong to the machine intelligence category of concept drift and using IFD provided better cognitive capabilities to extract complexity of mutated malware.

9) Muhammad Salman Khan, Sana Siddiqui, Ken Ferens, "Cognitive modeling of polymorphic malwares using fractal based semantic characterization", in proceedings of IEEE 2017 International Conference on Technologies for Homeland Security (HST), pp. 1-7, April 2017, Waltham, MA, USA. (doi: 10.1109/THS.2017.7943487).

This paper introduces the concept of semantic characterization of polymorphic malware (a form of mutation). Particularly, this paper contributed the development of graph theoretical approaches to extract features from the process tree of Windows 7 data. In this paper, we discovered that using correlation fractal dimension (CFD) based cognitive and semantic analysis approach, it is possible to differentiate mutation of malware from normal operating system operations. Zeus and Citadel malware were used for testing and validation purpose.

10) Sana Siddiqui, Muhammad Salman Khan, Ken Ferens, "Multiscale Hebbian Neural Network for cyber threat detection", in proceedings of IEEE 2017 International Joint Conference on Neural Networks (IJCNN), pp. 2290-2297, May 2017, Anchorage, Alaska USA. (doi: 10.1109/IJCNN.2017.7966020).

This paper advanced our group's research in the improvement of cognitive machine intelligence to detect mutated threats reliably. In this work, we found that often the feature space of data set shows signs of nonlinear class decision boundaries. Further, we discovered the challenge of class

inseparability over feature space, which is one of the challenges I discussed in this dissertation. In this work, multiscale neural network method was proposed which shows better performance in reducing false positive and false negatives when compared with single scale Hebbian neural network.

11) Sana Siddiqui, Muhammad Salman Khan, Ken Ferens, & Witold Kinsner, "Fractal based cognitive neural network to detect obfuscated and indistinguishable Internet threats", in proceedings of the 16th IEEE International Conference on Cognitive Informatics and Cognitive Computing (IEEE ICCI*CC 2017), July 2017, University of Oxford, UK.

12) Sana Siddiqui, Muhammad Salman Khan, Ken Ferens, "Cognitive computing and multiscale analysis for cyber security" in *Computer and Network Security Essentials* Book, pp. 507-519, Ed. Kevin Daimi, Springer, 2017. (doi: 10.1007/978-3-319-58424-9_29).

In these two research publications (a paper and a book chapter), we advanced our studies and analysis on malware and class inseparability problem. Further these papers contributed a distinguishing difference between features and attributes in the context of cyber security and provides guidelines on how to select features cognitively from raw data attributes. This dissertation advances further in addressing the challenge of class inseparability and analysis of features cognitively.

13) Muhammad Salman Khan, Sana Siddiqui, Ken Ferens, "Using information fractal dimension as temperature in Restricted Boltzmann Machine", in proceedings of IEEE 2017 International Joint Conference on Neural Networks (IJCNN), pp. 2290-2297, May 2017, Anchorage, Alaska USA. (doi: 10.1109/IJCNN.2017.7966133).

In this paper, we developed a new restricted Boltzmann machine (RBM) based deep learning mechanism to analyze improvement in cognitive intelligence of machine learning method. However, for this work, we did not use cyber security data set, but image data set was used to validate and benchmark the learning and validation performance. RBM showed better performance in reducing both false positives and false negatives using IFD based fractal mechanism. Further, this work also provided a validity of using fractal approach for images having overlapping and class inseparable features which are addressed further in this dissertation.

14) Muhammad Salman Khan, Sana Siddiqui, Ken Ferens, "A cognitive and concurrent cyber kill chain model" in *Computer and Network Security Essentials* Book, pp. 585-602, Ed. Kevin Daimi, Springer, 2017. (doi: 10.1007/978-3-319-58424-9_34).

In this book chapter, we worked on developing a cognitive and concurrent cyber kill chain to map the current human analysis process of threats with traditional cyber kill chain. This kill chain

model augments the cognitive analytical capabilities of CSOC experts and provides a guideline to perform cyber forensic, incidence response (IR) and proactive threat hunting. Further, this chapter also provides a mechanism of defining a cyber-threat model for an effective characterization of malicious activities.

1.2 Research Questions

Characterizing malware behavior inside an operating system process tree poses serious challenges of the identification of suitable features and devising an appropriate methodology such that data analysis can provide accurate and relevant details of the presence of malware objects from within an enormous data of normal operating system processes consistently. Further, data analysis requires statistical knowledge which entails the need of statistical validity of the selected data analysis techniques. Therefore, this dissertation addresses these challenges using variety of features and statistical validity mechanisms in a methodical way and test the proposed methods on ten different malware executable files in a controlled experimental environment. Each executable is run separately and twice on similar environment with real time and simulated user behavior so that a reasonable generalization of the characterization technique can be ensured and feature validity can be tested. In particular, this dissertation claims to provide a cognitive **framework/methodology** to the following malware characterization problems, which can be used further for variety of cyber security based malware/threat hunting technologies and methodologies:

1) What are the **statistical properties** of host process data and how does it help in characterizing malware behaviour **cognitively**? Further, can this characterization be represented in a time based structure so that the dynamics of the system can be analyzed likewise a cyber-expert cognitively analyzes data in a cyber-security operation center (CSOC) environment? – *The main goal is to aid the CSOC cyber-experts in reducing their cognitive analysis load using an autonomous or semi-autonomous machine intelligence characterization technique*.
2) What are the appropriate time graph based **features** or set of features of operating system process tree so that malware characterization can be consistently **generalized** regardless of the type of the degree of mutation in the malware or a family of malware? – *The main goal of this characterization is to augment existing cyber-security technologies and processes of CSOC so that unknown malware objects can be hunted with sufficient degree of confidence*.
3) How to **characterize** malware behavior and **quantify** its behavioral complexity **cognitively** without having a-priori knowledge about the malware (unknown or new malware) for improving the unsupervised machine learning based clustering performance considering the **challenges** of **class inseparability** and **class imbalance**? – *The main goal is to aid CSOC experts in increasing the robustness of high fidelity alerts against advanced deceptive malware which mimic normal behavior and hide within high volume of normal data.*
4) Is it possible to improve machine intelligence performance by **reducing** false positives and false negatives **simultaneously**? – *The main goal is to improve the cognitive performance of CSOC experts who are faced with enormous false alerts and are distracted to analyze each alert which creates an opportunity for the threat actors to sneak into the network/system*.

1.2.1 Summary of Research Questions

Malvidence is a data driven malware characterization framework for cyber threat hunting and provides empirical analysis. In addition to the formal problem definition mentioned in last section, this dissertation also addresses the following theoretical and mathematical research questions:

1) Can cognitive complexity measures be used to distinguish objects from an overlapping set of objects? A corollary of this question would be: Is it possible that mutating malware behavior can be distinguishable from legitimate behavior?
2) Is there a unique set of features that can be used for characterizing mutating malware behavior reliably and demonstrates better generalization capabilities?
3) Given the limitations of conventional methods of analyzing cyber threats, is there a way to improve the modeling of mutated malware and to reinforce reliability in cyber forensic analysis?
4) What are the data driven challenges of cognitive computing in mutating malware characterization?
5) What is the appropriate data set of an operating system that can be used to ensure full visibility on malware and normal activities?
6) Can we reliably characterize activities of new (zero-day) malware in a host operating system?

1.3 Dissertation Organization

This dissertation is organized into seven major sections including section 1. In this subsection, a high level overview of each section of this dissertation is provided and a brief of how each section is related to each other is mentioned.

Section 1 presents the overall objectives and the motivation of this research work. A summary of our previous research publications and earlier efforts is provided with a brief overview of how they incrementally contributed to the final outcome of this dissertation. Further, problem definition is outlined for the proposed Malvidence framework and formal dissertation claims are established. This section also provides details of the artefacts generated in this work.

Section 2 presents literature survey and develops the background necessary to understand the domain of cyber security and the specific challenges addressed in this dissertation. It starts with a description of cyber kill chain which is used to model cyber threats and then advances into a detailed discussion on different types of malware mutation. Afterwards, a detailed description of ten mutated malware samples is provided which are used in this dissertation. It is followed by current research status in malware characterization techniques for mutated malware. Afterwards, this section proceeds into the core challenges of malware mutation which are addressed in this dissertation. In this subsection, the use cases of these challenges in the context of classification analysis and cognitive burden due to alerts triage in cyber security operational center is also provided to demonstrate a practical view of these challenges. After establishing that mutated malware characterization is posing difficult cognitive challenges, the role of cognition and cognitive computing tools in malware analysis is discussed which is followed by an elaborate discussion of the existing techniques in characterizing mutation. Afterwards, the role of graph theory in malware characterization is presented. At this point, statistical distribution tests are introduced as a way of characterizing and validating graph features for analysis of mutation in malware. It is followed by a discussion of k-means based unsupervised clustering mechanism using traditional and proposed cognitive complexity based similarity measures. Finally, this section concludes with performance evaluation metric used in cognitive machine intelligence.

Section 3 starts with the description of the threat model used in this work and shapes out the scope of Malvidence framework. It is followed by the details of the collection and processing of data in the malware sandbox. Afterwards, details of the malware dataset attributes used in the sandbox are mentioned. Finally, algorithm subsection provides high level or pseudo-code algorithmic view of the characterization techniques used.

Section 4 provides a detailed analysis of the experiments, results and their analysis. This section starts with a discussion on features extracted from the attributes of the dataset and argues the extraction of intelligent features from raw data attributes. It is followed by graph theoretical characterization of the collected data which is a process tree based dataset infected by each malware instance. This subsection also provides the mechanism of labelling malware and normal samples in each dataset. This subsection provides a detailed description on how the graph based feature transformation is applied on datasets and illustrates the application of adaptive and sliding time windowing technique to find a suitable and statistically valid graph theoretical time series.

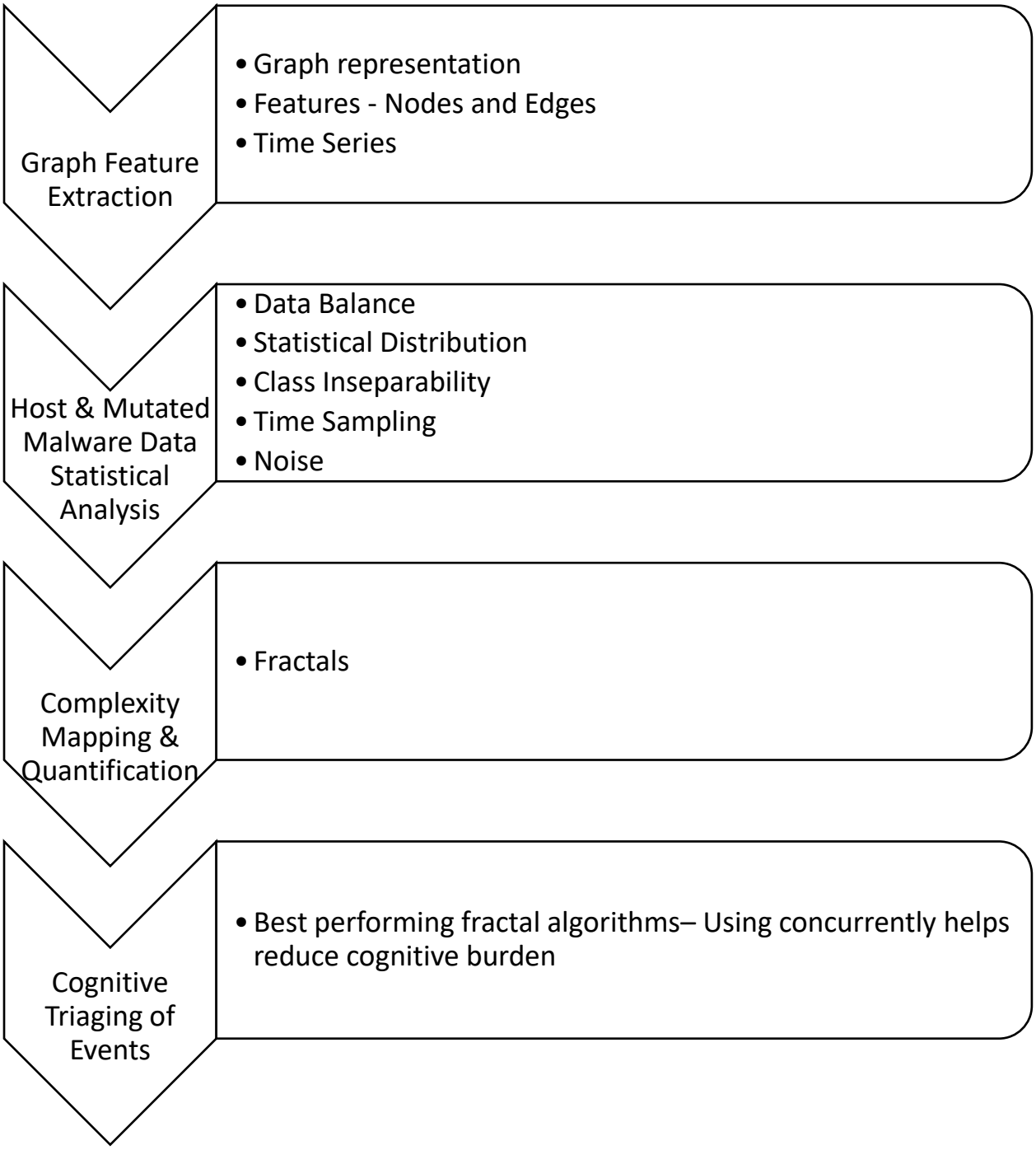
Afterwards, a fractal based cognitive characterization framework is applied to the statistically valid time graphical features and validated using mathematical models. Subsequently, graph theoretical and statistically valid time graph based features are extracted from each malware dataset and are analyzed for cognitive characterization of mutated malware such as statistical validity, generalization and significance which illustrates methodologies of reducing cognitive load by reducing false positive and false negatives.

Section 5 concludes with the summary of the major contributions claimed in this dissertation with a discussion on the limitations and the proposed future work.

Section 6 provides a list of all references used in this dissertation for citation purpose.

Section 7 lists details of the features used in this dissertation for all malware samples. First subsection provides a visual plot of all features for each malware where malware sample is labelled red. The second subsection lists the names and IDs of nodes and edges for each malware process tree data set. Malware nodes and edges are mentioned in red fonts.

1.4 Components of Malvidence



1.5 Artefacts

Several artefacts have been developed in this research work and are available for research community on request basis. These artefacts include the twenty data set files of infected Windows 7 process tree having simulated and real time user behavior. This data set also contains network related information produced by network based processes including the malware processes, although their utilization for characterization is not explored in this work. Further, several software programming scripts have been developed for host based data acquisition sandbox, MySQL database table processing, pre-processing of the raw data file and graph generation scripts for which pseudo code and algorithmic details are available in subsection 3.4.

2. Background and Related Work

In this section, a detailed study of the concepts, terminologies and challenges relevant to this research work is provided. This section has following ten subsections:

Subsection 2.1 Modeling Cyber Threats Using Cyber Kill Chain

This subsection provides a detailed analysis the methods and models used to analyze a cyber-threat systematically. This subsection provides a basis to define the threat model used in this work. Moreover, this subsection also describes the cognitive problems and challenges associated with the cyber kill chain analytical model.

Subsection 2.2 Mutation in Malware

Malware is the payload of a cyber-kill chain by the adversary. After describing the cyber kill chain model as an analytical tool for CSOC expert, a survey of the existing malware mutation techniques is provided. Through this study, this work establishes that mutation is an effective tool that malware writers use to attack a computer system in the evading existing cyber defenses successfully.

Subsection 2.3 Literature Survey on Selected Malware Samples

Now, having knowledge of the state of the art malware mutation challenges and knowing how cyber kill chain is used to launch those malware to the target victim, this subsection provides a survey of the mutation techniques of the ten selected malware used in this work. These state of the art malware mutate their existence inside an operating system using various behavioral obfuscation techniques that include mimicking a legitimate process in an operating system. This subsection provides a detailed study of these malware samples.

Subsection 2.4 Research Status in Malware Characterization

This subsection discusses in detail the status of research in malware characterization including but not limited to malware mutation techniques. It includes techniques using signatures, heuristics, anomaly and semantics. Also, this subsection summarized available sandbox methods and technologies for malware analysis. Further, this subsection also mentions the need of having Microsoft Windows based characterization framework.

Subsection 2.5 Challenges of Cyber Threats

Now, knowing that characterizing malware mutation is an open research challenge in cyber security, problems of class inseparability and class imbalance are discussed as pre-dominant challenges of malware characterization in cyber security. These challenges pose problems to the traditional cyber detection and machine intelligence techniques including but not limited to machine learning. Further, these challenges increase the cognitive load of triaging alerts in a CSOC and thus increases the probability of a successful miss. Through, the use of two use case examples, this subsection emphasizes these challenges with sufficient details.

Subsection 2.6 Cognition in Malware Analysis

As this juncture, it is established that new cognitive techniques are required to uniquely identify the characteristics of mutating malware and thus introduces the role of cognition in malware analysis. Cognitive computing is introduced and the role of complexity analysis as a tool of cognitive computing is discussed. Using fractal analysis as a cognitive complexity analysis tool, challenges of class inseparability due to malware mutation are discussed in detail. Various fractal algorithms are also described. Moreover, a new cognitive cyber kill chain model is also introduced which can provide better cognitive and concurrent analysis of cyber kill chains and can serve as an improvement in the CSOC operational and forensic process.

Subsection 2.7 Application of Graph Theory in Malware Characterization

This subsection describes the role of graph theory in transforming an abstract interdependent and dynamic process into a cognitively simple model. Moreover, a literature survey is provided to emphasise the role of graph theory in general malware characterization. A summary of the graph theoretical techniques used in this work are provided.

Subsection 2.8 Heavy Tailed Distribution and Statistical Distribution Tests

In this subsection, a detailed discussion on the theory and significance of heavy tailed distributions and statistical distribution tests for characterizing behavior is elaborated.

Subsection 2.9 K-means Based Unsupervised Clustering Approach

This section discusses k-means based unsupervised clustering approach and an argument on using K-mean over other available unsupervised clustering methods.

Subsection 2.10 Performance Evaluation Metrics

Finally, this section concludes with a quick discussion on the performance evaluation metrics used in this work.

2.1 Modeling Cyber Threats Using Cyber Kill Chain

2.1.1 Stages of Cyber Kill Chain

In 2011, Lockheed Martin adapted the military notion of *kill chain*, which models the structure of a military attack for cyber security and intrusion in a computer system and network. They developed a kill chain to define the different stages of a cyber-attack and proposed an intelligence driven framework around this kill chain for the analysis, detection, and prevention of cyber-attacks and intrusions [15]. As shown in Figure 1,there are seven stages of the Lockheed Martin cyber kill chain model; (1) Reconnaissance (R), (2) Weaponization (W), (3) Delivery (D), (4) Exploit (E), (5) Installation (I), (6) Command and Control (CnC), and (7) Actions on Objectives (A). This framework lays out a sequential model or process of how an adversary would carry out its malicious objectives. The model is based on the premise that threat actors attempt to infiltrate computer networks in a sequential, incremental, and progressive way. The model is structured so that, if any stage of the kill chain is blocked, then the attack will not be successful. Cyber security experts aim to detect a threat as early in the kill chain as possible to minimize losses. Nowadays, Security Operation Centers (SOC) or Cyber Security Operation Centers (CSOC), Incident Response (IR) and Threat Intelligence (TI) teams in organizations use the cyber kill chain model as a process guide to analyze the data captured from attacks, perform forensic analysis and take preventive measures at each step of the kill chain [16]. These seven sequential steps in a cyber kill chain provide information about the tactics, techniques and procedures (TTP) of the adversary and are described below.

Figure 1: Lockheed Martin cyber kill chain model.

2.1.1.1 Reconnaissance (R)

Reconnaissance is the first step in the kill chain, during which a threat actor collects network and/or endpoint information about the potential target, who could be a single person, an organization or a hardware/software part of the target system or network. At this stage, a threat actor performs covert investigations about the target entity and identifies the potential methods to break into the network. Also, research at this stage provides information on what type of malware objects could be deployed into the target network without getting detected by the cyber security defenses (vulnerabilities) [17]. Further, backdoors in the target system or network are determined [15]. Moreover, at this stage the adversary determines an appropriate set of infiltration objectives to be carried out into the target. If the objective is to steal private information, then the threat-actor must research, identify and find a way to create a two way link, so that it can first enter the network, find the information of interest and then exfiltrate it out of the network in a stealth mode. If the

objective is to destroy or disturb the network, then a one way link can do this task. Regardless, the threat actor aims to find weaknesses of the system/network or the users to exploit and enter illegally. For example, spam phishing email can be considered a one way link to deliver malware as email attachment [18]; As soon as the email recipient opens the attachment, the system will be compromised and damaged. This example demonstrates how a threat actor exploits the email communication medium to attack the network. An example of a two way link is finding open ports using a port scanner; upon finding an open port, an authorized two way telnet communications session may be created.

2.1.1.2 Weaponization (W)

Weaponization is the second stage, during which the threat-actor develops the deliverable payload. An adversary uses the information collected at the reconnaissance stage (target vulnerabilities and backdoors) to prepare and plan how the vulnerability/backdoor should be exploited and what methods should be adopted to deliver the malware. [19]. There are two types of payload that can be delivered at this stage, (1) malware that does not require any communication with the adversary, e.g. viruses and worms, or (2) malware that requires communication with the adversary to get command and control signals and/or send the stolen information back to the adversary. The latter are known as Remote Access Trojans (RAT). A RAT requires both client and the command and control server. The RAT client is the actual deliverable payload that is also configured on how to communicate back with the command and control server, which resides on the internet and is controlled by the adversary. For example, from the reconnaissance stage an adversary learned that at a certain university, the email system does not allow *.exe file but does allow *.pdf file attachments in the emails. Also, the adversary learned that professors routinely open *.pdf files of emails from students seeking registration to the university's graduate programs. Accordingly, the adversary creates a RAT malware file, with the capability of communicating with a command and control server, and embeds this malware file within a portable document file (pdf) named myCV.pdf, which is to be sent as an attachment via a phishing email. Another example is the credential harvesting mechanism to lure/force the target to visit a well-known, but counterfeited and cloned website and gather privacy information that will be exploited against victims.

2.1.1.3 Delivery (D)

After the malware payload has been developed and the backdoor to deliver the payload has been identified, the delivery stage is executed. The malware can be delivered either by luring or forcing the user to interact with the malware exploit or it can be delivered automatically by exploiting the weaknesses of the protocols and/or software. For example, the phishing email can be used to deliver the malware payload in a file attachment by duping the user to think that the email is genuine and thus download the malicious attachment; or, they are duped to input their privacy information in a typical phishing email that will be transmitted back to the attacker. Delivery is a critical part to ensure a successful attack by remaining undetected by existing security mechanisms. Therefore, adversaries design their attacks in such a way that, although the traces of

their attack may not be removed, those traces should masquerade the attack source from the security and forensic experts. Further, threat actors utilize multiple delivery methods to increase their rate of success. The malware exploits which do not require user interaction are most difficult to catch, because they utilize an inherent flaw in the protocol, program or software to deliver the payload or execute a piece of software for illegitimate purpose [20]. This inherent flaw is called a vulnerability of the software and requires software patching. For example, a malicious Java script within a Flash software file can be exploited to deliver the malware to the target computer as demonstrated in [21]. A detailed discussion is available in [2].

2.1.1.4 Exploitation (E)

After a successful delivery of the malware payload to the target computer, the exploitation stage is initiated by preparing for the successful installation of the malware inside the target computer/system. As mentioned in [22], following conditions should be fulfilled to ensure successful installation of a malware:

a) The malware should have the required access rights to be installed in the target computer.

b) The operating system or software of the target computer should be able to install the malware without additional requirements. For example, malware compiled for the Linux operating system cannot be installed on a Microsoft Windows operating system.

c) The antimalware defenses of the target computer should not be able to detect the malware otherwise the attack will fail causing cyber kill chain to be broken.

The exploitation stage does not actually perform the installation; rather, it prepares the environment to launch the installation stage of the kill chain. However, this stage is connected closely with the installation phase since all the requirements of the installation stage should be fulfilled by the exploitation phase. In order for the delivered payload to be installed, there must be a software or hardware bug that the payload can exploit for either installation or execution. These bugs are called Common Vulnerabilities and Exposure (CVE). A public database of the vulnerabilities is available at [23] which is updated as soon as a vulnerability is discovered. Further, researchers and developers use this database to improve their software and provide patches. However, this database is incomplete and there are unknown vulnerabilities which can be utilized by the threat actors to execute the exploit stage. Moreover, attacks can be a combination of the above categories, e.g. a web based ransomware attack is launched after exploiting both software vulnerabilities and network vulnerabilities [24]. Further discussion is available in [2].

2.1.1.5 Installation (I)

A computer infection starts at the installation stage. If the malware is an executable file or the malicious activity is based on code injection or an insider threat, then the installation stage is not required. However, if the malware needs to be installed in the target computer, then the delivery stage should have delivered the dropper or downloader in the target computer and the exploit stage has already been completed by disabling the security defenses and finding a hook in the operating

system to start the installation of the malware. At this stage, malware is installed and the installed files either use the libraries and support files of the operating system or acquire those files from the downloader or dropper packages [25]. Further, the malware installation updates the file access mechanism of the operating system using the privileged access rights. In addition, the malware changes the appearance of its files either by changing the format of the file or hiding those files from user access. Also, advanced mutated malware are able to change their memory footprints to evade detection by sandbox algorithms or behavior based antimalware systems. These malware are also called as either polymorphic malware or metamorphic malware respectively [26]. A detailed description of polymorphic and metamorphic malware is provided in the later sub-section. Installation stage not only installs the backdoor inside the target victim but also ensures that the threat actors are able to communicate with the victim computer persistently [27]. It is noted that this stage does not start communication with the command and control mechanism for the malware activity. Also, this stage differs from the Exploitation stage due to locality of the activity i.e., the Exploitation stage ascertains that the malicious package is ready for installation and all requirements of the Exploitation stage are fulfilled while during the Installation stage, the actual payload starts setting up its foothold inside the victim computer locally. Also, a persistent connection with the server is established to initiate command and control communication. For example, a malicious web shell is installed on the victim computer at this stage, which ensures persistence and evasion from detection mechanisms using either new signatures or changing heuristics of its behavior by introducing mutation.

2.1.1.6 Command and Control (CnC)

Command and control networks can be servers, peer-to-peer networks or social media servers. Further, there can be multiple levels of command and control networks (e.g. bot networks) to evade detection. The Command and Control stage is present in those malicious attacks whose objectives are as follows:

a) Steal the information (e.g. passwords, financial data and intellectual property) from the target computer, e.g. key loggers, Zeus and Trojan.Coinbitclip [28].

b) Send instructions to the malware in the target computer to spread the malware to other parts of the network connected with the target computer, execute the malware or activate the encryption for ransomware activities, among others.

It is worthwhile to mention that for cyber defenders, the CnC stage is the last stage to block the malicious activity. The CnC stage takes place similar to normal internet communication. In addition to endpoint defenses, network perimeter monitoring plays an important role in detecting an illegitimate network connection. There are two major types of command and control servers based on communication:

a) Servers having meta-information about the compromised nodes through beacons or heartbeat messages.

b) Servers communicating actively with the target nodes by issuing commands to control the victim nodes and performing more malicious actions like data exfiltration.

Further, command and controls servers can be divided into direct and indirect communication categories as follows:

a) In direct communication, malware at the victim node contains a list of various command and control server IP addresses so that if a certain IP address is blocked, the malware hops for another IP address to maintain the communication. This trait is also called persistence.

b) In indirect communication, threat actors utilize legitimate intermediary nodes to maintain communication. A group of legitimate nodes is compromised for the purpose of establishing communication link whereas the source of the link remains hidden from the victim [12]. Therefore, a botnet is created to re-route the communication from victim to the source.

Attackers may use different methods to establish an outbound connection. They may use email protocols to deliver the payload but then use single or multiple HTTP connections to establish an outbound link. Further, they may use compression mechanisms for siphoning data. Attackers would diversify their tactics and techniques to evade detection. However, the common denominator is network traffic, and if an endpoint security mechanism cannot detect the presence of a communicating malware, network defenses can do the job.

2.1.1.7 Actions on Objectives (A)

This is the last stage of cyber kill chain and is responsible for executing the objectives of the attack. At this stage, if the malware is deployed in the target computer then it starts performing the programmed function either through the instructions from command and control server or independently. This stage is also known as the detonation stage where the cyber kill chain is completed successfully.

Following are the major categories of actions that fall in this stage:

a) Data exfiltration: stealing personal and/or intellectual data from the network.

b) Ransomware: Threat actors hold victim data hostage by encrypting the victim’s data, change credentials or blocks network resources using various encryption methods and demand ransom payment.

c) Cyber terrorism: threat actors inflict damage by erasing data or corrupting the files completely.

2.1.2 Critique of the Cyber Kill Chain Model

As Internet has evolved from a traditional web model to a cloud based model, and with the prevalence of social networking and mobile technologies, traditional security measures including, but not limited to, firewall, antivirus, intrusion detection/prevention systems and access control lists are proving to be futile and insufficient. Even with multiple layers of security defenses, threat actors are able to infiltrate a network and render persistence in their tactical measures and techniques. Persistence is a characteristic of threats whereby threat actors launch sophisticated attacks in such a way that the behavior and signature of those attacks evolve dynamically to remain undetected by the security defenses and the duration of attacks spans a large time interval [29]. These threats are typically orchestrated by organized entities and the threat actors are resourceful, patient and aim to exfiltrate confidential information, damage the network's operational capabilities (e.g. taking down an online shopping website) and ultimately strike at the organization's credibility in the eyes of their clients and customers. For example, [30] reported that Yahoo declared hacking of more than 1 billion user account IDs and passwords from the Yahoo email servers in 2013 and 2014. This attack is known as the largest known attack in the history of internet thus far. This attack also involves stealing of user private information including date of birth and security questions. Also, these attacks include stealing Yahoo proprietary source code that is equivalent to stealing intellectual property information. This news of attack was disclosed when Yahoo was negotiating with Verizon Inc. to sell its Yahoo email business at a price of US$4.8 billion. This news has reportedly hurt this deal as well. According to [29], persistent threats should be analyzed using adaptive approaches and the network should be scanned continuously for new and old anomalies. Further, along with traditional security approaches, defense-in-depth and layered security should also be considered to stop mutating threats such as advanced persistent threats (APT). These defenses include sandboxes, honeypots and machine learning engines to analyze existing data for a possible command and control activity.

Existing cyber kill chain stages remain valid but the factor of persistence should be taken into account for those chains which are not completed yet. According to [31], a cyber kill chain attack contains one intrusion or one attempt of an intrusion while APT attack is composed of multiple kill chains. Each kill chain contains one of many indicators of attacks and APT attack could be detected by evaluating and analyzing all such indicators together. For example, an APT attack starts with initial reconnaissance, skips weaponization, finds an exploit to escalate the privileges, performs an internal reconnaissance, moves laterally to the high valued computing nodes, waits and performs internal reconnaissance again, adapts the behavior according to the normal behavior of the network to avoid detection, ultimately infiltrates the target computer(s), and establishes command and control. As can be seen in Figure 2, there are multiple reconnaissance stages and various stages of the kill chain are skipped. Further, there are many permutations of each cyber kill chain stage that could be taken by the threat actors to infiltrate a network successfully [32]. Also, it can be considered a reuse of different stages of cyber kill chain multiple times to achieve the final malicious objective.

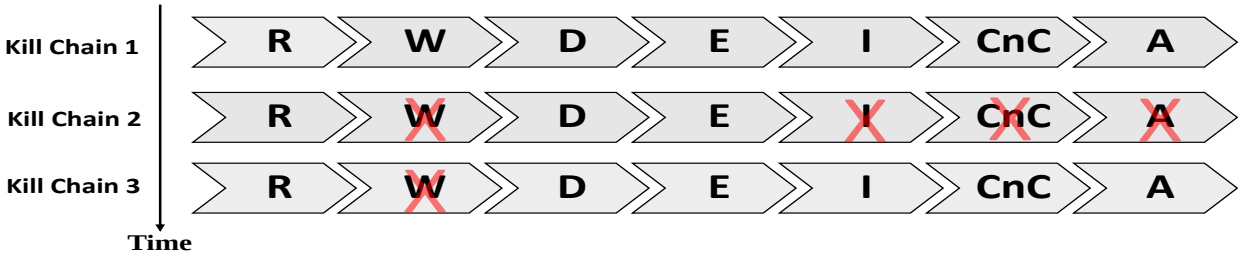


Figure 2: Example of an APT attack with multiple cyber kill chains.

It is of paramount importance that security research should not be focused on conventional single kill chain; however, a holistic idea of multiple kill chains (persistence) should be taken into consideration when beefing up against threats. Further, it should be important to understand the motives of the attacker, rather than looking at what the attack is doing. For example, if the motivation is to steal financial information from servers, then there will be a command and control communication going outbound the network, and it should be visible to network monitoring system for detection and prevention. In order to curb APTs, there are various modifications proposed in the literature as follows:

a) Author in [33] suggested a modification to look at internal cyber kill chain stages. However, this model lacks the critical factor of analyzing the network defenses in a layered approach. Network perimeter security does an important job of holding back plethora of network based threats, such as illegitimate SSL connections.

b) Marc Liliberte in [34] proposed an updated cyber kill chain as shown in Figure 3, where the weaponization stage is removed and the lateral movement is introduced after the command and controls stage, which emphasizes the horizontal movement of the attack to gain access on the targeted assets with the use of intermediary nodes. However, many advanced threats perform lateral movement using multiple command and control communications [33]; therefore, this model lacks a holistic approach in addressing the variety of threats altogether.

c) Author in [35] discussed a holistic model covering the policy making, technical and legal aspects of an attack simultaneously. Their model performs better in generating a consensus among various stakeholders about an attack and deciding the course of action to thwart it. However, their work is more focussed towards addressing the shared inference concerns of a threat faced by an organization and helping the stakeholders in converging towards a combined consensus.

Similarly, there are variety of other models that emphasizes one or more aspects of the cyber kill chain and either add or modify the kill chain stages to reinforce the defenses.

Figure 3: Modified cyber kill chain by Marc Liliberte.

2.2 Mutation in Malware

2.2.1 Malware Obfuscation Techniques

The signatures used by malware detection software comprise of patterns that can be used to detect the presence of an infected program. A pattern may refer to, but not limited to, a set of strings, a group of assembly program instructions, or a hash function. Further, a malware program or software primarily consists of two main components:

1. Payload.
2. Decryptor.

The payload is the actual code which is responsible for the core functionality of the malware, while the decryptor is a block of instructions, which decrypts the payload and executes it in the memory. It is important to understand that the payload is often morphed using techniques like encryption and thus, changes its signature. On the other hand, the decryptor routine remains constant, which may be exploited to detect the presence of malicious code in an executable. Knowing this, a malware developer may consider writing a new decryptor for each instance to avoid detection by the anti-malware systems; however, this is not a feasible idea. Hence, malware developers also apply mutation techniques for each replica of the original code. Some of these mutation techniques are discussed below [36] [37] [38] [39]:

2.2.1.1 Dead Code Insertion

The type of program instructions which do not perform any particular function like NOP (No Operation Performed) are introduced at different offsets in the malware code to make the signature based evaluation difficult.

2.2.1.2 Instruction Substitution

This technique involves replacing the instructions with their equivalent counter parts. It implies that the new instruction will perform the same function as the previous ones but will have a different program structure.

2.2.1.3 Register Swapping

This method replaces the unused registers with registers used in malware code.

2.2.1.4 Subroutine Re-ordering

Another way of achieving a mutated code is to change the order of the subroutines such that the behavior of the malware remains unchanged.

2.2.1.5 Entry Point Obfuscation

The malicious code is placed in an unlikely position in the infected file. Usually, the entry point of the target executable is modified to point towards the malware payload, which later returns the control back to the host executable. However, the EPO enabled malware are placed such that they are not pointed directly by the target executable, rather gains the execution control during apparent benign program execution. Thus, the malware detection programs which investigate the modification in the entry point may not detect the presence of this malicious piece of code.

2.2.1.6 Using Executable Packers

An executable packer is a program that compresses a binary leaving the program unreadable. The packed binary resumes its original form in the memory whereas it is stored in the compressed format on the storage.

2.2.2 Malware Categorization based on Code/Syntax Obfuscation

Based on syntactical mutation techniques, as suggested in the literature [40], malware can be broadly classified into three main categories in the order of increasing detection complexity due to obfuscation:

2.2.2.1 Oligomorphism

One of the simplest ways of obfuscation is the encryption technique employed on the payload. However, a decryptor is needed to unlock the malware in order to execute it. The detection of these types of encrypted malware which have a distinct decryptor is easier. Therefore, the malware writers created samples which have a limited number of decryptors stored as data in its body. The decryptor selection for an instance is random [40] but is a fixed size. A malware sample, which can generate multiple number of decryptors, say n where $n > 1$, is considered oligomorphic malware [41]. The signature based detection of these types of malware is feasible since, it requires generation of n number of patterns, where n is fixed. Another limitation of oligomorphic malware is that the decryptor is stored in the malware body and hence, increases its size. One of the first oligomorphic malware was ‘Whale’ [40].

2.2.2.2 Polymorphism

The term polymorphism refers to the act of changing the appearance [42]. Malware which is able to generate a unique decryptor for every instance of the malicious program is called Polymorphic malware. On every execution, the new decryptor generated by the mutation engine is combined with the encrypted malware payload to generate a new malware variant. There are different ways to create malware, which are syntactically different, but perform the same function [43]. The first Polymorphic malware was a DOS virus designed in 1990 and was known as V2PX

[40]. The detection of these malware was not possible at that time; nevertheless, the x86 based emulators were introduced to emulate smaller sections of the code to check any possible matches with the known decryptors. The focal point of detecting these malicious software is the reliance on decryption of the original piece of code into plausible form. This is achievable by scanning memory for the known signatures [44]. For polymorphic malware the number of available automatically generated decryptors is relatively larger than that of oligomorphic malware.

2.2.2.3 Metamorphism

Metamorphic malware is classified as complex in term of its mutation characteristics, since it mutates the payload using the obfuscation techniques discussed in the previous section. These malware do not have a decryptor however, they have a continuously changing malware body. The detection of these malware is analogous to the detection of a moving target as the payload transforms with each instance [42]. The specialty of these malware is attributed towards the uniqueness in the sample variance, while the only constant is the behavior of this malware. The first metamorphic virus was 'Simile' which could disassemble its code into an intermediate form, then shrink itself by removing redundant instructions and after that permute this intermediate form which increases the size by adding redundant code, and finally re-assemble this intermediate form [45]. In order to generate the next sample, the metamorphic malware needs to re-analyze the mutated code of the previous version and requires some coding conversion mechanism or any specialized algorithm which can detect its own obfuscation. Thus, it clearly indicates the presence of a pattern in mutation, which can be exploited to detect these metamorphism in malware [40]. Currently, the syntactic detection of this malware utilizes automatic identification of the code and memory snapshots analysis. However, the semantic evaluation of this malware is the key towards robust and reliable detection of these highly sophisticated malware.

2.2.3 Malware Mutation based on Behavior Obfuscation

In this dissertation, malware mutation based on activities in the host process tree is analyzed and characterized [46] [47]. Behavioral based mutation is considered with respect to the malware execution activities to remain hidden inside the operating system's legitimate process tree data or mimic the legitimate process tree behavior i.e. using the legitimate process name, executing without file and code injection. Similar to syntactical mutation, the purpose of this mutation is to maintain anonymity or pose deception to evade detection. Although mutation in the malware software program is defined in terms of changing the syntax, malware behavior mutation is defined in terms of obfuscating its behavioral dynamics so that it is either considered legitimate falsely or is not found through traditional behavioral detection approaches e.g. class inseparability problem. However, to characterize the malware behavior dynamics, it is required that the malware process should be present in the process tree. When a malware executes inside an operating system, it is attached to the process tree by virtue of the operating system's function and therefore, it can be

characterized with the proposed Malvidence framework. However, if the malware sits idle in the memory and does not execute then it may or may not be characterized due to its unavailability in the process tree [48] [49] e.g. Duqu malware.

Once the malware is delivered successfully to the target host and is deployed in the host memory, its execution starts that may include exfiltrating target data to the remote command and control mechanism, damaging the memory of the host or ransomware operations. However, during this execution stage, advance and intelligent malware should be able to detect the presence of any malware detection technology and should mimic the normal host processes and remain low and slow in volume and activity to evade being detected.

A malware software requires similar resources to operate as a legitimate software may require i.e. memory resources, operating system calls, writing to registry and creating network endpoints. From the perspective of host based operating system, software execution is based on processes and modules which are visible through a process tree relationship program of the operating system. When a software executes, it opens certain processes and their concatenated modules through various system calls to the operating system. The processes and modules are well known for legitimate software and are also known for malware with pre-known signatures, however, new malware or their mutated variants are being created in a matter of few seconds [50] daily and therefore, introducing new processes and modules. Further, new generations of advanced mutating malware are able to mimic the behavior of legitimate software, not only in adapting the process and module names, but also behaving similarly in the time changing process tree structure of the operating system [51] [52] [53].

2.3 Literature Survey on Selected Malware Samples

In this thesis, ten different malware samples are selected to study and characterize malware mutating behavior inside a Windows 7 operating system. A summary of the selected malware samples along with their types, objectives and behavioral mutation mechanism is presented in Table 1 and then described in detail later. These malware are selected because of their capability in their persistence and render intelligence and anonymity in evading detection mechanisms. Further, these malware are discovered within the last ten years and are highly polymorphic in nature. As can be observed from Table 1, the example of process names and the behavioral mutation activities for each malware sample shows that all these malware mimic legitimate Windows 7 processes in their syntax and attributes and thus bears the capability to mutate and obfuscate their existence.

Table 1: A behavioral summary of selected malware samples.

No.	Malware Name	Malware Type	Malicious Objectives	Behavioral Mutation Mechanism	Example of process name (using legitimate names)
1	Zeus	Backdoor Trojan	Exfiltrate Confidential Information to remote CnC	(1) Mimicking legitimate Windows operating system process name, (2) Copies into Windows System Directory,(3) Injects into Windows Processes	Winlogon.exe, explorer.exe
2	Citadel	Backdoor Trojan	Exfiltrate Confidential Information to remote CnC	Mimicking legitimate Windows operating system process name	firefox.exe
3	Poweliks	Backdoor Trojan	Exfiltrate Confidential Information to remote CnC, Click Fraud Operations	Fileless Trojan and uses legitimate Windows DLL files	dllhost.exe *32
4	Nivdort	Backdoor Trojan	Exfiltrate Confidential Information to remote CnC	Disabling host firewalls and removing strings from memory to evade memory based signature detection	issch.exe

5	Stabuniq	Backdoor Trojan	Exfiltrate Financial Information to remote CnC, Click Fraud Operations	Creates multiple copies with different names of the files/processes with legitimate names	iexplore.exe
6	Proteus	Backdoor Trojan	Exfiltrate Financial Information to remote CnC, Click Fraud Operations, Converts victim into a proxy server for malicous traffic flow	Creates multiple copies with different names of the files/processes with legitimate names in %AppData%	Google Chrome Executable
7	Alina	Backdoor Trojan	Exfiltrate Point of Sales Financial Information to remote CnC	Creates file/process with legitimate names in %AppData%	adobeflash.exe
8	Zurgop	Backdoor Trojan	Exfiltrate Confidential Information to remote CnC	Creates file/process with legitimate names in %AppData% and then in %temp%	Systemini.dll
9	Hupigon	Backdoor Trojan	CnC is used to control the victim machine	Injects malicious code into the thread of another legitimate process	calc.exe
10	Carberp	Backdoor Trojan	CnC is used to control the victim machine and steal confidential information	Injects malicious code into the thread of another legitimate process	svchost.exe

2.3.1 Zeus

Often known as Zbot, Zeus is a Trojan malware which was first detected back in 2007. It laid the foundation ground for a lot of other malware families, which spawned from its public source code, thus, compromising the integrity and security of millions of computing machines. It was spread worldwide through spam campaigns and drive-by-download techniques. The victims include giants like Bank of America, NASA, ABC, Oracle, Cisco, Amazon and BusinessWeek [54]. Primarily, this Trojan was designed to capture confidential personal and financial information including target machine information.

In order to spread the infection to other machines, Zeus malware owners create a network of bot executable files which can be controlled by the attacker through a command and control server. Then, it is dropped to the victim's computer using spam techniques like fraudulent email attachments or by corrupting legitimate websites, which drops the files on the target machine [55], when visited by the user,. The information stealing mechanism includes recording the key-strokes and monitoring the users' visited webpages by form grabbing. Some variations even affect the mobile devices to capture the two-factor authentication. It creates different files under the system folder of the Windows and even affects the registry entries to ensure its presence on machine reboot. Another variation of Zeus was observed in 2013 and called Gameover Zeus. Due to its inherent peer-to-peer communication nature, this malware was least susceptible to the detection strategies. It even distributed the deadly CryptoLocker ransom virus worldwide. Later on, it evolved into Chthonic and Sphinx and has infected more than 3.6 million computers in US alone [54].

When the Zeus bot reaches the target computer, it is copied according to the user's privileges. If the compromised user is an administrator, it is copied under the system Windows system folder; otherwise, it is copied in the user profile directory. Along with the executable file, some DLL files (Windows operating system files) and a configuration file are as well delivered to the attacked system [56]. It keeps a text file to store the stolen information and creates new Registry entry upon installation. Further, it injects itself into one of the Windows services, i.e., winlogon.exe or explorer.exe, depending on the user privileges. It also checks for the availability of updated configuration file periodically. Once, the attacker gains control of the system, multiple illicit operations can be performed including but not limited to downloading and executing file, rebooting the computer, deleting critical folder and files, disabling access to particular websites, stealing cookies and digital certificates, injecting fake HTML code into valid webpages, and activating and de-activating the bot [57].

2.3.2 Citadel

One of the offspring of Zeus, Citadel, is a malware toolkit to create and maintain botnets, which can be directed to steal critical personal and financial information from the target by logging key strokes and capturing screenshots of the victim's system. It has been reported to infect about 11

million computing machines across the world and caused financial losses of half a billion [58]. It is usually spread and dropped on victim's computer using drive-by-download technique.

The malware kit requires the threat-master to create a webserver and establish a database. Usually, Apache and PHP are used to setup the server and MySQL is used as a database. Once the kit is installed, the information about the active or inactive bots on multiple victim machines can be tracked easily. Each bot is created using a component called builder and is distributed using compromised websites. Each bot is able to evade standard malware detection software and further prevents the access to the antivirus vendor sites. Once infected piece of code is installed successfully it communicates back to the command control server. The logs of the victim machine containing sensitive data are periodically shared with the attacker who can further control the infected machines through sending command. Moreover, the control panel of the Citadel toolkit provides detailed information of each of the infected clients, including the operating system information, installed programs, stolen credentials, visited web pages and screenshots. It can also be transformed into a ransomware and lock the system [59] [60] [61].

Citadel established one of the earliest examples of the malware-as-a-service on dark-web forums. One of the special features of the Citadel was its online technical support system, which let the cyber-criminals file bug reports, provide their opinions on updated version of the botnet and track the tickets referencing an older issue. It enables the Citadel users to share information with fellow malware developers and users. However, it is this unique feature which led to the arrest of the Citadel developers and maintainers [58].

2.3.3 Poweliks

First discovered in August 2014 [62] by G Data Security Labs researchers, Poweliks is a ***fileless*** Trojan horse which performs click-fraud activities on the infected system. Fileless infections are characterized by their sole presence in the Microsoft Windows registry database and hence, do not reside on victim's hard disk in the form of a file [63]. Moreover, click-fraud operations primarily involve interacting automatically with the covertly downloaded online advertisements in large number on the targeted computer. The key objective is to earn advertising revenue for the attacker. The persistence of this threat comes from the fact that its code is not saved in a file rather is available in a registry key in Windows Registry, thus ensuring its stealth nature on the compromised system. After the initial installation, the installer deletes itself [64].

Different variants of this Trojan have been distributed through spam email attacks or through the use of exploit kits, depending on which the malware may perform the following actions on a victim's computer [64] [65]:

- Collect user and system information and exfiltrate it to the remote server.
- Execute click-fraud operations.
- Cause secondary infections by malvertisement.
- Connect to the remote server to get further instructions from the threat-master.

The advertisement request mechanism for Poweliks is based on keywords while manipulating searches such that it appears a legitimate user request. Then, it loads the URL returned by the advertisement network, allowing the attacker to receive money. The catch is these advertisements are not displayed to the victims, and hence, they remain unaware of infection. It can request about 3000 advertisements per day directed towards the compromised system, thus causing the victim's system to be slow due to heavy utilization of processing power and network usage. Also, due to the downloading of huge number of advertisements, it acts as a vehicle for downloading other malwares like ransomware [66] [62].

As Poweliks executes without a filesystem object, it easily evades detection by running directly from the registry and memory. This is achieved using Microsoft Windows operating system executable "rundll32.exe", which is a legitimate Windows file used to execute Javascript code embedded within a registry sub-key. This code further reads data from the registry which acts as a payload that is executed as a Dynamic Link Library (DLL) in memory [67]. A snapshot of the Trojan Poweliks in the registry is shown in Figure 4. The placement of code in the hidden registry keys ensures the persistence of the threat after the system reboot. Also, a "watchdog" process is installed to verify the operation of the Trojan, which may modify access rights and use obfuscation techniques like unprintable characters to keep the keys hidden. Also, it reinstates them if they are deleted [62] [67]. Multiple dllhost processes are spawned after the initial setup of the Trojan which perform the actual search engine injections and click fraud operations [68].

In addition, the Trojan horse hijacks CLSID keys [69] to use new load points. Basically, CLSID entries provide proper run functionality in the Windows operating system. Augmenting them with the malicious sub-keys indicates that Poweliks is executed every time a legitimate activity like folder opening is performed [70]. Further, it exploits zero-day vulnerability to take control of the compromised system [66]. The innovation in obfuscation strategies used in Poweliks is a glimpse of the capabilities of future threats.

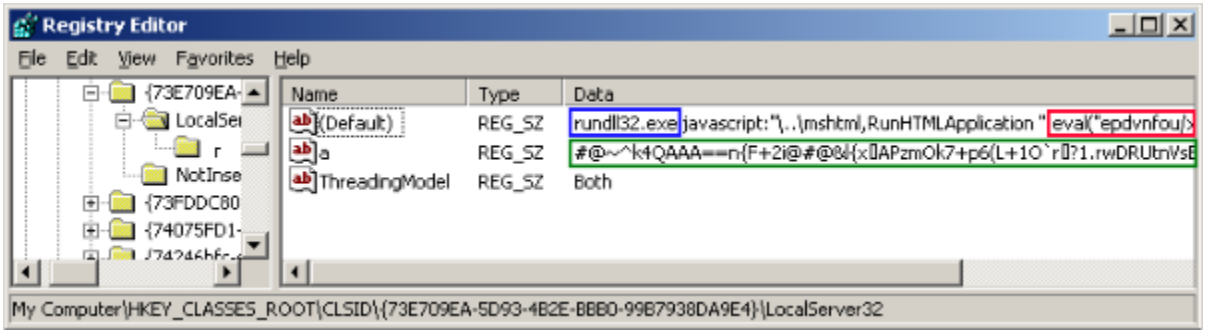


Figure 4: Poweliks inside the Windows OS registry [66].

2.3.4 Nivdort

Nivdort belongs to the family of password collecting Trojans which can additionally steal other critical data like victim's IP address, system configurations, running processes information, credentials, and banking information [71] by recording keystrokes, code injection, reading metadata of the visited websites and taking screen shots. The gathered sensitive data is then exfiltrated to the remote server from where further information is obtained. Even some versions of this malware can automatically run, upload and download files [72] to update themselves and/or launch additional malware.

Nivdort is not capable of spreading on its own; rather, it is often shared using an attachment in spam email, pretending to be legitimate, and social engineering to entice user to open the malicious payload. Upon execution it displays an error message which is fake and thus, successfully installs itself on the victim's node. The installed files are available in the Windows system folder and the modules are placed under the Windows Startup directory in a hidden folder [73]. Moreover, a registry entry is also created to ensure the malware presence is maintained after system reboot [74]. Also, advanced variants of the malware can modify the Windows hosts file to redirect specific URLs to different IP addresses. It means that on a compromised system, a user may not be able to access security related websites. Further, this Trojan can disable host Windows firewall notifications [75].

One of the characteristics of Nivdort is that each generated sample is different from the other one. This is because the recipient's email address is encoded and embedded in the malware binary file. Hence, it is one of the few most circulated Trojan in terms of unique samples prevailing in the cyber-space [71]. Another important aspect of this Trojan which adds to its complexity is the usage of domain generation algorithm for command and control server addressing thus, making its memory dump difficult to be analyze. In addition, the dumping mechanism used in Nivdort ensures that the strings are cleared from memory after execution hindering the string analysis method of sandbox based malware detection [76]. Thus, based on email phishing campaign, Nivdort family of malware has demonstrated several improvement in its obfuscation mechanism and therefore, is among few malwares with high number of unique infections [77].

2.3.5 Stabuniq

Stabuniq is a Trojan horse which was discovered in 2012 and aims to steal confidential information from the compromised system. The sensitive data it gathers may include system information, IP address, processes information, installed programs, and operating system's knowledge [78]. The collected data is then transferred to the remote command and control server. Earlier, it targeted the Eastern financial institutes of United States and has been found in proxy, mail and gateway servers of these institutes. This is in addition to the infection of desktop PCs and computers in security firms.

This malware relies on spam emails for delivery and distribution, which contain links to the server hosting web exploit kits. These kits are responsible for download and activation of the Trojan [79]. Upon execution, the installer creates multiple files under the Windows application folder, thus, masquerading itself as legitimate. Also, the executable obtained after the malware copies itself may have one of the following possible names:

- jqs.exe.
- issch.exe.
- smagent.exe.
- acroiehelper.exe.
- groovemonitor.exe.

Moreover, it creates malicious registry entries to ensure its persistence after a windows reboot [80]. After the installation, the original file is deleted. Further, it injects code inside the "iexplore.exe" process and exploits it to silently execute malicious activities like sending sensitive information via HTTP protocol [81].

2.3.6 Proteus

Proteus is a versatile botnet that can convert the compromised system into proxy servers for malicious traffic flow, keystrokes logger for stealing sensitive information, stolen credentials validator to check the integrity of the stolen information, and Cryptocurrency miner [82]. It is written in Microsoft .NET language and has the capability to download and run files on request thus, also enabling threat-masters to update malware [83].

Proteus can be spread through social engineering based spam attacks, hacked websites, relay chats and peer-to-peer (P2P) file sharing networks. It was dropped as a Google Chrome executable file on the targeted system by its cousin, Andromeda botnet. When executed, Andromeda drops copies of itself in %AppData% folder and establishes a connection with the command and control server. Then the exfiltration of critical system information is initiated to create a distinct fingerprint of the victim. Further, a Keylogger and miner is installed in the infected system [83]. The malware may utilize SHA256 miner, CPUMiner and ZCashMiner to mine crypto-currency using local CPU or GPU [84].

The communication of the bot with the command and control server utilizes symmetrical encryption. Also, a hardcoded mutex of the bot is generated to ensure execution of single instance at a time. After specified interval of time, the bot checks for the presence of command and control server and if it active, the malicious activities are carried on [85]. In short, Proteus launches a multi-faceted attack causing high utilization of processing power and bandwidth. It can severely affect victim's computer by performing its malignant operations.

2.3.7 Alina

Alina is a Point of Sale (PoS) malware which was originally created in 2012 and is used to steal banking cards credentials for monetary gains. In late 2013, the source code of Alina was sold online which sparked the generation of further variants. Some of the malware which uses the same or updated code base of Alina include Backoff, JackPOS, Spark, Eagle, and Katrina [86].

On a PoS system, when Alina gets executed, it installs itself on the system and checks for the updated code. If an update is discovered, the existing malware is removed and the new one is installed. Then, the file path is added as a registry entry for automatic execution of the malware every time the system boots. It may copy itself with different filenames, some of which resemble the legitimate filenames on a system. Following is a list of possible file names [87] for Alina under the user's %APPDATA% directory:

- adobeflash.exe.
- cmd.exe.
- csrss.exe.
- ctfmon.exe.
- dasHost.exe.
- defender.exe.
- desktop.exe.
- dwm.exe.
- explorer.exe.
- jucheck.exe.
- jusched.exe.
- rundll32.exe.
- scvhost.exe.
- services.exe.
- svchost.exe.
- Taskmgr.exe.
- win-firewall.exe.

Malware Alina is known to scan and monitor the running processes on a system using the Windows API calls like CreateToolhelp32Snapshot() and Process32First() / Process32Next(). It also maintains a blacklist of processes which indicates the processes that are unlikely to have any information about the financial cards like system processes. For those processes which are not blacklisted, it takes the memory dump for them and uses techniques like regular expressions to find card track [88] information. To further optimize the content evaluation, only those portions of the memory pages are processed which have read/write attributes attached to it. Once the desired information, i.e., the financial records are found, the exfiltration process is initiated. The information shared back to the attacker from the infected system is encrypted via XOR key of "0xAB" and is then converted into HEX format. The communication with the command and control server is based on HTTP Post requests [89]. Some of the snippets from the HTTP communication by Alina and the decoded information is shown in Figure 5 to Figure 8 . Once, the

Command and Control (CnC) server receives the correct request, it responds back with a 666 status code. The basic spreading method for Alina malware is the use of weak passwords.

```
POST /wordpress/sam.php HTTP/1.1
Accept: text/*, application/octet-stream
Content-Type: application/x-www-form-urlencoded
User-Agent: Alina v4.0
Host: x.x.x.x
Content-Length: 767
Cache-Control: no-cache

act=l&b=bc095f64&c=TRUSTWAVE&v=v3.5&p=C:\desktop.exe&ldata=f0c2c5d8dfcac7c7c8c3cec8c0919a9a9c8b979b95f68befcec7ce
dfcecf8be891f7efc4c8dec6cec5dfd88bcac5cf8bf8cedfdfc2c5ccd8f7e1c4d8c3f7eadbdbc7c2c8cadfc2c4c58befcadfcaf7c1dec8c3c
ec8c085ced3ce8bcdd9c4c68bc4c7cf8bd8cedfdedb858bcfcec7cedfc2c5cc8bcadedfc4d8dfcad9df85a1f0c2c5d8dfcac7c7c8c3cec8c0
919a9c928b979b95f68be2c5d8dfcac7c7cecf8bdfc48be891f7efc4c8dec6cec5dfd88bcac5cf8bf8cedfdfc2c5ccd8f7e1c4d8c3f7eadbd
bc7c2c8cadfc2c4c58befcadfcaf7c1dec8c3cec8c085ced3ce878bd8dfcad9dfcecf8bc5cedc8bdbd9c4c8ced8d88bdcc2dfc38bcac7c2c5
ca96e891f7cfced8c0dfc4db85ced3ce
```

Figure 5: An example of Alina sending log data to the C&C server [89].

```
1.9.2p290 :001 > puts "f0c2c5d8dfcac7c7c8c3cec8c0919a9a9c8b979b95f68befcec7cedfcecf8be891f7efc4c8dec6cec5dfd88bcac
5cf8bf8cedfdfc2c5ccd8f7e1c4d8c3f7eadbdbc7c2c8cadfc2c4c58befcadfcaf7c1dec8c3cec8c085ced3ce8bcdd9c4c68bc4c7cf8bd8ced
fdedb858bcfcec7cedfc2c5cc8bcadedfc4d8dfcad9df85a1f0c2c5d8dfcac7c7c8c3cec8c0919a9c928b979b95f68be2c5d8dfcac7c7cecf8
bdfc48be891f7efc4c8dec6cec5dfd88bcac5cf8bf8cedfdfc2c5ccd8f7e1c4d8c3f7eadbdbc7c2c8cadfc2c4c58befcadfcaf7c1dec8c3cec
8c085ced3ce878bd8dfcad9dfcecf8bc5cedc8bdbd9c4c8ced8d88bdcc2dfc38bcac7c2c5ca96e891f7cfced8c0dfc4db85ced3ce".gsub(/(
..)/){ ($1.hex ^ 0xAB).chr }

[installcheck:117 <0>] Deleted C:\Documents and Settings\Josh\Application Data\jucheck.exe from old setup.
deleting autostart.
[installcheck:179 <0>] Installed to C:\Documents and Settings\Josh\Application Data\jucheck.exe, started new
process with alina=C:\desktop.exe
```

Figure 6: An example of decoded log data send by Alina to the C&C server [89].

```
POST /wordpress/sam.php HTTP/1.1
Accept: text/*, application/octet-stream
Content-Type: application/x-www-form-urlencoded
User-Agent: Alina v4.0
Host: x.x.x.x
Content-Length: 767
Cache-Control: no-cache

act=c&b=bc095f64&c=TRUSTWAVE&v=v3.5&p=C:\desktop.exe&cdata=e99e9b9b9b9392999e999e9899999e9b9cf5f1cad9cfc4c884edd9
cac5c0f59a999b939a9b9a9b9b9b9b9b9b9a92989b9a9b9b9b9b9b939c9c9b9b9b9b9b94909e9b9b9b9392999e999e9899999e9b9c969
a999b939a9b9a9a92989b9a9b939c9c94d7989f999a9c9a9c939f9c9e9d93999398969a9e9b9a9a9b9a9a92989b9a9b939c9c94d79e9b9b9b
9a929e929c9992999392929c969a999a9a9a9b9a9a92989b9a9b939c9c94d7989f999a929f9c9a999a9d939b9e9a92969a9e9b989a9b9a9a9
2989b9a9b939c9c94d79e989f99929a939c99999c9998989c9b969a989b9d9a9b9a9a92989b9a9b939c9c94d79e9999999d93939a929e9293
9f999b9d969a999a999a9b9a9a92989b9a9b939c9c94d79e9999999f989f939e93929f9b9e9f9d969a989b939a9b9a9a92989b9a9b939c9c9
4d7e99e9b9b9b9a929e929c9992999392929cf5f8dfcad9d8c8d9cecac684f9cadec7f59a999a9a9a9b9a9b9b9b9b9b9a92989b9a9b9b9b
9b9b9b939c9c9b9b9b9b9b9b94909e9b9b9b9a929e929c9992999392929c969a999a9a9a9b9a9a92989b9a9b939c9c94d7
```

Figure 7: An example of Alina sending card data to the C&C server [89].

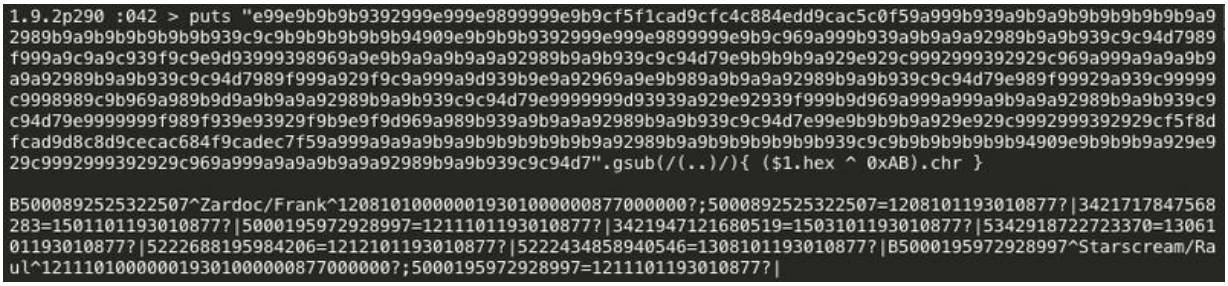


Figure 8: An example of decoded card data sent by Alina to the C&C server [89].

2.3.8 Zurgop

Zurgop is another infamous Trojan for which the major activity was reported during the summer of 2012. Later on, it was also exploited in other cyber threats and scams like Avatar rootkit. The highly modular Zurgop kit is available on underground forums. Some of the key features of this malware involves (i) ability to remain stealthy by using legitimate processes names, (ii) capability to steal credentials on a victim's computer, (iii) small file size, (iv) connection with the threat-master to control the infected node, (v) capability to download other files including malware, (vi) ability to detect testing environment and (vii) possibility to turn infected system to a proxy server to launch further attacks [90].

Like other malwares, the delivery mechanism includes infected email attachments, downloading of free software, and other social engineering techniques. Upon execution, it then installs itself while gaining administrative privileges without user consent. It copies itself to the %appdata% and %temp% directory. It also creates a shortcut to the actual malicious file under the Startup directory in addition to the registry entry which initiates the execution of Trojan after every boot. Basically, this piece of malware works by creating and executing a new thread with its code in all running processes. It also checks for the internet connectivity of the system by connecting to the msn server. The interesting characteristic of this malware is its ability to detect the virtual environment, which is an indication of a testing setup, hence, making it difficult to be detected by the sandboxing technique [91].

2.3.9 Hupigon

Hupigon is a family of malware categorized as backdoor. It enables the attacker to gain illicit control of the victim's machine and use it for malicious purposes. It is achieved by installing the malware as a service, which may establish a server that can be exploited for connecting to the targeted device. The package consist of multiple DLL files and a dropper which is copied under the system folder in Windows. The DLL files, some of which may be stealth, perform various functions including hosting a telnet server, recording activities with user's webcam, logging key strokes and stealing credentials. The stealth component of the package hides the files and processes related to the Hupigon by intercepting Windows API function calls. It can also inject its code as threads in others legitimate processes [92].

When the backdoor is installed, it copies itself with the name “Hacker.com.cn.exe” under Windows operating system folder and uses legitimate Windows executable names like calc.exe, cmd.exe, mspaint.exe, svchost.exe to make itself appear credible. In addition, it edits and add new registry key value entries and communicates with the malicious URLs [93] [94].

2.3.10 Carberp

Targeting the major Russian banks, Carberp family of malware was the first one to be designed specifically as a sophisticated banking Trojan and attacks the financial institutions. The first samples were observed back in 2009 [95] and is a forerunner of Zeus and SpyEye. It has the capability to infect both the 32 bit and 64 bit Windows operating system architecture and is spread through the social engineering techniques or web-pages containing exploit code.

The dropper comes in a visual basic pack and is sent to the target as a zip file as shown in Figure 9. Upon execution, the malware copies different files under Windows root and system directory. Further, it copies itself in the Windows Startup folder of the current user and add new registry entry to ensure its presence upon reboot. Moreover, it creates a new folder with a random name and a MicroST folder under Windows root and user profile respectively [96]. Once installed, the Trojan code is injected into a seemingly legitimate Windows OS process, i.e., ‘svchost.exe’. If the malware is under surveillance, one of the malicious components will trigger system crash to avoid detection. Another component is responsible of downloading the malicious payload while killing the processes and injecting it into memory to keep the infection in stealth mode [97].

Carberp Trojan is primarily designed to snip credentials and utilizes hooking technique in the Windows native API. It has command and control server communication components which aid the attacker connect to the target system to perform malicious activities. Further, the malware can download new or updated configuration files and receive commands from the threat master while compromising the system’s security [98]. It is capable of altering the current webpage being visited by the user by injecting a fake HTML code to steal dynamic one-time passwords from two-factor authentication tokens. In addition, the malware is designed in a way to remove previous infection on the targeted host; so, Carperb will have no contender on the victim’s computer. It has a highly modular structure and ability to operate in a stealth mode, which make it extremely difficult to be detected [99] [100].

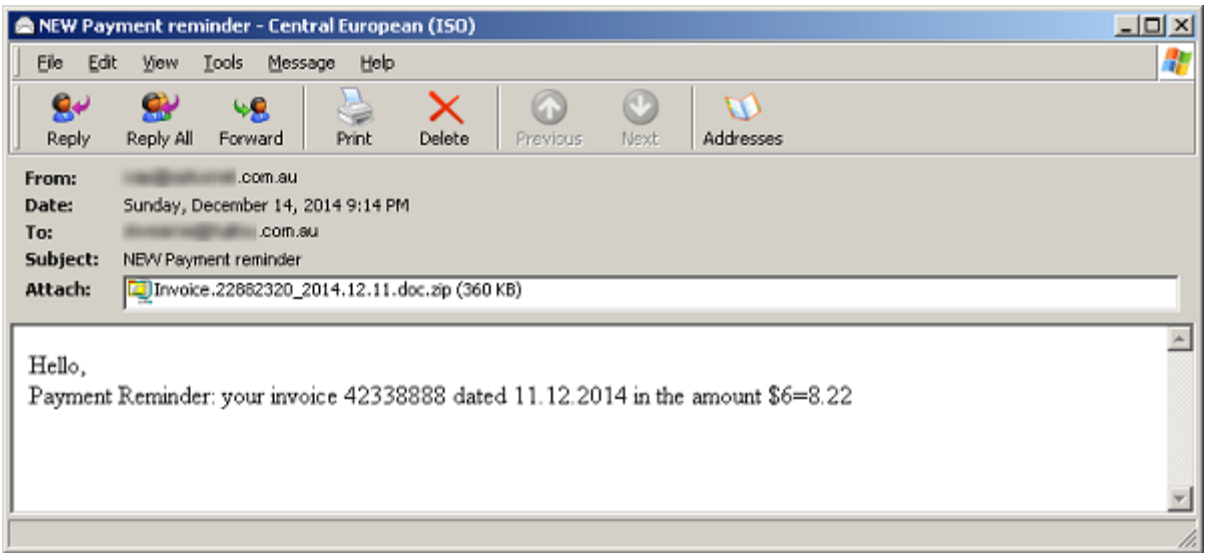


Figure 9: Carberp dropper attached in the email pretending to be a valid invoice [98].

2.4 Research Status in Malware Characterization

2.4.1 Malware Characterization Approaches

With the increasing sophistication in the malware obfuscation techniques, the characterization strategies are also evolving. There are a number of methodologies which have been proposed in the literature and are currently being used in the cutting-edge security products. However, they can be broadly classified into four main categories: signature based, heuristics based, anomaly based and semantic based malware characterization schemes. With the evolution of cognitive computing and cognitive informatics, semantic based analysis is also taking a significant position in the domain of malware characterization and detection.

2.4.1.1 Signature Based Approach

In the cyber realm, a signature refers to group of strings, functions, expressions or instructions that remains constant across the variations in the malware family, and therefore, serves as a finger print for catching any instance of that particular malware [101] [102]. The important characteristic of a signature is that it is unique, and hence, when employed in scenarios with simple malicious threats which do not morph or obfuscate themselves, the detection error is low [103]. The ease and simplicity in detection is the basic advantage of using signature based schemes for threat classification. Also, this strategy is effective for detecting malware which is already known, and hence, a corresponding fingerprint is available in the database to catch another similar sample [104]. Moreover, this places a requirement of continuous update of the signatures database, which needs human intervention to study, analyze and develop new patterns for every new malware that is encountered. Further, with the current extensive usage of advance morphing techniques by the malware writers, signature based malware detection is proving to be futile in terms of generating a lot of false negatives, as these days signatures are being updated in merely few seconds [105]. In addition, behavior is a special type of signature which remains consistently similar with the evolution of the malware variants. This distinct feature has rendered it a strong place in mutating malware detection approaches as their behavior is preserved irrespective of the syntactical or structural changes.

2.4.1.2 Heuristic Based Approach

Heuristics based threat detection methodology is often employed to detect new malware and the variants of the existing ones. There are two different methods for heuristics based analysis of a suspicious program. The first one is considered to be a static approach and the other is a dynamic one and are named as follows [106] [107]:

1. Rule based malware detection.
2. Sandboxing.

In the first approach, the malicious executable is disassembled and the resultant source code is analyzed to find a close match with a pre-known malware pattern. When the similarity between the suspected code and the known pattern reaches or exceeds a pre-defined threshold, the file under observation is marked as a threat. The set of patterns which play a key role in determining a malicious file consists of a group of instructions which pose serious threat to a system upon execution and may render it unusable [108].

The dynamic scheme, often known as sandboxing, is based on emulating a piece of malicious code under specially created testing environment which is similar to the target platform of the security threat under observation [186]. These malicious codes are executed in a highly controlled virtual environment to observe and analyze their behavior upon execution, while ensuring that they do not infiltrate other systems. Some of the suspicious behavior involve altering the system files, changing the registry, remaining stealth in a process tree, downloading infected files, and communicating with a command and control server. If the file is found to be performing these malicious activities, it is flagged as malware [109].

Although effective, heuristics analysis is quite resource intensive, which is, in addition to its high dependence on the rule engine to flag a file as malicious or clean, and is vulnerable to false positives. Moreover, there are highly intelligent malware variants in the cyber-world which are able to detect the virtual emulation environments like sandbox, and therefore modify their behavior to appear benign under surveillance, hence, making this detection technique incapable of detecting them [110] [111].

2.4.1.3 Anomaly Based Approach

Anomaly based malware detection is an experiential learning approach towards finding malicious behaviors and is based on determining the patterns which deviate from the normal characteristics. The key advantage is that it does not require creation and maintenance of signature database and is as well effective for the detection of unknown malware, commonly known as zero-day threats. However, the fundamental limitations of this approach can be attributed to high false alarm rates and the implementation complexity which involves determining the most suitable set of features that are needed to train the learning algorithm [112].

It comprises of two distinct phases, the first is called the training phase and the second one is called the testing or the detection phase. In the training phase, the decision making engine learns to differentiate between the anomalous and the normal classes of data using the pre-obtained test dataset. While in the later phase, it provides decision based on this learning for unseen data [113]. The data used in the initial learning phase may be a mixture of anomalous and normal samples, anomalous samples completely, or normal samples completely.

2.4.1.4 Semantics Based Approach

Semantic analysis is the domain of knowledge science which deals with the study of the meaning and inferences of structures under observation. In the domain of linguistics, semantic analysis is used to elaborate the meanings and inferences of words and statements using patterns

and contextual analysis. It can be thought of as a mental cognitive process that requires knowledge and intelligence to recognize common and unique patterns to comprehend the intent of the writer [114]. In the domain of malware analysis and characterization, semantic analysis is used to analyze, benchmark and determine the intent, techniques and motivations of malware for detection and subsequent protection purpose. Malware analysis literature provides varying definitions of malware semantics such as extracting patterns from the signature/code/syntax [115] [116] [117] of a malware program to the behavioral and heuristic analysis of malware objects [46] [47]. However, semantics is a wide field of study in other domains and therefore, a general model of malware semantic analysis is not available and is an open area of research. Mostly, in cyber security, semantic analysis requires cognitive and contextual knowledge to comprehend the meaning of a particular object under study [118] [119] [120]. For example, a malware program activity can be detected based on certain steps that it takes to execute its malicious objectives e.g. a decryptor is loaded into the memory which will subsequently decrypt the malware file. This malware file will then spawn various modules in the memory to start executing its malicious purpose. The semantics of this malware can be abstracted from temporal utilization of memory where decryptor loading will increase memory size for a small amount of time and then the spawning of modules will consume certain locations of the memory. Knowing this behavior can provide knowledge of the malware activity using memory footprints. However, this activity can be performed by legitimate programs as well, for example, a VPN tunnel using multi factor authentication can download a normal file from the tunnel communication that can cause the same changes as mentioned in the previous example. This example demonstrates the challenge of uniquely characterizing malware using memory footprints which are similar for both malicious and legitimate functions. It is important to note that semantic characterization is different from signature based, heuristic based or anomaly based analysis systems [121] [122]. Semantic based methods utilize reasoning and the inferences. Signature based systems only search for the actual known signatures while heuristic based analysis search for rules. Signatures or rules are not semantic or behavior but provide a syntactic knowledge of the object under observation. Further, these methods do not provide a behavioral or dynamical detection approach. Similarly, anomaly based detection systems search for pre-defined behavioral patterns or knowledge. It is observed that semantic based systems may intersect anomaly based detection systems in the sense of searching pre-defined behaviors. However, the concept of reasoning and inference is missing from anomaly based detection systems. In the era of advanced and mutating malware, reasoning is important to ensure accurate characterization and is largely dependent on the selection of features and their analysis, while anomaly based detection systems lacks reasoning [123] [124] [113]. Further, anomaly can be true or false due to lack in reasoning, while true semantic analysis will reinforce true characterization and discourages false classification. Having contextual knowledge through semantic analysis helps in categorizing a threat which is broader in scope than finding a variant of malware. This contextual knowledge provides information of the intent, motivation, tools, techniques and procedures of a source of threat that can characterize multiple variants of the same malware family [125]. In this work, semantic of malware is referred to the dynamic behavior of malware object inside an operating system process tree and observed through the extraction of the graph theoretical features which are analyzed to infer the activity behavior in time domain. Also, the cognitive complexity of the feature set is measured to quantify the feature based behavior

for discriminatory analysis using fractal based non integer dimensions (through simultaneous analysis of local and global scales) which reveals inherent and hidden patterns showing long range correlation and self-affinity in the observed object. This way, an inference about relationship can be quantified uniquely that subsequently helps in characterization significantly.

2.4.2 Recent Research Status in Mutating Malware Characterization

Characterization of mutated malware is an active area of research in cyber-security. The available literature suggests that the characterizing methodologies can be broadly categorized as syntactic or semantic analysis of the polymorphic and metamorphic malware. .

One of the most widely used detection techniques is through signature/syntactical analysis of the mutating malware. The identifying signatures may consist of a byte-sequence, a regular expression (RegEx) or a particular program flow (heuristic) as detected in a sandbox. Since, polymorphic malware varies in terms of coding structure with each instance, using the heuristic signature is being explored currently by the research community for detecting these threats, as signatures remain unchanged. For instance, the authors in [126] have proposed a polymorphic malware identification technique based on the dropped files, which upon successive executions, if creates a distinct child process at every instance, then it is marked as a polymorphic sample. Another interesting methodology to combine static and dynamic analysis approaches for the classification of malicious and benign polymorphic samples is proposed by James and Marco [127]. The discussed methodology involves topological evaluation of file characteristics and runtime relationship using belief propagation. In a dataset of about 4000 files, the researchers report a true positive rate of 99% and a false positive rate of less than 1%.

In order to hunt the polymorphism in a malware file, it is imperative to understand that no matter how distinguished the variant appears, the underlying algorithm will always remain the same. This notion has been explored by Alcatel-Lucent researchers in [128] where they discuss the mapping of the malware's algorithmic code to a context-free grammar which is then normalized. Then, a similarity comparison between the grammatical structures indicate the presence of mutation in the code. Further, reconstruction of state machine model is another technique employed in the research for the detection of polymorphic malware. Researchers in [129] have presented a framework based on Hierarchical Hidden Markov Model (HHMM) for detecting polymorphic malware which have a self-similar structure in their signature sequences. About 15,000 samples of the malware, each having different size, were used to reconstruct state machine models using HHMM. This hierarchical approach was able to infer correlated information in the mutated instances of the malware samples, which differ greatly in their size and hence, produce distinct signature sequences. Moreover, Hidden Markov Model (HMM) in its crude form has been applied to identify malware instances; however, the metamorphic malware instances which completely transformed themselves could not be easily determined using HMM. Therefore, a strategy to extract only the important sequences of malware software op-code to train the HMM have been explored in [130].

These particular sequences are selected based on their mismatch with the normal executable files. The authors claim that promising results were obtained with this improvement in the basic model.

Another form of signatures employed in the polymorphic malware characterization is based on the control flow graph generation. As suggested in the study [131], isomorphism between flow graphs of different malware can be used as a key to determine the mutation in the malware sample. The authors proposed using heuristic based matching algorithms to find the similarity between generated flow graph of the sample under consideration and the pre-populated flow graphs of the known malware. The prototype system was able to correctly identify large number of malware samples with low false positive rate. Another publication [132] by the same authors elaborates the use of minimum matching as a distance metric to find similarity between two Control Flow Graphs. The research study claims to propose novel feature vectors, i.e., k-subgraphs and q-gram strings of decompiled source code, which were used in the variant detection setup. It is reported that low false positives were observed during the experiment.

To cater for the unique characterization of polymorphic variants, automation of the signature generation mechanisms have been investigated by the researchers lately. The experiment in [133] proposed the use of Principal Component Analysis (PCA) method to collect substrings that appear repeatedly in a malware file and assign them to each known malware instance to be used as signatures. Further, the automated signatures as described in [134], based on the usage of position-aware byte frequency distribution, have been reported to be more accurate in detecting polymorphic variants of the worm. The research study utilizes Expectation Maximization (EM) and Gibbs sampling algorithms to compute these distributions. Also, authors in [135] elaborates the semi-automatic signature extraction mechanism based on the context-free grammar. The proposed scheme performs a static analysis of the malware binary code and involves a little manual information collection step. A similar tree based approach to automatically generate and store the polymorphic worm signatures, such that it reflects the familial characteristics of the variants, is presented in [136]. The authors argue in favor of using the tree structure named as PolyTree to cluster worm signatures, since it represents the connection between different variants of the same worm. This PolyTree consists of two main blocks, the generator and the selector. The tree generator is an algorithm to collect and update not only the signatures but their positions in the tree as well. Further, the selector matches the signatures with the pre-available worm fingerprints in the tree and also searches the pre-collected benign samples to find a close match. This approach is innovative in the sense that it captures the evolutionary aspect of the mutation in the malware. Also, a buffer overflow vulnerability based signature generator, called LESG, has been proposed in [137]. The created signatures have been reported to be attack resilient and were additionally tested under noisy environment.

An interesting approach for polymorphic malware classification is available in [138] which is based on a concept similar to the one applied for gene sequence classification. The basic difference is that the gene classification tools are optimized for structured nucleic acids, which are represented by four letters only. On the other hand, the proposed methodology can deal with unstructured data like malware source or machine code. The selected classifier is called "Strand gene sequence classifier" and the experiment were performed on about 500GB of malicious data obtained from Kaggle Microsoft Malware Classification Challenge [139]. There were 9 different classes of

polymorphic malware and using the suggested strategy authors were able to achieve an accuracy of approximately 95%. Moreover, a method primarily employed for Protein and DNA matching has been utilized to detect highly obfuscated metamorphic malware, as discussed in [140]. It is assumed that the difference in the malware software op-code sequences is the mutation point of the malware variant. Therefore, a sequence alignment method is used to construct three distinct signatures for each family which are termed as (i) single, (ii) group, and (iii) probabilistic signatures. The presented results in the paper indicate that for the single signature, the detection rate is about 91%; however, the false positive rate is relatively high. On the other hand, the group signatures which employ wildcard characters yield a lower false positive rate but the detection rate is 72 % approximately. For probabilistic signatures, multiple length mnemonics were collected and the same experiment was repeated. A detection rate of about 71% is reported for this category of fingerprints with the length of 200 which is reported to be considered optimum by the authors.

Research literature on behavioral signature classification is another approach that utilizes code behavior rather code syntax to detect malware and is proved to be better than syntactical detection approach in not only finding a single malware but a group of malware originated from same family of mutated malware. Behavioral detection approach uses characterization of malware code behavior in distinct identifier and can be applied equally to the polymorphic and metamorphic variants of a malware with increased robustness and reliability. The authors [141] have proposed a signature unifying concept for the entire family of a malware instead of creating individual fingerprints of each variant. The investigation in the paper involves selection of malware's behavioral properties and the selection of those patterns which are the most significant and provides better discrimination power. These patterns can be used in a proposed equation which will work as a signature. The idea was initially tested on the VCL family of malware and then later was extended to include 30 other families. It has been claimed that this methodology will aid in reducing database size and increase query speed. Moreover, authors in [142] suggest constructing a sequence consisting of malware behavior to form a cluster that will help in generating behavioral signatures. The method is named as "MalHunter" and works on the principle of grouping similar behavior patterns and aligning the resultant clusters. The paper claims that this technique is robust in the sense that it stores single signature instead of multiple signatures for a single family of malware. Further, a cognition based framework using behavioral characteristics of polymorphic malware has been proposed by University of Manitoba researchers in [14]. The proof of concept is presented using the process tree information available in a Windows 7 host operating system. Fractal analysis of the data stored in the directed graph format is used to detect the presence of malicious operating system processes in the system and presented discriminatory method to detect malware activities.

Graph based techniques are popular when dealing with the metamorphic malware characterization as they reflect the intricate resemblance between the malware family members. To capitalize this idea, an op-code based similarity between the graphs of metamorphic malware variants has been proposed by Reza et al. [143]. The uniqueness of the proposed technique is attributed towards the use of Linear Discriminant Analysis (LDA) to determine discriminatory malware indicators which in this case are distinct edges that can linearly separate two classes while the rest of the redundant edges are removed. The proposed methodology has been tested on Next

Generation Virus Construction Kit (NGVCK) and Metamorphic WORm (MWOR) kit with reportedly low false alarm rates. A similar API call flow graph (CFG) based approach has been discussed in [144] which utilizes a feature selection algorithm to determine the most significant indicators in a call graph. Also, WEKA tool is used for the classification purpose and the assignment to a particular family is performed using the histogram and chi-square distribution analysis.

The static evaluation and analysis of the malware software executable files in the host operating system has been widely exploited for the classification of mutating malware. However, it has proved to be futile in the face of the obfuscation techniques used by the malware writers. Therefore, automation of these analysis has been researched by the cyber-security community. As discussed in [145], based on the system and operating system's library function call pattern, the semantic analysis of the malicious executable is carried out. The concept was tested for the benign and malignant instances of software programs and the most significant finding was that it was possible to determine the code re-use in an executable which is often an indicator of morphism in the code. This is in addition to the correct identification of some of the common metamorphic malware families and the ability to detect unrelated software code. It is of paramount importance to understand that the obfuscation process for the generation of a malware variant mostly preserves flags and constants in the code. This scheme is utilized in [146] where authors were able to classify possible samples to a metamorphic family and high detection rates have been reported in the experiment.

Researchers also exploited feature engineering for text categorization to reliably detect the mutated variants of a family. Different schemes like Categorical Proportional Difference (CPD), Odds Ratio (OR), Galavotti-Sebastiani-Simi Coefficient (GSS), Linear Discriminant Analysis (LDA), and Weight of Evidence of Text (WET) are used to identify the most appropriate bi-gram features from the executable files as discussed in [147], [148] and [149]. The resultant selection of features are then analyzed to determine their presence in the normal or anomalous class of malware software executable files. Synthetic and real world test samples used by the research group provided better results on selected data sets.

An alternate to the analysis of actual structure or behavior of the obfuscated malware is to evaluate the malicious executable file directly on a byte level. A simple technique for this purpose is to use compression based classifications schemes which have been successfully evaluated earlier for the text mining tasks. Authors in [150] proposes two compression techniques i.e. Approximate Minimum Description Length (AMDL) and Best-Compression Neighbor (BCN) for determining malicious programs. Their experiments reveal that the AMDL technique performed poorly and worked just like a random guess whereas BCN was able to detect malignant code with an accuracy of approximately 67%. Also, measurement of structural entropy of a file can be used as a key concept to detect the presence of morphed malware. A study by Jared Lee et al. [151] investigated the resemblance between the executable files by first segmenting them and then using compression ratios to compute different scores between file pairs to determine the variants in a malware family.

A heuristics approach based on the statistics of the assembly code e.g. instruction count has been presented in [152] which proved to be much faster than the contemporary techniques.

Promising results have been reported by the authors in the experiment. Also, other statistical measures like probability of a string occurrence, probability of a character to be located at a specific position, and the similarity between the malware variants has been used to train the hidden Markov model based detection system [153]. The presented results indicate that the suggested methodology is more effective in determining the obfuscated executable files even when they are encrypted compare to the traditional antivirus software like Avast, Symantec, Microsoft Security Essential, and AVG Internet Security.

To identify the thwarting behavior of the malicious executable files, a scheme based on the artificial immune system (AIS) has been suggested in [154]. The multilayer defense mechanism of an immune system comprises of skin, skeleton and B-Cells. Therefore, the proposed replica of this immune system for detecting mutated malware has three layers. The first is the skin layer where the hash value of the executable file is compared to the hash values of the benign files. Then at the skeleton level, the flow graphs are generated and the corresponding matrices are then compared using metrics like Euclidean distance, hidden Markov model, n-gram, and neural network. At the B-cell step, the encoding of the file is checked to verify the malicious or normal nature of the code. The results were obtained by testing the viruses generated from NGVK and VCL32 kits and a detection rate of 86 % was achieved.

An interesting metamorphic malware identification framework is proposed in [155] where the authors consider that the detection of metamorphic malware is a NP-Complete problem. The proposed system is termed as MARD (Metamorphic malware Analysis and Real-time Detection) and inspect the binary executable files using an intermediate language called MAIL (Malware Analysis Intermediate Language) for distinct patterns which are then converted to the control flow graphs. These control flow graphs are further divided based on their functions and are then searched into the potential malicious files to verify the presence of a malicious code. This system is parallelized for efficiency and is able to produce detection rate of about 99% with a very low false positive rate of 4%. The uniqueness of this framework comes from the fact that it supports both the Windows and Linux operating system binaries.

Semantic analysis to characterize and detect cyber threats is a new and emerging field which is gaining traction in the cyber research community due to its discriminating dynamic analysis of threat actions, tools and techniques with improved performance. It combines various individual aspects of security to infer meanings [156] e.g. situational awareness, logs and risks. Mostly, semantic analysis refers to the aggregation of data from various sources to add situational awareness and dynamic quantification of the behavior such that the legitimate and malicious objects are differentiated uniquely. Authors in [157] describes a Natural Language Processing (NLP) based ontological framework to scan email text to extract indicators of attacks using the grammatical structure and cross association of the lexical meanings of words. A new method of extracting patterns from the email subject lines to classify user groups/departments is proposed in [158]. Another research in [156] proposed an ontological framework to integrate various sources of data so that the sparse knowledge of the threat can be aggregated and a body of threat based knowledge can be developed. This paper provides an overarching framework to reason relationships of the threats based on the type of exploits they use, vulnerabilities and weaknesses, and what might indicate a compromise. Through an example of web attack, authors have modeled

and characterized the attack from both the attacker and the target victim ends and considered all the entities involved. Concept of categorization is used to express relationships to enable proper reasoning of the cyber exploits. Research literature [159] [160] [161] also points to analyze user actions on a host operating system to detect cyber threats. This analysis uses knowledge of the complex sequence of user actions to define semantic patterns to infer user intent to differentiate threat actions. A recent paper [162] proposed a semantic based situational awareness mechanism for Internet of Things (IoT) which uses semantic ontology and user defined rules to provide the context, attack, vulnerability and network flow information for a heterogeneous data network of IoT to provide an early warning cyber security mechanism.

In this thesis, malware behavior is analyzed using a set of features from the dynamic process tree data temporally. This behavioral analysis provides semantic meanings using multiscale fractal analysis of each feature set which fuses information from local (finer) and global (coarser) scales to indicate a strong discriminatory difference between the malware sample and the normal sample and thus provides a unique way to characterize threat hidden inside an operating system process tree. Further, the selection of features is driven by the contextual meanings of the dynamics of process tree which is then transformed and quantified into a fractal dimension based coefficient.

2.4.3 Recent Research in Malware Sandbox

To better understand the behaviour and impact of malware, one method is to let it run in a controlled environment, in which the targeted operating system is replicated. This helps in evaluating not only the static code similarities but its dynamic behavior to compare and classify it into a corresponding malware family. It is important to note that a true static analysis will also reveal the expected behavior based on the code assessment. Therefore, a good sandboxing approach will consider the integration of both static and dynamic analysis techniques.

Irrespective of the underlying technique, i.e., static or dynamic, sandboxing is an extremely resource intensive approach for evaluating network packets. Hence, it is suggested in [107] to use sandboxing for host based threats and also provides a layered design approach by stacking together different methodologies based on the increasing order of computational intensity. The core concept is to first analyze the file with a method which is the quickest and least resource intensive. If the file is identified as malicious on a particular stage then it is blocked and not fed to the next stage for further processing. Also, it is then removed from the analytical flow; therefore, only those threats which are extremely obfuscated are analyzed by the sophisticated techniques, which are more resource and time intensive. The report mentions four different levels, the first of which is the fastest and most common threat detection technique, i.e., signature based analysis. The second phase involves using heuristics and emulation phenomenon to detect more obscure attacks. This is then succeeded by dynamic analysis in a virtual environment. The final phase includes the processing of source code of the file after its decryption and unpacking. It aims at deciphering the behavior of the file based on the used instruction set.

Limon [163] is another interesting Python programming based Sandbox, which aims to capture Linux based threats. It captures the runtime information of the malware based on the static,

dynamic and memory analysis of the suspicious file in a virtual environment. It supports analysis of a number of different files using open source tools like Tcpdump [164], Yara [165], volatility memory forensics framework [166] and VirusTotal public API [167]. After execution, it keeps the logs, screenshots, packet capture data, and memory image associated with the malware under scrutiny. Thus, it provides an option to analyze the malware before, during and after execution, which aids in developing and understanding the expected behavior in a bigger picture.

Further, the Cuckoo sandbox based experiment was conducted by authors in [168], where they have implemented a distributed firewall in Linux using 'iptables' and 'ipsec' and named it ***Distfw***. This firewall was integrated with Cuckoo sandbox for the analysis of malicious URL samples automatically. Also, manual analysis of the same samples were performed to obtain their behavioral information. The automatic and manual analysis reports were compared and it was discovered that both methods of evaluation revealed the same information; however, the sandbox methodology was found to be much faster. Moreover, researchers in [169] have also utilized system call report generated by Cuckoo sandbox, which is in the form of n-gram, to find the best fit classifier. It is reported that the information gain was used as a feature selection methodology and a number of classifiers were used from the WEKA tool. The results indicated that the stochastic variant of the Pegasos (Primal estimated sub-Gradient solver for SVM) performed the best in terms of higher true positive rate and lower false positive rate.

A similar machine learning approach has been utilized in [170] where authors have used an online dynamic analysis tool called Anubis [171]. This tool provides detailed report upon submission of a suspicious executable, which is then processed into sparse vector model to be used by the machine learning classifier. As reported in [170] different learning algorithms including Naïve Bayes, k-Nearest Neighbors, Support Vector Machines, decision tree and multilayer perceptron neural network were utilized and their results were compared, which revealed that J48 decision tree performed the best in terms of low false positive rate, high recall, accuracy and precision.

The Cuckoo sandbox has also been used in the evaluation and analysis of the deadly ransomware recently. As elaborated in [172], an experiment was conducted to generate logs with and without the presence of malware in a sandbox. For this purpose, two polymorphic malware samples were used in addition to the famous ransomware WannaCry. Using the Term-Frequency Inverse Document Frequency (TF-IDF) method, relevant features were extracted from both types of the event logs, i.e., with and without malicious activity. A manual analysis of the malware was performed to compare and validate the accuracy of the feature extraction algorithm from logs. The paper claims that the resultant patterns produced by the proposed algorithm was effective in detecting other morphed samples of the WannaCry ransomware, which successfully evaded 63 antivirus products.

Further, Peter and Barry [173] have proposed a sandbox for the detection of PHP based Trojans, often known as web shells. These are often exploited by the attackers to gain backdoor access of the victim's system. Therefore, an automated approach of evaluation was needed for the analysis of these shells. The basic framework consists of a decoder and Ubuntu based virtual environment which served as the sandbox. Decoder performs the preliminary tasks of de-obfuscation and

normalization of the code before it is executed in a controlled environment which logs the function calls of the malware. It is reported that the proposed system requires some improvement before it can be taken into production, however, it served pretty well from the proof of concept point of view.

One of the earlier Windows based sandboxes was developed by Ulrich et al. and was named as ***TTAnalyze*** [174]. It has the capability to dynamically analyze behavior of the Windows executables using hooking and branching technique. The generated logs include recording Windows native system calls and Windows API function calls. The QEMU [175] emulator handles the binary in such a way that it does not alter the execution of malicious samples, thus, making it a suitable choice for scanning a Windows executable for threats. A comparable approach was ***CWSandbox*** [176] designed by University of Mannheim researchers for the automated evaluation of Win32 executable files by hooking in the native system and API calls. It records the behavior of an executable in terms of network communication, operating system calls, and file system and registry modification.

In addition, an isolated dynamic simulation approach was experimented for malware behavior detection and called the ***Norman Sandbox*** [177]. It basically executes the binary in a virtual environment based on Windows operating system with network connections and generates a log file containing information regarding file changes, registry modifications, system alterations, network details and operating system information. . However, the basic drawback is that this system do not permit the malware executable to interact with the system processes which resulted in loss of critical information for analysis.

Panorama [178] was another QEMU emulator based sandbox which was built on the key feature of information access and processing by the applications that defines the malicious nature of an executable. Both the network and hardware resources were monitored for capturing this behavior which include both the data and address related changes. The analysis further involved creation of the process and module graphs which were related to the tainted data. Even, this was able to capture that certain non-malicious applications like Google Desktop was accessing and sharing sensitive information in certain configuration which is as well undesirable for end-user.

A parallel computing based distributed version of the Cuckoo sandbox was used by the authors in the experiment as discussed in [179]. About 80,000 malware samples were collected from VirusShare Website and their corresponding reports were generated. A combination of static and dynamic malware analysis techniques were employed such that if a sample is classified as belonging to the class of pre-known malware instances, only pattern matching based static heuristic analysis is performed. However, for the new unknown malware samples, dynamic analysis in a virtual environment which involved multiple Windows guests on a single control unit is carried out. Moreover, to ensure security during the execution phase, instead of taking the system online, an internet emulator called InetSim was used to provide responses for the request generated by the malware. The extracted data is stored in the form of malware actions and is used to build a random forest classifier. The proposed classifier performed well in terms of having an average weighted area under curve value of about 0.98.

An important aspect of malware evaluation using sandbox is the execution timing of the file which should be sufficient enough to capture the malicious behavior. Delayed malware execution is one of the most commonly employed techniques by the malware designer to evade detection. A research study [180] was carried out using Cuckoo sandbox to predict the minimum timing required to unveil the malignant intent of the executable files. To do so, a combination of static analysis of the suspicious files and a dynamic analysis in a controlled environment was performed. This timing information is then fed to a machine learning classifier to predict a model for requisite runtime. The result indicate a success of 90% in correct determination of runtime. In addition, a malware family classifier was also build and an accuracy of 92% was reported.

Although, sandboxing technique is generally much more reliable and robust in detecting obfuscated threats, but, newer more advanced malware are able to detect the presence of surveillance and can morph their behavior. Therefore, the sandbox developers have come up with different solutions to stop malware evasion by removing information which can reveal virtual environment. Also, some of them have completely abandoned the idea of emulation and virtualization and use bare-metal hosts to perform the experiments and analyze malicious behavior. However, the authors in [181] have argued that ”wear and tear” of the real computing machine is a feature that can be exploited by the malware to distinguish experimental and real environment from each other no matter if the sandbox utilize a bear-borne machine. To prove their point, a simple decision tree based analysis was performed on a very large dataset collected from computing machine users and malware analysis tools. The experiment revealed that the malware can differentiate between a real and artificial environment with an accuracy of 92.86%. Further, system’s usage and other parameters were modeled statistically in this experiment to help create operating system images which mimic a real environment to avoid malware evasion.

A different but effective approach of posing experimental setups as the real system to an intelligent malware is presented in [182] where the authors have integrated the concept of software defined networking (SDN) with a regular sandbox mechanism and named it ***MARS*** (MAl-waRe Analysis Architecture based on SDN). It is known that the advanced malware are aware of their environment and can therefore, evade the detection in such scenarios by behaving as benign software. This research proposed a malware analysis architecture that continuously reconfigures the networking environment as a trigger for malware to start behaving in a malicious manner. It has been claimed that this strategy can reveal distinct behaviors of the malware which are triggered under special network profiles only and thus, provides a way to capture unknown threats which otherwise may remain dormant.

Further, ***Ether*** [183] was one of the first papers to propose hardware virtualization as a solution for the vulnerability aspect of the advanced malware systems which emulate the target operating system that can be easily exploited by the malware to detect the presence of scrutiny. The virtualization was implemented in XEN hypervisor and the system logged the details about the function calls, debug related exception and in special cases CPU flags.

With the omnipresence of mobile devices in our daily lives and our growing dependence on them, it has become imperative to protect them from advanced malware threats. Most of these devices are Android based which is a strip-down version of Linux operating system. Research

efforts are being directed to introduce techniques that can automatically scan and classify android applications as safe or malicious before they hit the end user. One such methodology is to use sandbox which can combine the static and dynamic threat evaluation of these applications as elaborated in [184]. This research study proposes an Android Application Sandbox (***AASandbox***) that performs the static analysis based on pattern matching to detect the presence of suspicious activity. On the other hand, a dynamic evaluation which installs the application in an isolated virtual environment and records the behavioral activity of the application is also carried out. The paper further claims that this technique can be deployed on a cloud where mobile applications can be scanned in store (like Google's Android market) before they are downloaded. AASandbox can be integrated with the state-of-the-art mobile antivirus packages to improve their efficiency and robustness in terms of detecting mobile malware. ***DynaLog*** [185] is another Android based framework for the detection of malicious applications by dynamic evaluation of their behavior. It captures the high level behavior by considering the records of API calls and critical events that are extracted through open-source tools. The proposed system was validated with benign and malicious Android applications and promising results have been reported, which is in addition to its inherent extendible design due to the utilization of open source resources.

With the increase in cyber-security related awareness, public malware analysis systems are growing popular. Users submit the suspicious files to these setups which execute these samples in a controlled environment and provide an analysis report back to the user. However, it is important to understand that these systems are connected to the Internet and can be abused by the malware-creators as well. This poses a risk in the analysis of these file as the threat creators can get a trigger when the malware tries to communicate with the command and control server. As a result, an attacker can disturb the evaluation of such samples. As discussed by the authors in [186] an IP address is one such parameter which can be easily exploited by the malware designer who can submit a decoyed sample to obtain the IP address of the sandbox machine. This address once discovered can be shared in the malware developer community where it can be further blacklisted and can be used to program malware to obscure its malicious behave on such machine. Most of the public sandboxes are vulnerable to these Decoy Sample Injection (DSI) attack as termed by the researchers. The experiment was performed on nine such systems and six of them were found to be susceptible. Moreover, it was discovered that some of the background activities performed on these systems during the analysis phase was also revealed under DSI attacks. One of the proposed solutions is the acquisition of dynamic IP as discussed in the paper.

Also, Fernando et. al. [187] have proposed an automaton model for the detection of obfuscated malware based on the improvement in current sandboxing mechanism The approach is termed as ***Segmented Sandboxing*** which has reduced the problem of determining semantic equivalence of two binaries to the comparison of system's states after the controlled execution of malware samples. The results reported in the research study indicated very high detection rate and lower false alarm rate.

A comparative analysis of significant sandbox tools available in the industrial market is provided in Figure 10. As evident, all these tools provide dynamic behavior analysis of the capture payload [188] [189] [190] [191] [192] [163] [193] [194] [195] [196] [197] [198] [199] [200] [201] [202] [203].

	Cuckoo	ThreatAnalyzer	Joe Sandbox Ultimate	Limon	Forcepoint Advanced Malware Detection (AMD)	FortiSandbox	VxStream Sandbox	Fireye AX Series Malware Analysis	Lastline Analyst	Symantec Malware Analysis	SecondWrite Sandbox	True Bare Metal Cloud Sandbox
Former Name	N/A	CWSandBox, GFI SandBox	N/A	N/A	N/A	N/A	N/A	N/A	Anubis	Bluecoat Malware Analysis	N/A	N/A
Open Source	Yes	No	No	Yes	No	No	No	No	No	No	No	No
Vendor	N/A	ThreatTrack	Joe Security	N/A	Forcepoint	Fortinet	Payload Security	Fireeye	Lastline	Symantec	SecondWrite	Binary Guard
Supported OS for Analysis	Windows, OS X, Linux, Android	Windows, Linux	Windows, OS X, Android	Linux		Windows, OS X, Android	Ubuntu, Windows	Windows, OS X		Windows	Windows	Windows
Virtualization Support	Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes (cloud based)	Yes		Yes (cloud based)
Web Interface	Yes	Yes	Yes	No	Yes	Yes		Yes	Yes	Yes	Yes	Yes
Dynamic Behavior Analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Memory Analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes
Network Inspection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
URL Parsing/Analysis Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Archives Analysis	Yes	Yes		No	Yes	Yes	Yes	Yes		Yes	Yes	Yes
Supported File Types	PE, Office files, PDF,VBS, JS, PHP, CPL, DLL	Multiple Files	Office Files, PE	ELF	PE, Office files, PDF	PE, Office files, PDF,VBS, JS, PHP, CPL, DLL	PE, Office files, PDF, VBS, JS, PS1, HTA, ELF, Bash, Python, Perl	PE, Office files, PDF,DLL	PE, Office Files PDF, JS, Flash	PE, DLL, Office files, PDF, Java, MSI, RTF	PE, Office files, PDF, HTML, DLL, .NET, JS	PE, Office files, PDF,VBE, JS, HTML, Media Files
Yara Rule Support	Yes	No (Custom Inbuild Rules)	Yes	Yes		Yes	Yes	Yes	No	Yes	Yes	
Download/Display Report	Yes	Yes	Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Third Party Integration	Maltego, Security Onion, Bro	Threat Secure, RESTful API, VirusTotal	VirusTotal, Metadefender, TheHive, Fame, MISP, CRITs, Phantom, Demisto, Viper, Malsub	VirusTotal	Forcepoint Websecurity, Forcepoint Email Security, Forcepoint Next Generation Firewall (NGFW)	FortiGate, FortiMail, FortiWeb, FortiClient, CarbonBlack, Ziften	VirusTotal, Metadefender,Suricata, Whitelists(NSRL, Kaspersky)	Fireeye DTI, Fireeye CM	Carbon Black, Opentext, Tanium, Tripwire, Barracuda, Symantec, Cofense	Symantec Content Analysis, Symantec Mail Threat Defense or Symantec Security Analytics	Available via API	
Android Files Support	Yes	No	Yes	No	No	No	No	No	Yes	Yes	No	No
Downlaod Pcap	Yes	Yes	Yes	Yes		Yes	Yes		Yes		Yes	Yes

Figure 10: A comparative analysis of available sandbox tools.

In this dissertation, a Windows operating system based sandbox [1] is presented which acquires detailed temporal data of the operating system process tree. Process tree of an operating system is a fundamental monitoring tool that contains information of the legitimate and malware processes at any given instance of time. A process tree can be considered as a state of the operating system at a given time instance and varies dynamically based on the execution of each executable file in the memory. Any executable file that requires computing resources must attach itself to the operating system process tree and therefore, it is possible to characterize the malware behavior using process tree information. However, there is a scarcity of research based tools available to extract process tree information from Windows operating system with high precision, therefore, the proposed sandbox provides such tool to capture the temporal state of the operating system up to nano second resolution. This data set represents extracts information such as parent processes, child processes spawned by the parent processes, modules used by each process, information on number of OS threads, network connections and the Windows 7 directory locations used. Further, this extracted data is processed and stored in a MySQL database for further analysis. This sandbox is unique in the concept of providing comprehensive operating system information at 100 nano-second interval precision. Therefore, it captures virtually all activities except those which varies

within 100 nano-second. This sandbox does not provide semantic analysis of the process tree information directly, but provides a highly precise data acquisition framework such that the process tree relationship is extracted and can be used for further analysis of process tree dynamics using the process and module information thoroughly. Using Microsoft Developer Network libraries, this sandbox captures both the user level and privileged level information and can be used to augment existing sandboxing methodologies to characterize execution of malware processes and modules. It can be run both in a virtualized environment and also in a bare-metal setup.

2.5 Challenges of Cyber Threats and Characterization Systems

In the field of cyber security, the massive evolution of different characteristics of cyber-attacks has posed researchers with an unprecedented challenge of extracting unique set of features from available data attributes to cope with the dynamics and incessantly evolving nature of cyber threats [3]. Moreover, it is getting extremely difficult to determine a unique feature set or algorithms which can be used to detect a variety of cyber-attacks simultaneously with sufficient generalization. The primary rationale for this problem is attributed towards the intelligence introduced by adversaries in the latest threats, which not only morph in real time, but are also multi-faceted (e.g. can persist for long duration of time and fulfills their objectives in multiple stages [2]). Traditional cyber-security measures like firewalls, IDS/IPS, antivirus/antimalware systems and encryption techniques rely heavily on pre-known signatures (syntactic/heuristic/behavioral) for the characterization of cyber-threats. However, these techniques are proving to be futile in the face of advance mutating cyber threats, which are able to change their signatures in merely 15 seconds [105].

Increasingly, machine learning based approaches for the behavioral analysis of anomalous and legitimate traffic are being utilized. These techniques are based on determining the deviation of an observable object's behavior from an observed/known normal behavior, and further analysis and decision making is required to evaluate the deviated object as legitimate or false anomaly. Therefore, one of the limitations of machine learning is to know normal behavior of interest a-priori that can be further used to find deviation of objects from the known normal behavior [3]. In addition, human intelligence, expertise and feedback is also required to analyze and optimize the alerts produced by these machine learning engines to identify false positives/negatives and to activate blocking mechanisms (rule updates in firewalls, whitelisting approaches or IPS), when required. There are two major challenges faced by existing traditional machine learning algorithms to characterize/detect advanced persistent/mutated cyber threats and the subsequent human analysis for reliable decision making, (1) class inseparability problem (due to persistent, mutated and advanced nature of threats), and (2) class imbalance problem (due to big data challenges and stealthy behavior of malicious activities to evade detection – "finding a needle in the haystack" problem). These two challenges are described in detail in the following sub-sections. Further, due to these two challenges, existing cyber threat characterization mechanisms (such as event analysis methods in cyber security operations center - CSOC) produces high rate of false alerts which subsequently increases the cognitive burden of alert triaging and is also discussed later in detail.

2.5.1 Class Inseparability

Advanced persistent threats include malware, which are often encrypted and persistent in nature, render obfuscation and mutation by masquerading the behavior of a normal or legitimate data sample [3] [204] . It implies that on a feature space, the malicious and benign samples lie on the same co-ordinates (follow the behavior/characteristics of normal samples), making it difficult to detect the anomaly. For instance, phishing emails are used to deliver a malicious payload to the end user. The content of the phishing emails is generated using known legitimate email content/meta patterns of users and thus are able to dupe them to open those emails which in turn deliver the malicious payload without letting the user know. Therefore, in this case, the positive (threat) and negative (legitimate) samples are inseparable on typical single scale feature space. For example, if the feature of information gain [205] is used to discriminate the content of malicious email from legitimate email content, there would be very little or no information gain measured between the two and therefore, classification systems utilizing information gain as discriminatory feature will falsely classify phishing emails as legitimate. Further, the advanced phishing emails contain web links which can only be detected by the intrusion detection systems if the signatures are available in their database already. Unless we know the domain name, source IP or the regular expression (RegEx) of the malicious email content, phishing attacks may not be detected. Thus, this may become a signature based detection problem, which requires a human expert to analyze the unique signatures and then update them manually. This example demonstrates that threats are able to successfully masquerade within legitimate/normal flows of traffic, and they are able to change signatures so quickly that, if there was initially a non-overlapping classification feature space, it is merely a matter of time that the feature space would become overlapped, and the data samples would become inseparable and indistinguishable, thus, making the feature space selection an NP-hard problem [3] [206].

It can be argued that if a feature space is not separable in two dimension, then it may be possible in more than two dimensions. For example, SVM based classifiers can be used to project the features in higher dimensional space for linear classification. However, this poses three problems in malware analysis; (1) curse of dimensionality, (2) a-priori knowledge of the number of dimensions (features), and (3) generalization. Besides a big data analytic issue, the curse of dimensionality is also a well-known problem in malware analysis [207] [208]. Static malware analysis mechanisms can perform better with lower dimensionality (or low features) and the accuracy of detection decreases with increasing dimensionality. Further, as malware behavior inside a process tree is not static and varies greatly by virtue of malware intelligence, therefore each new morphed instance [209] is not detected by anti-malware defenses [210]. Also, it is not possible to find a unique set of features (or set of dimensions) to characterize a threat (or a family of threat) reasonably and reliably [113] . Moreover, in the application domain of cyber security, finding a set of particular features (statistically independent) which can distinctly detect cyber threats uniquely is a NP-Hard problem [206]. Further, new and advanced mutation tools and increasing cognitive intelligence of malware objects have made it possible to change the malware feature set very quickly e.g. in mere 15 seconds [211]. Therefore, evaluating and re-evaluating (when a new data instance having the possibility of malware) classification or decision boundaries is not practically feasible anymore. Also, using a large number of features (dimensions) for

malware analysis is not cognitively reasonable due to additional complexity of the higher dimensionalities and the presence of heavy tailed distribution [113] which makes it unsuitable to classify or characterize malicious samples in a data of large number of outliers. Also, it is not practical to visualize higher dimensions for cyber security experts and therefore, a feature set with lowest possible dimension should be used to extract malicious behavior discriminately and continually to ensure sufficient generalization.

In order to further emphasize the role of complexity and dynamically changing threat landscape, Figure 11 [3], Figure 12 [3], and Figure 13 [3] provide a visual interpretation of how malware classification using traditional machine intelligence mechanisms is becoming difficult. As shown in Figure 11 [3], a two dimensional feature space is depicted where blue cross (x) represents normal network traffic and red dot (o) represents attack traffic. As can be seen, it is a linear classification feature space and any properly configured machine learning system can easily classify these samples with sufficient reliability and accuracy.

However, as shown in Figure 12 [3], the feature space depicts that the attack and normal samples are not separated across a linear classification boundary but still occupy discrete location which separates attack and normal samples. The boundary is highly nonlinear and classification for such data set is difficult to achieve using existing Euclidean metric based machine learning systems which tend to suffer from either under- or overgeneralization issues. Available literature discusses in detail about these two classification cases (linear and nonlinear separation decision boundaries) and the efforts are concentrated in finding a suitable machine learning algorithm that can classify and characterize non-linearly separable samples with sufficient generalization and regularization [212].

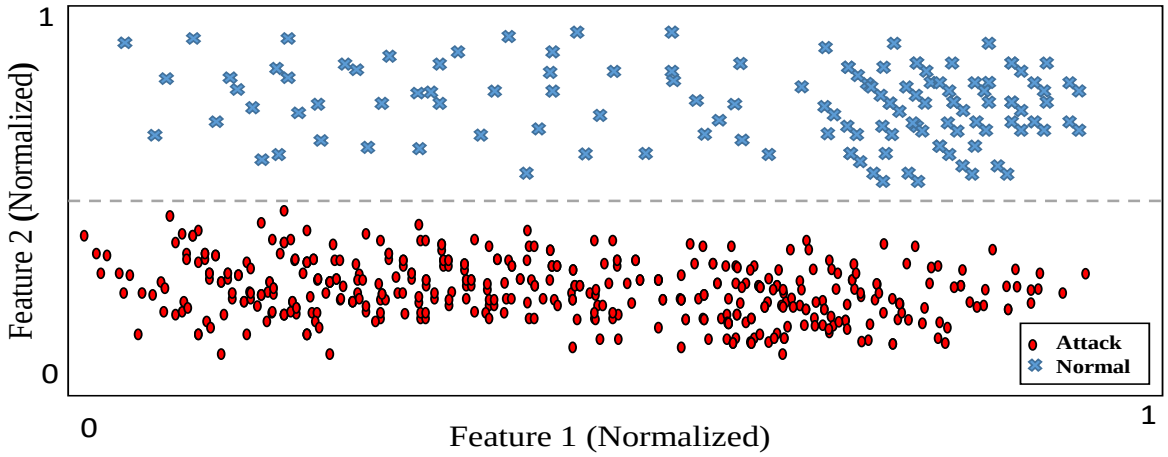


Figure 11: Malware samples having discrete (non-overlapping) and linear classification boundary.

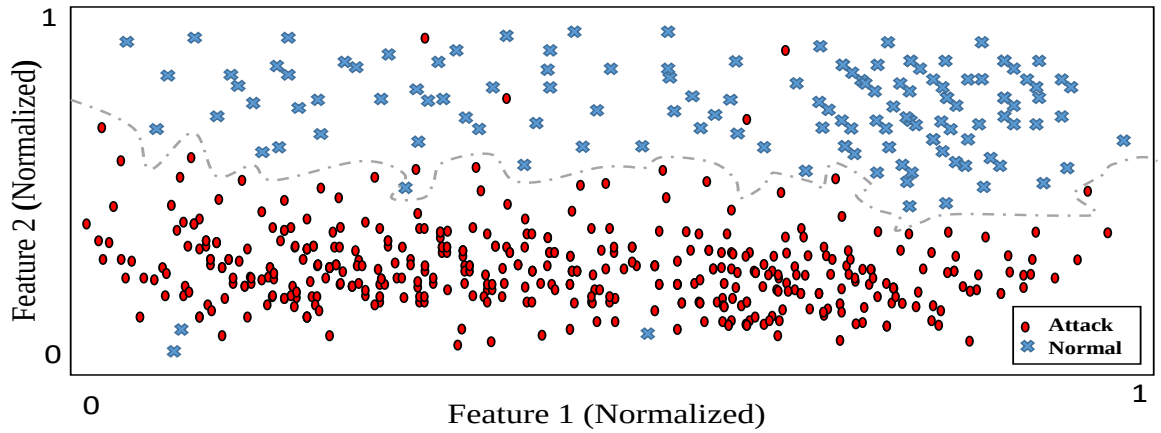


Figure 12: Malware samples having discrete (non-overlapping) and highly nonlinear classification boundary.

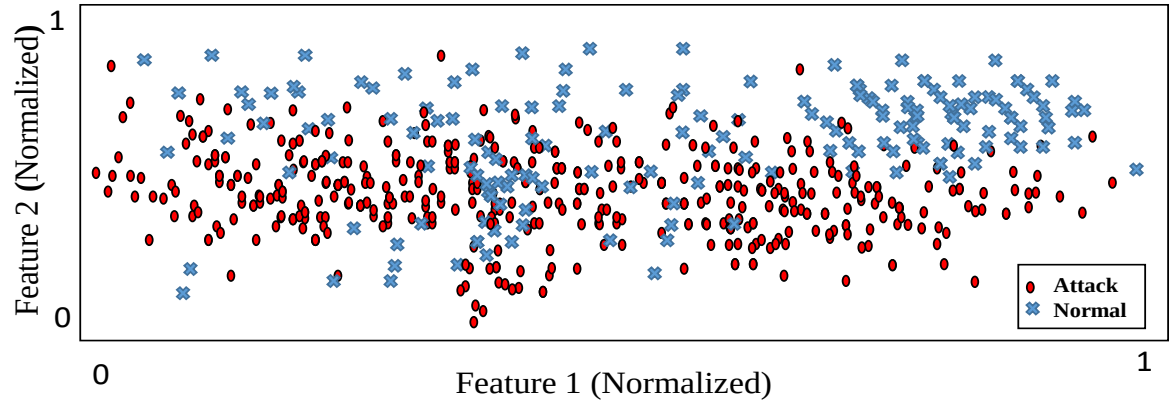


Figure 13: Malware samples showing overlapping classification feature space.

On the other hand, it can be observed in Figure 13 [3] that the feature space is extremely overlapping and complex. Both the attack and the normal data samples either lie on the same co-ordinate or are not sufficiently separable and therefore are indistinguishable. These scenarios are quite common in the domain of cyber-security where advanced threats try to mimic the behavior of a legitimate internet flow and are successful in concealing themselves. Thus, it becomes imperative for the security researchers to consider the cognitive relationship between different data attributes by introducing the concepts of multiscale analysis (as discussed in section 2.6.3) in feature space analysis and algorithm. This will help in understanding the details which otherwise are hidden over single scale.

Research literature [213] [214] indicates that overlapping patterns are ubiquitous in the area of image and vision processing. Overlapping patterns are similar, repetitive and intersect each other. They can be geometrically superimposed or can be continually changing or static. From the perspective of image and vision processing, an overlapping pattern can be considered an illusion for the viewer. This overlap or superimposition creates a new pattern. Fractals are self-similar patterns which shows a sense of similarity and long range correlation when analyzed at different measurement scales and are thus an important tool to analyze overlapping patterns. A detailed description of fractals and their measurement is provided in section 2.6.3. The challenge of class inseparability in cyber security can be analyzed using fractal dimensions which provide a measureable way of finding self-similarity at different measurement scales. Fractals and overlapping patterns can be related using the concepts of self-similarity and long range correlation [113] [215]. Further, heavy tailed statistical distributions are considered as an indicator of fractal behavior and can therefore encourage to apply fractal analysis [216]. As heavy tailed distributions exhibit memory and large number of outliers, the long range correlation does not decay quickly and thus renders self-similarity at multiple scales, which warrants the application of fractal analysis [217] .

2.5.2 Class Imbalance

The class imbalance problem refers to the challenges of collecting sufficient samples of normal and anomalous class so that data analysis can be performed with statistical sufficiency and an optimum balance between statistical bias and statistical variance for reliable analysis can be obtained. As supervised machine learning systems try to capture the underlying relationship between the input data features and their corresponding ground truth labels (using certain measures e.g. Euclidean), there exists a tight coupling between the performance of a learning algorithm and the proportion of the selected training examples with respect to different classes. Often, the process of collecting labelled data from real-world applications is so cumbersome that it hinders the selection of suitable and sufficient data quantity that can be used for training these learning systems [218]. Commonly, this results in a problem where data from one of the classes outnumbers the other and thus called a class imbalance challenge. For example, fraud detection in banking transactions, anomaly detection in computer systems, and cancer detection in humans. In the domain of cyber security, this problem appears frequently due to the stealthy and obfuscated/mutated behavior of malicious objects, which either tries to mimic the normal data or use obfuscation techniques to avoid detection. Further, state of the art malware are capable of remaining inside the victim networks for many years before executing their malicious objective. Further, due to the challenges of big data where high volume, velocity and veracity are common [219], finding malware is equivalent of finding a needle in a haystack! [113] [14] [29].

In such a scenario, classifiers tend to follow the characteristics of majority class and tend to ignore the characteristics of minority class causing suboptimal classification results. This is because the learning algorithms are trained to consider accuracy measure as a performance measuring tool, which is directly proportional to the overall error, in which the contribution of the minority class is very small. Moreover, a strong assumption in such classification experiments is that the cost associated with the error contributed by each of the class is equal, which is not true as most of the time the cost is not known a priori even to the experts [220] [221].

In order to mitigate the effect of class imbalance, two major approaches are recommended:

1. Re-sampling based approaches.
2. Cost function based approaches.

The sampling based approaches which are aimed towards artificially balancing the data set can be further categorized in three different ways i.e. (i) under-sampling, (ii) over-sampling, and (iii) hybrid. In the first approach of under-sampling, the samples from the majority class are eliminated until the balance is achieved in the data [222]. This helps to reduce their representation in the feature set and overall effect on the learning algorithm [223]. The major drawback with this process is the loss of critical information which may be necessary to obtain the correct generalized results. The next method of over-sampling deals with duplicating the minority class instances until the data rebalance is achieved [224]. This may lead to the problem of over-fitting the given data by the classifier. A nice alternate to replication process is to create new minority class samples as suggested in [225] . Another approach is the hybridization of the already stated technique where

majority class is under sampled while the minority is over sampled [226]. In this scenario, the advantages and disadvantages of both the techniques are combined.

On the other hand, the cost function based techniques exploit the assignment of different error penalties to each of the misclassified class sample. It implies that for the minority class instance the penalty will be larger compared to that for the majority class. It has been argued in the literature that using different costs for each of the classes is proportional to altering the data distribution that eventually leads to data rebalance [227]. A detailed discussion is available in [228] [229] [230]. Thus, using cost-sensitive learning algorithms can be helpful in mitigating the effect of class imbalance.

2.5.3 Cognitive Load of Processing Alerts in CSOC

The existence of class imbalance and class inseparability issues result in the generation of enormous alerts which place a lot of cognitive burden on CSOC human analysts in terms of threat hunting and threat investigation tasks. As mentioned in [231], a recent study by Advanced Threat Analytics (ATA) organization reveals that existing methods of analysis are mostly manual and therefore, takes an average of more than 10 minutes to investigate each alert. Further, these manual methods of threat analysis which are mostly rule-based, generate more than 50% false alerts which implies that half of the time the investigation efforts are futile. In addition, same report reveals that CSOC experts are inundated with thousands of security alerts per day, which is not possible to handle by manual methods, and therefore, they prioritize alerts based on their alert configurations and ignore certain categories of threats, which opens venue for high false negatives. Another recent report from Cloud Security Alliance [232] reveals that existing state of the art CSOC technologies generates more than 2.7 billion alerts in an average sized enterprise which further contains an average of 2500 anomalous events out of which only 23 are actual threats. Thus, the manual configurations for triggering an alert often ends up in generating anomalous events which are about 99% false. Also, this reveals that capturing a true malicious event is extremely difficult and can end up being ignored quite easily due to the analysis burden on the threat investigator. Therefore, the issue of false positives and false negatives is a serious challenge with existing CSOC technologies and is attributed to the following limitations:

1) Manual analysis of events for threat investigation – lack of cognitive intelligent mechanisms for threat investigation.
2) Evasion of threats from CSOC monitoring mechanism due to class inseparability and class imbalance (high false negatives) – requires cognitively intelligent methods for threat hunting.

2.5.4 First Use Case - Class Inseparability and Imbalance Challenges in Operating System Process Tree Dataset

This research characterizes temporal characteristics of a host process tree infected by a mutating malware in a controlled experimental environment. To further emphasize the challenge of class inseparability and imbalance over a selected set of features, an example of Carperb malware based infection of Windows 7 operating system is presented in this section with labelled (malware process is a red node and legitimate node is green) process tree graphs as shown in Figure 14 and Figure 15 for two separate instances of Carperb malware execution. Each node of the graphs represents the process ID (PID) and process name of the process tree in a directed flow graph. These two instances indicate the dynamic morphing behavior which Carperb malware exhibits in each execution iteration. Detailed graph based analysis of this malware, along with others, is available in the experimental section. Carperb malware instance 1 opens Windows processes as 151(svchost.exe), 152 (svchost.exe) and 47 (wow64cpu.dll). PID 151 and 152 are the real Carperb malware processes mimicking a legitimate Windows 7 process name i.e. “svchost.exe”, while PID 47 is a legitimate Windows 7 dynamic link library (DLL) file required to execute “svchost.exe”. As can be observed in Table 44, Carperb malware shows a very high class imbalance where malware nodes are 6% of the total nodes and edges are 1% of the total edges. This process tree graph represents evolution of Windows 7 operating system for an execution time period of 87 minutes. Executing Carperb malware file again in Windows 7 operating system shows that the process changed to 152 (svchost.exe), 153 (svchost.exe) and 49 (wow64cpu.dll) again mimicking legitimate Windows processes. Windows operating system uses “svchost.exe” file to host multiple instances of Windows concurrently [233] and is a legitimate Windows core file. However, Carperb uses this file name to evade antimalware software which uses whitelist approach (keeping a list of all legitimate programs including “svchost.exe”) to block or alert any program not listed in the whitelist. Further, as observed, running a new instance of Carperb malware exhibits different PIDs but legitimate process names and therefore, process name based approach to detect the presence of malware is not effective and also has class ratio is 1% for both malware nodes and edges further adding the issue of class imbalance.

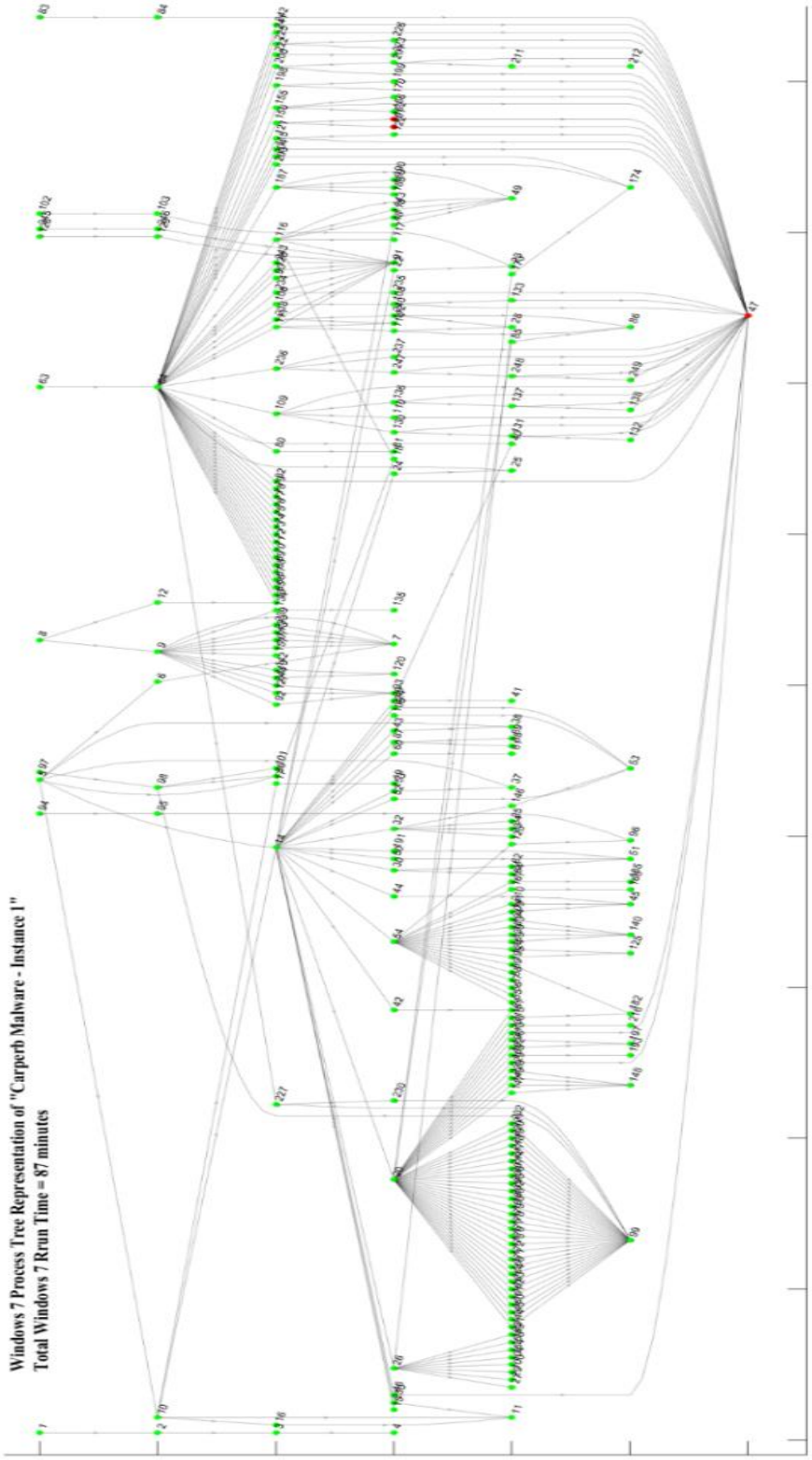


Figure 14: Carperb Malware - Instance 1 - Graph representation of Windows 7 Process Tree.

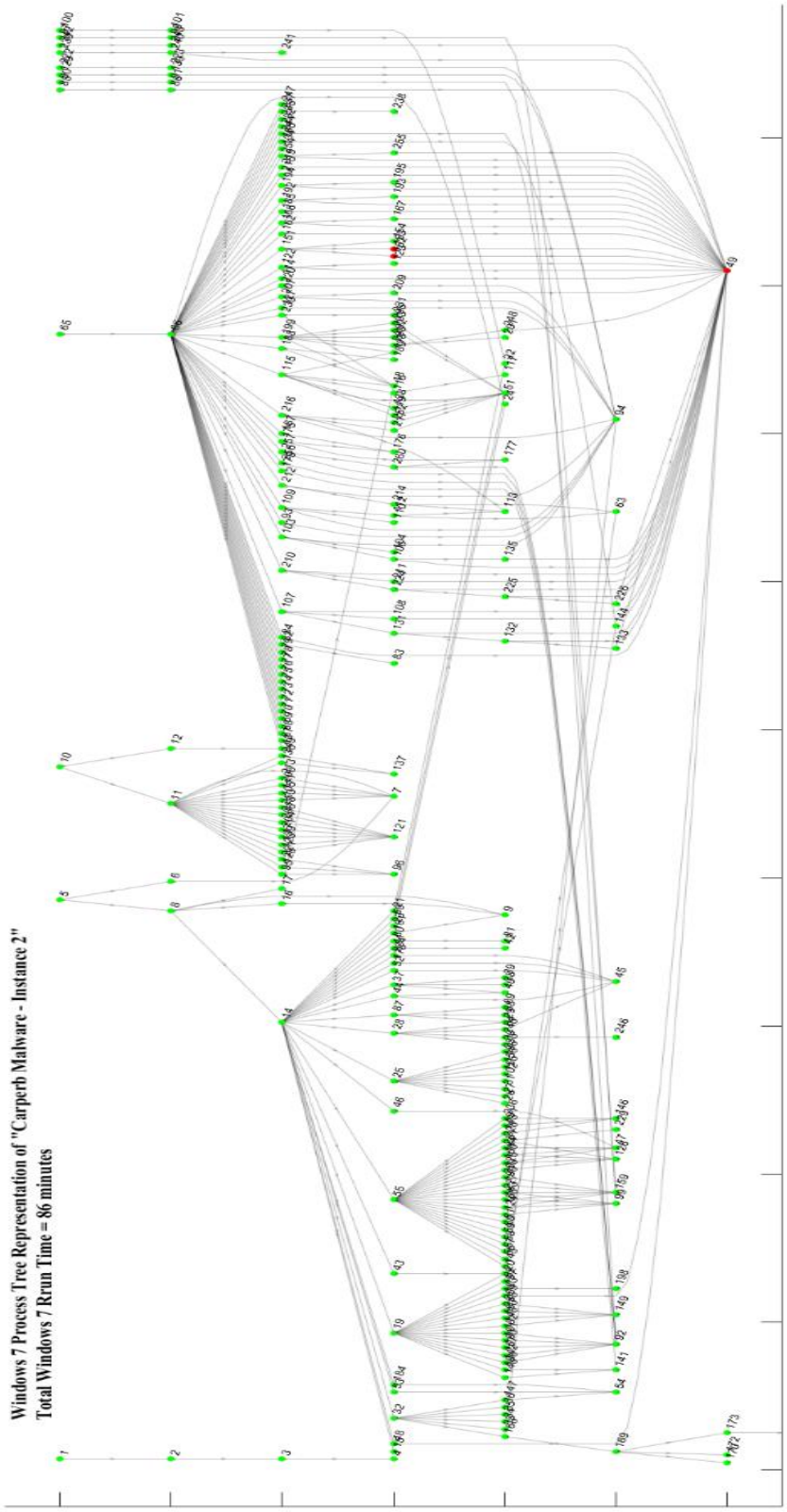


Figure 15: Carperb Malware - Instance 2 Graph representation of Windows 7 Process Tree.

To augment analysis of host operating system process tree, a time based snapshot of process tree graphs of both Carperb instances is shown in Figure 16 and Figure 17. These time based snapshots are developed using an adaptive and sliding time windowing algorithm as mentioned in subsection 4.2.5. These graphs represent the state of the operating system process tree for each time window lag of 1 micro-second. Further, each time window represents the active process tree illustration using graph. For example, time window 61 shows the graph of the processes active during this 1 microsecond lag based adaptive time window and does not show any detail of the time window 60 or 62. This provides a highly filtered and clear view of the process tree dynamics. As can be seen in Figure 16, malware node (colored red), time windows 61, 69, 70 and 71 show the malware presence which indicate that the malware did not appear in each time. This also shows that the execution accuracy of Carperb malware is at least 1 microsecond as observed from the changing footprint in evolving time windows. Further, the malware uses the same process name as the legitimate process and therefore, is not identifiable using any process tree based knowledge such as PIDs or process names. Also, malware attaches itself to legitimate process nodes such as 150 and 47 and therefore, cannot be detected as a disconnected process tree having only malware nodes. An example of a disconnected process tree is shown in time window 66 where the legitimate process tree of 10-145-99 and 32-146-153 are disconnected graphs. Also, as the time window increments, the structure of process tree also changes and is not possible to assign any graph theoretical structure behavior to the malware e.g. time windows 65 and 70 show a diamond shape graph while time window 65 is a legitimate graph and time window 70 has malware processes. Running Carperb malware again shown an entirely different tree structure as shown in Figure 17. Time windows 67, 68, 69 and 73 contain the malware processes and shows different node attributes.

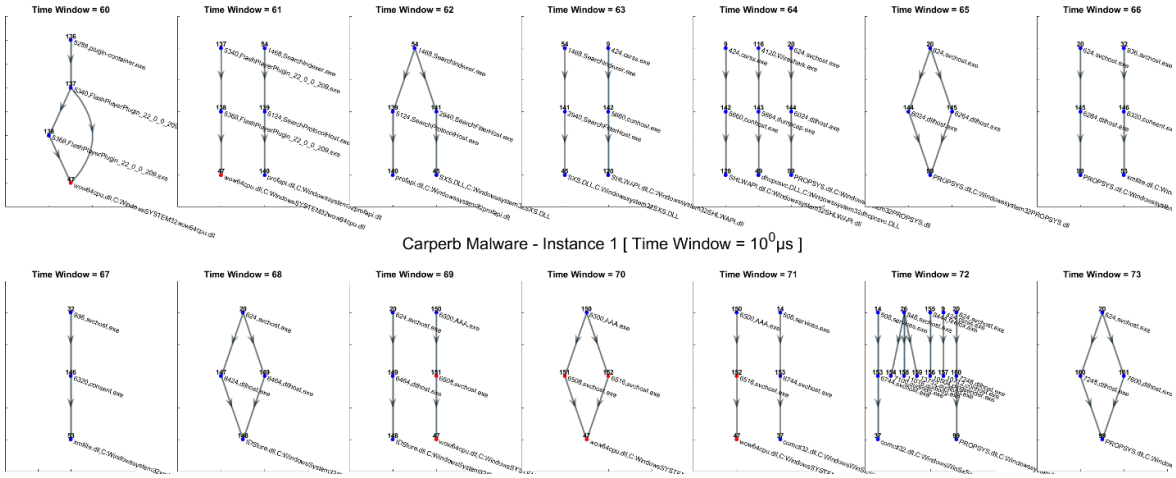


Figure 16: Carperb Malware - Instance 1 Time Graph - 14 Time Windows of 1 microsecond each.

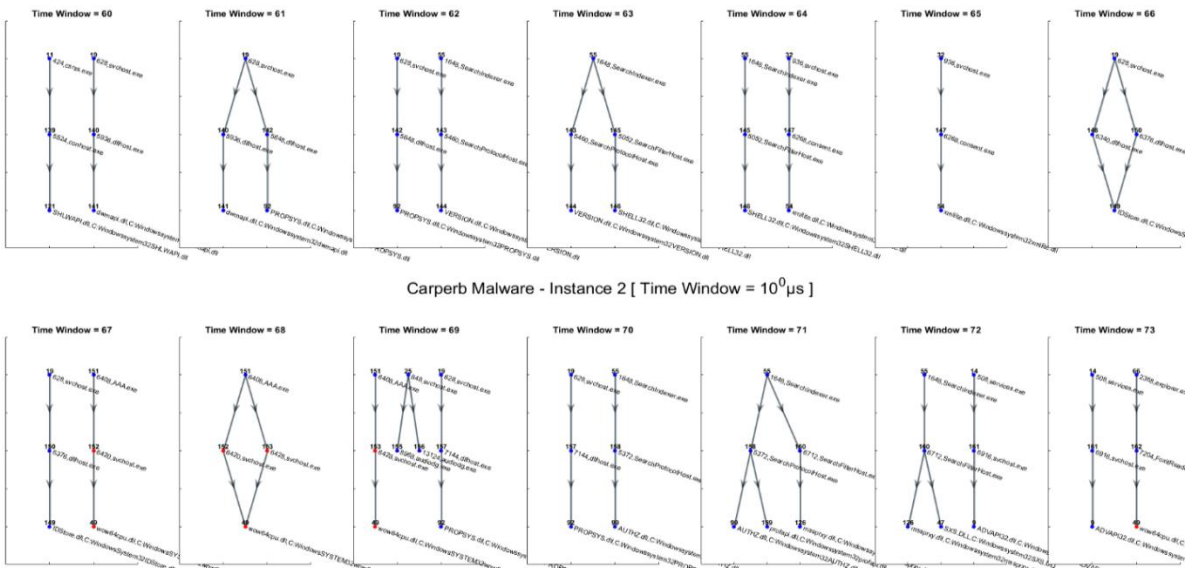


Figure 17: Carperb Malware Instance 2 Time Graph - 14 Time Windows of 1 microsecond each.

From the time graphs of Figure 16 and Figure 17, many features can be extracted to study and characterize legitimate and malware behavior semantically and are presented in detail in the experiment section. Here, features of node and edge counts is shown in Figure 18 and Figure 19. Node count feature represents total number of nodes per time window where if a time window contains one or more than one malware nodes, the time window is labelled red. The primary objective of this feature is to detect the presence of any abnormal increase or decrease in the node count to analyze the presence of malware node. Cognitively speaking, this approach to label the time window is feasible since knowing the time window will point out a very small subset of processes which can be analyzed further for malware detection. As can be observed in Figure 18 and Figure 19, malware and legitimate processes are overlapping (red and blue samples overlaps) as malware process is following the same syntax (process name) and same heuristic (graph structure and node counts) as the legitimate process. Similar deductions can be made for the graph based edge count feature in Figure 20 and Figure 21.

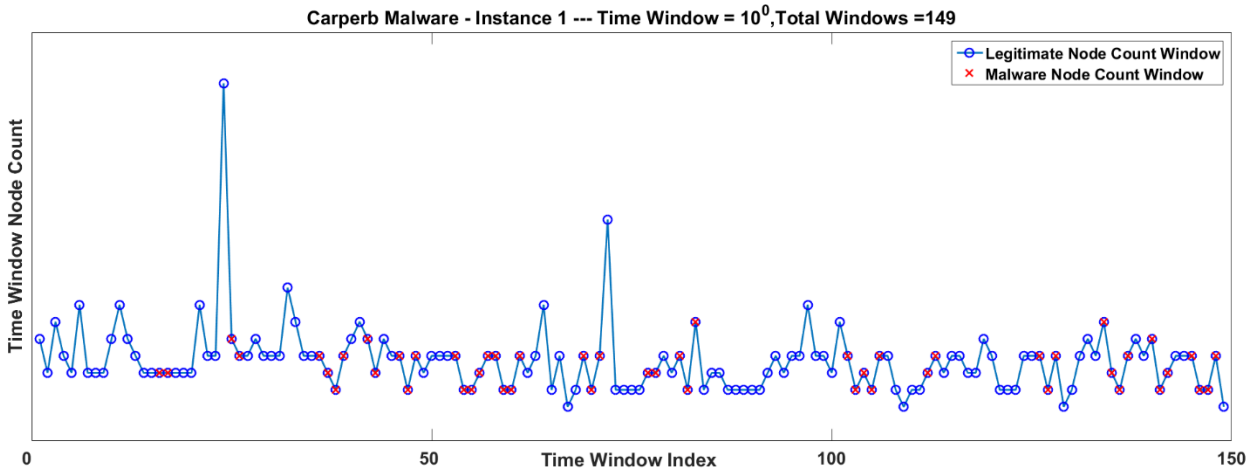


Figure 18: Carperb Malware - Instance 1 - An example feature of labelled node count time series.

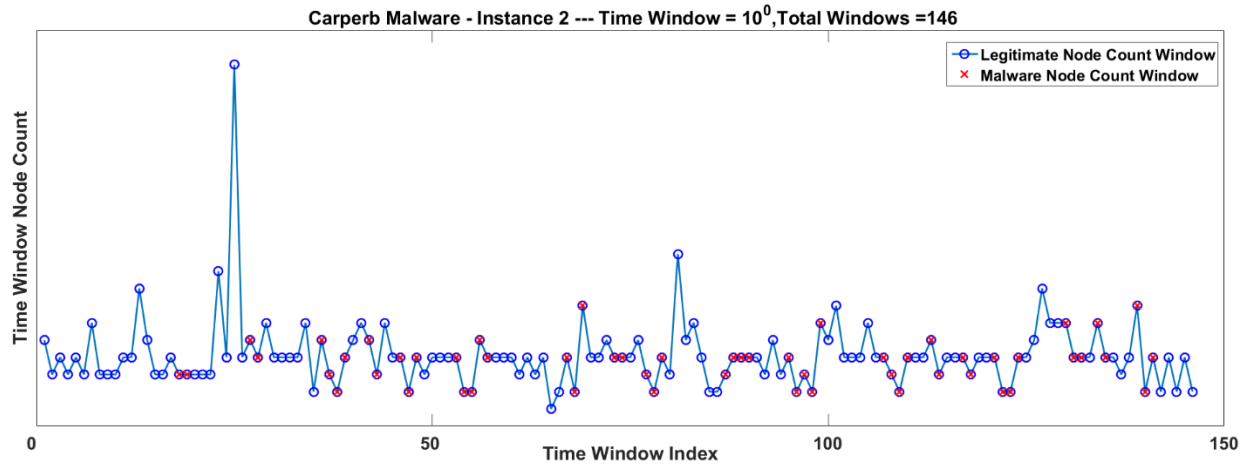


Figure 19: Carperb Malware - Instance 2 - An example feature of labelled node count time series.

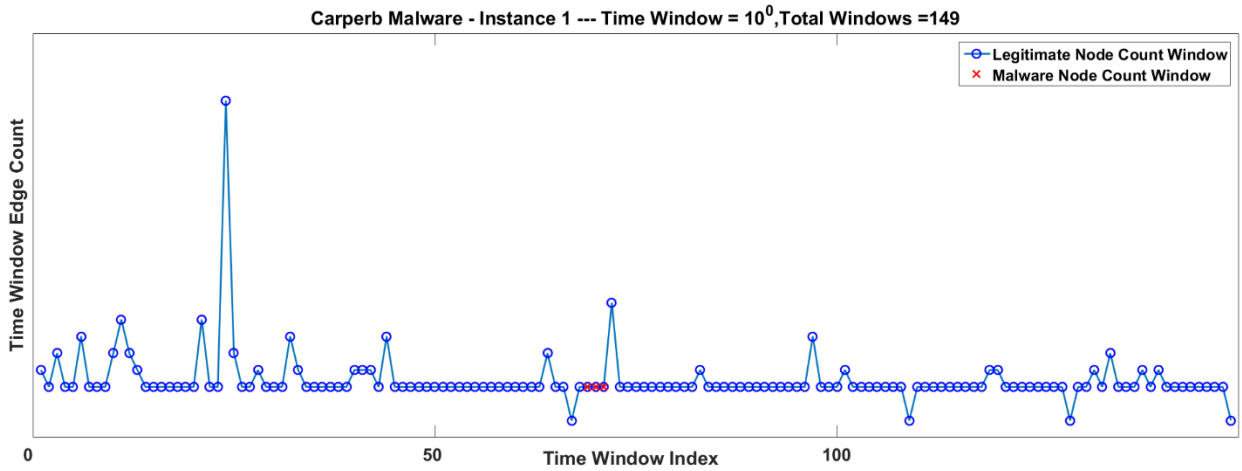


Figure 20: Carperb Malware - Instance 1 - An example feature of labelled edge count time series.

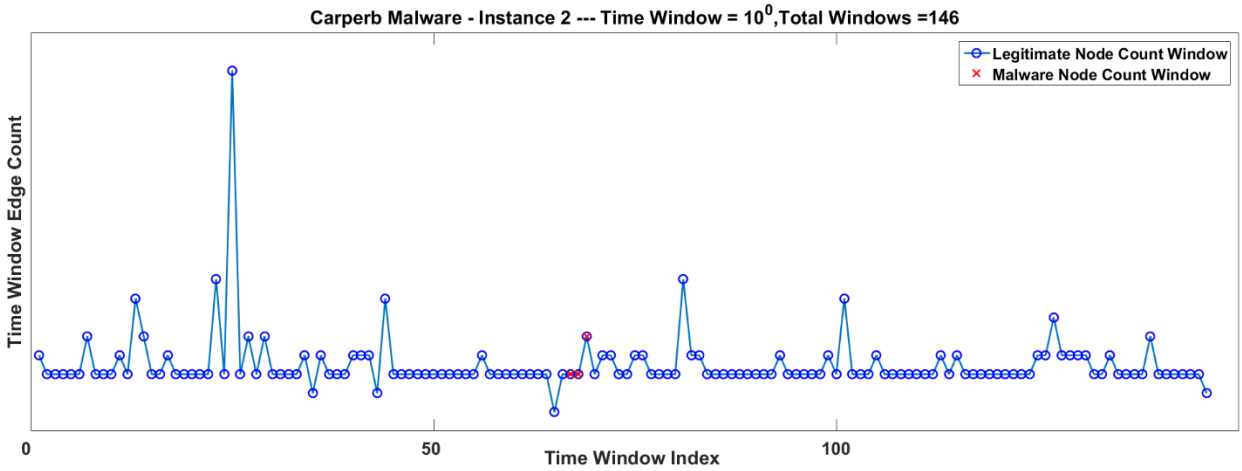


Figure 21: Carperb Malware - Instance 2 - An example feature of labelled edge count time series.

As Figure 22, Figure 23, Figure 24 and Figure 25 shows, both node and edge count features show heavy tailed distributions as evident from the estimated Kurtosis value. Kurtosis is a 4^{th} order statistical moment and indicate the presence of the heaviness of the distribution tails i.e. large number of outliers. Higher the Kurtosis, higher the heaviness. Kurtosis of 3 represents light tailed Gaussian distribution.

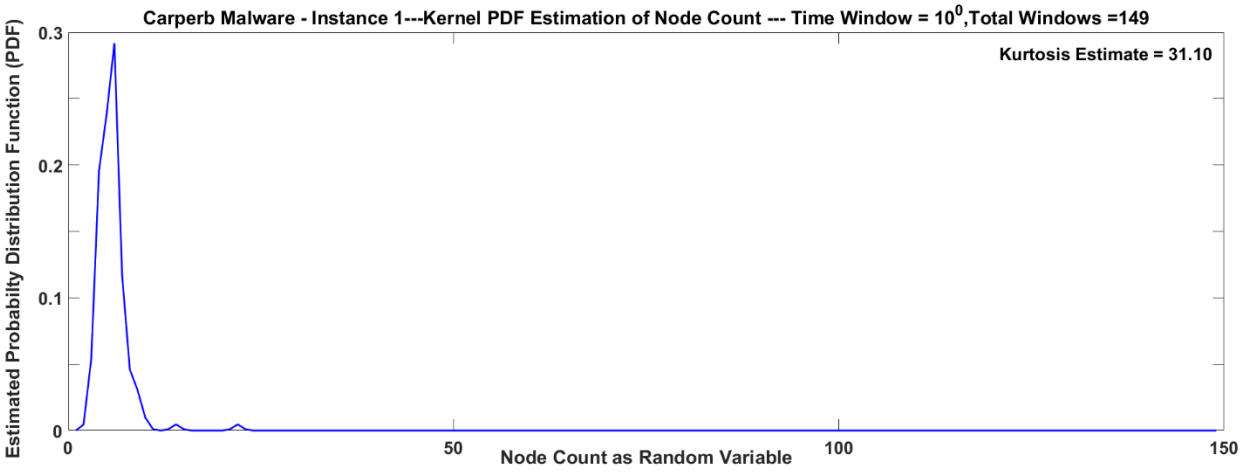


Figure 22: Carperb Malware - Instance 1 - Estimated PDF of node count time series.

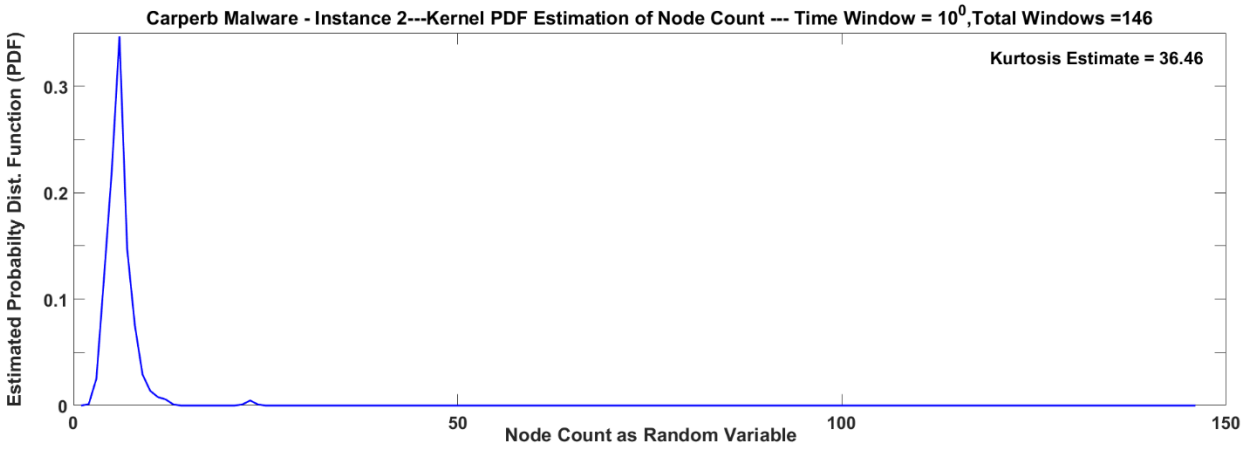


Figure 23: Carperb Malware - Instance 2 - Estimated PDF of node count time series.

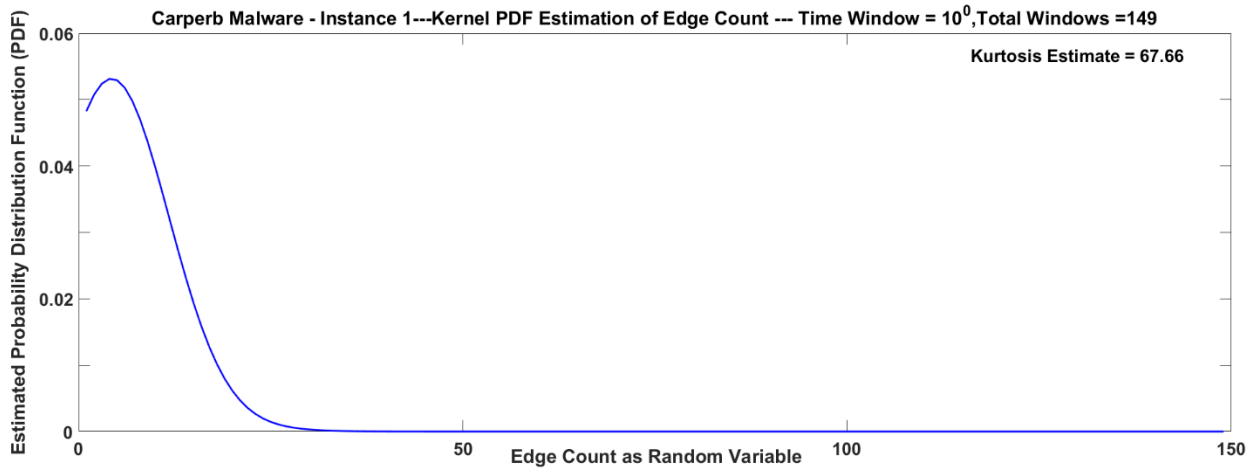


Figure 24: Carperb Malware - Instance 1 - Estimated PDF of edge count time series.

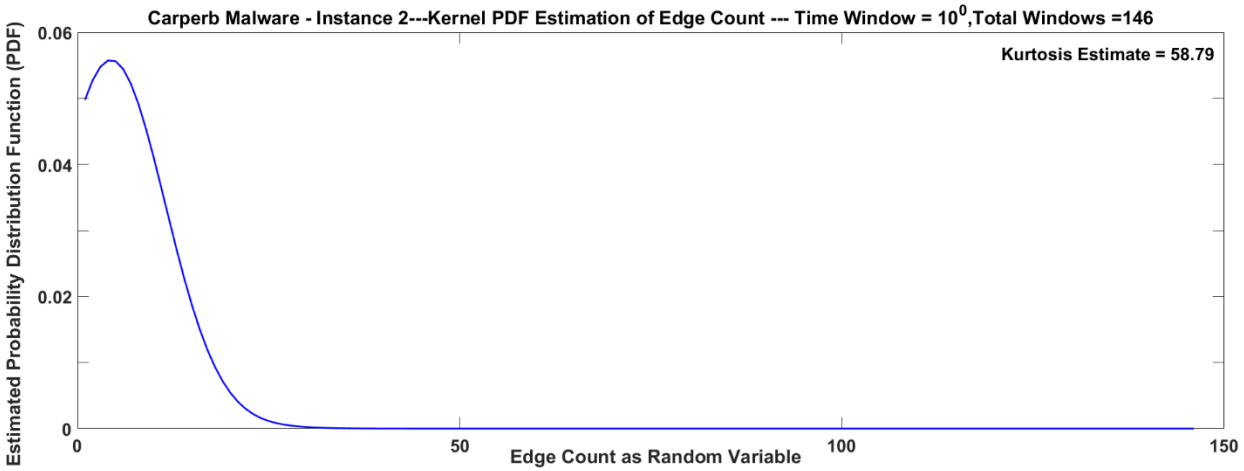


Figure 25: Carperb Malware - Instance 2 - Estimated PDF of edge count time series.

Therefore, through this example, it is analyzed that intelligent malware like Carperb mimic the behavior of normal and legitimate Windows operating system process over a feature of counts by adopting the legitimate process names and using other legitimate operating system resources. Further, the example feature of count per time window (for both node and edge) shows that the mimicking malware overlaps the legitimate feature coordinates and thus poses the issues of inseparability. However, as the feature statistical distribution is heavy tailed, it is possible to analyze the feature using fractal which is an established method of overlap analysis in image and vision processing.

2.5.5 Second Use Case - Class Inseparability and Imbalance Challenges in a Network based IP Dataset

Another data set in the field of cyber-security which depicts the inseparability characteristic is the UNSW-NB-15 dataset captured and processed in the year 2014 at Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) [234]. This contains total number of samples as 206, 2730 and the ratio of attack to normal samples is 10.06% [9] which represents class imbalance. HTTP flow based analysis for this dataset [113] is performed, as it is one of the widely exploited protocols to launch attacks due to its wide prevalence in internet applications. Out of 49 different attributes and features listed in the dataset, only four features are assessed, which include packet duration, total number of bytes in each packet exchanged between the source and destination, packet round trip time and total packet inter-arrival time. It is discovered that all of the selected features followed heavy tailed distribution (Kurtosis estimate is very large) to evade detection methods as shown in Figure 26, Figure 27, Figure 28 and Figure 29 respectively for each feature. It was found that the distribution of the attack samples was indistinguishable from that of benign data samples, which is due to the masquerading behavior of network based threats that follow the patterns of normal packet data. As evident, it is impossible to classify this data using any linear or non-linear learning algorithm with these features. This is a challenging situation in the context of machine learning although fairly normal for state-of-the-art attacks. Therefore, applying a Euclidean measure (mono/single scale) based learning technique which expects at least light tailed distribution (low number of outliers) is not feasible [235]. Hence, complexity based cognitive capabilities are needed as discussed in the section 2.6.

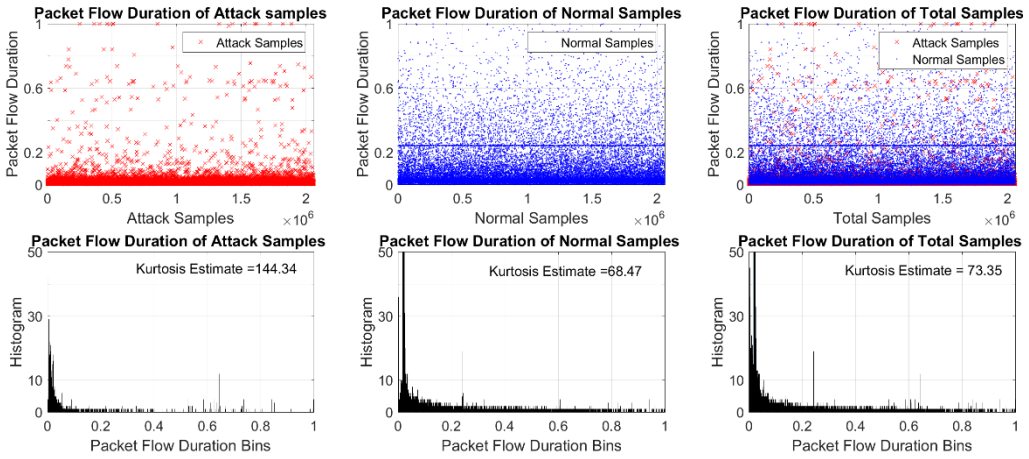


Figure 26: UNSW-NB-15 network packet dataset – Labelled packet flow duration feature.

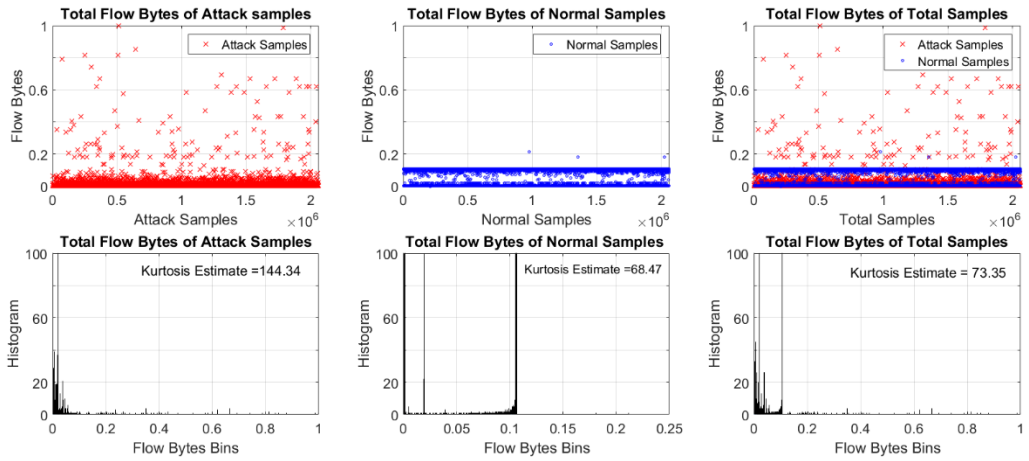


Figure 27: UNSW-NB-15 network packet dataset – Labelled total flow bytes feature.

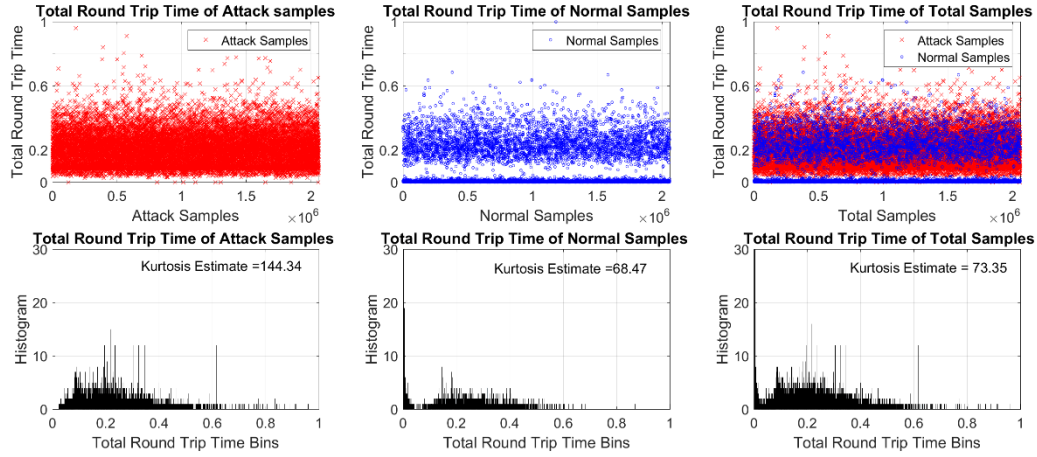


Figure 28: UNSW-NB-15 network packet dataset – Labelled total round trip time feature.

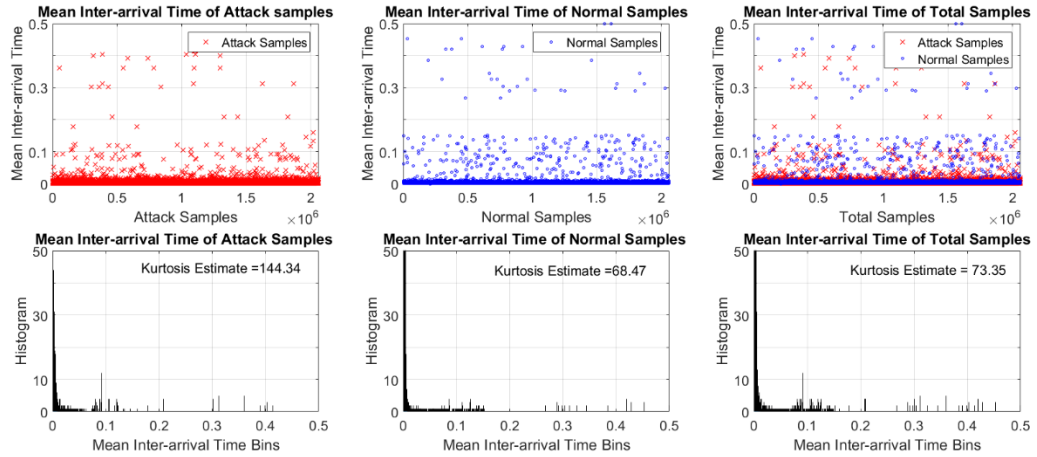


Figure 29: UNSW-NB-15 network packet dataset – Labelled mean inter-arrival time feature.

2.6 Cognition in Malware Analysis

In the research world [236] [237] [238] [239] [240], the terminology of intelligence is defined as the human mental capability to reason, learn and solve problems. Cognition is defined as the human brain mechanism which is required to carry out a task. Intelligence can be considered as a measurement of human cognitive capabilities and therefore, improved cognitive abilities corresponds to higher intelligence. Also, intelligence can be considered as an integration of cognitive functions such as perception, memory, attention, language and reasoning, among others.

Artificial Intelligence is a broad domain covering wide range of machine intelligence theories and models including but not limited to machine learning, deep learning, decision making, Fuzzy logic, cognitive informatics and cognitive computing. [241] [242] [243] [244]. The vision of empowering machines with simulated human cognitive abilities has led to the development of Artificial Intelligence and Machine Learning theories, models, and concepts. The domain of information theory has evolved from classical Shannon based models to cognitively inspired models and has given rise to the field of Cognitive Computing and Cognitive Informatics. Wang in a keynote in 2002 defines the term Cognitive Informatics (CI) [236] which investigates new and existing methods of how a human brain perceives and processes information, which can be engineered to enable a machine to cognize information and take decisions. In order to apply the human inspired cognitive informatics model into machine applications, Cognitive Computing evolved as a promising domain to devise new computing mechanisms based on Cognitive Informatics to improve machine intelligence. Therefore, Cognitive Informatics and Cognitive Computing are associated closely and research progression applies to both domains. As the current state of cyber security, particularly malware analysis, is heavily dependent on human insight, interaction and analysis, therefore, this dissertation applies cognitive computing techniques to analyze and characterize malware behavior in an operating system in a systematic method.

In this chapter an introduction to cognitive computing and its relationship with complexity is described. Further, the concept of complexity is connected to cyber threats and the most difficult challenge of threat classification in cyber security, i.e., class inseparability problem.

2.6.1 Cognitive Computing

Cognitive Computing (CC) systems learn and interact with humans naturally and measure complexity of data to extract meaningful information for humans [245]. Current research in the field of cognitive computing mostly focuses on the development of computational tools and autonomous intelligent systems to mimic human-like behaviors, for example, inductive inference that humans use to solve complex problems. Cognitive science deals with human behaviors, which are studied using subjects from neuroscience, philosophy, linguistics, anthropology and psychology [246]. Research in cognitive computing is heading towards developing computational models and tools of cognition, i.e., modeling improvements in decisions using experience and historical data (learning) or changing the classification engine to cater new needs using stimulus-response mechanism of human behavior (adaptability). Such models and tools include but not

limited to artificial intelligence, artificial neural networks, natural language processing, data mining, decision theory, statistical inference models, and multiscale and multifractal analysis.

In the domain of Computational Intelligence (CI), components of human cognition are perception, foresight and investigation [247]. A recent study by IBM [245], founder of the world's first cognitive computer named Watson, intelligent computing is not only performing close to human cognitive mechanisms in many aspects, but is also faster than human cognitive systems. For example, searching for best price of a product, humans do lot of searching (investigation) and decide a particular brand and price (perception) based on multiple factors, i.e., utility, ease of use, and foresight. With the help of cognitive computing, this process can be accelerated by providing constraints as inputs and running the search over available data of product and their prices.

In the context of network security, object classification literature shows that computer software and hardware algorithms are increasingly showing signs of cognition [5] and are necessarily evolving towards cognitive computing machines to meet the challenges of today's engineering problems (e.g., [248] [249] [250]). For instance [6], in response to the continual mutating nature of cyber security threats, basic algorithms for intrusion detection are being forced to evolve and develop into autonomous and adaptive agents, in a manner that is emulative of human information processing mechanisms and processes [251]. Indeed, the challenges posed by today's cyber threats on the security of computing systems and networks require intelligence beyond that provided by the outdated and ineffective conventional algorithms [252] [253] [254]. Today's object classification researchers are actively investigating ways of increasing the cognitive abilities of computationally intelligent algorithms [6], such as artificial neural network (ANN), artificial immune system (AIS), evolutionary computing (EC), and particle swarm optimization (PSO) to combat the ever mutating complex strains of cyber threats [250]. Moreover, researchers are exploring ways in which the mechanisms within the Human Immune System (HIS) can model cyber-threat detection systems in computer networks [255] [256]. However, base-line applications of these algorithms still have limitations in performing threat classification sufficiently well and are still less efficient than human beings at performing classification [250]. This limitation is mainly attributed to the shortcomings of existing machine intelligent algorithms in handling the ever increasing complexity of threats due to advance and intelligent mutation techniques employed by the threat adversaries e.g. threats are able to mimic legitimate behaviors of computing architecture and are able to hide their existence using deception techniques [14]. For example, phishing emails are crafted in such a way that normal human user considers them legitimate and are trapped to perform the adverse actions to fulfill the threat objectives. Further, cyber experts using advanced cyber security operation center (CSOC) technologies e.g. SIEM, Dashboards, are not able to detect the presence of malicious flows and malware activities because of their close similarities to the legitimate activities shrouded in big data (challenge of finding needle in the haystack). Therefore, it is desired to improve the performance of machine intelligence techniques to measure and annotate complexity to malicious objects to discriminate them from legitimate objects. Cognitive computing provides an answer to this problem using fractal analysis [14] [1] [257] [258].

Research on human cognition is an active area of research and there are many methods of modeling human cognition but there is no universal model that can fully explain the cognition in

humans and other living creatures [259]. Reptiles and other creatures make use of primitive stimulus and response mechanism in their cognition. More intelligent creatures like cats and animals infer from stimulus using analogies and then respond, while it is known that humans use perception, induction, abduction, deduction and take actions accordingly. So as the intelligence in cognition increases, the interacting components also increases, which also indicates an increase in complexity. However, it is also shown that there are multiple levels of cognition in humans, i.e., the instant reaction to touch a burning metal is controlled by reptile like behavior which happens well before the perception of brain is developed about what happened or when walking through a hilly area; the behavior gets more complicated and taking a decision to follow a ramp or climb a hill requires analysis [259]. Moreover, it is also known that learning a foreign language in the same culture is more efficient than learning in a different culture. This happens due to contextual awareness through learning that is accelerated in the same culture. Also, due to the presence of memory components, human brain use learning to improve performance of cognition and thus component of feedback plays an important role in adaptation of humans.

2.6.1.1 Complexity Analysis as a Cognitive Computing Tool

As discussed earlier, Cognitive Computing (CC) is an emerging research field capable of outperforming traditional artificial intelligence based state-of-the-art anomaly detection systems. It consists of tools and techniques that mimic or follow human cognition abilities, including but not limited to decision making, reasoning, comprehension, perception, inference and the human thought process. It constitutes probabilistic and statistical knowledge; theories of signal processing and dynamical systems; machine learning; natural language processing and multiscale analysis, to name a few [3]. The basic research motivation in this area is to improve traditional learning algorithms by mimicking the human brain and introducing models, which, not only learn through historical data (experience), but also, improve as a result of stimulus-response mechanism, which adapts with the changing environment and context (evolution). This is achieved by utilizing the concepts of complexity [3], which is defined as an important aspect of human's cognitive operations based on many interactions among the system's components which cannot be simplified further [260]. On the other hand, cognitive operations that involve fewer and limited relationships among components are considered simple [260]. So, ease in comprehending refers to simplicity in terms of human cognition, whereas difficulty in doing so is termed as complexity. It is note-worthy to understand that the simplest level of complexity cannot be further decomposed into simpler sub-systems without actually causing a damage to the system's dynamics [261]. Therefore, these notions are utilized to achieve tractability and robustness in the cognition process [3] [262].

Complexity has been defined in the literature from different aspects [3]. The author in [257] has categorized objects, systems and structures in two classes based on their interactions among themselves; mainly whether (i) they contain any type of order, which refers to the presence of a definite pattern or, (ii) they depict complete randomness, which indicates a lack of pattern and order. These patterns can be further classified as simple or complex. If the observed patterns involve interaction with fewer components, then it is considered as simple. Alternatively, complex systems have many components each of which interact with others in a variety of ways and may

contain some form of order or hierarchy among themselves, which further leads to the emergence of new patterns or behaviors. Similarly, from the perspective of dynamical system theory, the aggregate interactions in complex system give rise to the evolutionary behavior, which is responsible for new and unknown patterns, and this system cannot be further decomposed into independent components [263]. In the context of cognitive computing, complexity is regarded as (i) static, due to the fixed limited patterns in the system or object, (ii) dynamic, which refers the temporal behavior, (iii) functional, which is attributed to the system's functional components, (iv) organizational, which refers the degree of interaction among different components and, (v) design, which stems from the structural properties of the underlying system [264]. The author in [264] has discussed at length different complexity measures based on various system models. It can be categorized based on the scope, scale, statistics and fractality. Some of these include (i) mono-scale or multiscale, (ii) algorithmic or probabilistic, (iii) local or global, (iv) average or asymptotic, (v) arithmetic or logical, and (vi) absolute or differential.

In this dissertation, the concept of complexity is used to represent the dynamics of an operating system process tree temporally to characterize the presence of advanced and deceptive malware using fractal based complexity measures. Using various fractal dimensions, relevant degree of complexity is measured which provides detailed insight into the long range correlation relationship of the process tree objects at different measurement scales, which take into account both the local (measurement at multiple scale) and the global (combining multiscale relationships as an overall measure e.g. fractal dimension) changes in the system revealing the complexity of a system.

2.6.2 Cognitive Cyber Kill Chain

Using Cognitive Machine Intelligence, cyber security techniques can be transformed into an intelligence model where human brain inspired techniques can be used to detect sophisticated threats reliably. Every internet connected organization relies on cyber security professionals to thwart attacks. These professionals are typically categorized as cyber incident response (IR) and threat intelligence (TI) teams [265]. Some organizations rely on outsourcing the cyber security tasks to dedicated cyber security organizations to look after their network while other organizations employee local teams to do the security job (Cyber Security Operation Centers). Further, some organizations rely on both outsourcing as well as local cyber security experts and typically include banks, insurance companies and government offices. This methodology is called collaborative cyber security, whereby different cyber security expert entities share their expertise, knowledge and skills to stop unavoidable cyber threats. With the evolution of machine learning, cloud based data analytics and big data tools, cognitive cyber security has gained prominence to detect ever increasing sophisticated threats. Cognitive cyber security based first prominent application is attributed to IBM which developed the first cognitive computing infrastructure called IBM Watson [266]. With the evolution of open source Hadoop infrastructure, big data analysis has become easier, faster and near-real-time, thus, making possible the mining of large amount of data using machine learning to find correlation among various components of the network data including but not limited to network packet captures, firewall log and operating system logs. [267].

Cyber security is a complex research domain and involves various heterogeneous aspects of the data and network including the user behavior and the analysis of mental model of the threat actors. It is necessary to incorporate complexity measurement in the cognitive data analysis for the detection of threats adaptively and dynamically. It is required to understand the intellectual model of the threat actors and how they bypass existing security defenses. Expertise of cyber professional experts is required to be incorporated in the cognitive analysis of threats. Although, traditional cyber kill chain is an abstract model but in the current era of high speed evolution of cyber threats, a modification is required to incorporate additional details of cognitive aspects. Therefore, various stages of the cyber kill chain should be combined into following 4 categories:

1) External and internal reconnaissance for exploitation of security weakness (**R**).

2) Delivery of the payloads (**D**).

3) Develop persistence to hide from the security radar using mutation (**P**).

4) Command and control communications from the network and lateral movement within the network using endpoints/computing nodes (**CnC**).

As shown in Figure 30, a cognitive time series of the proposed model is shown conceptually. If the time series is divided into N time steps, then each step constitutes a four phase cycle of the proposed four stages of cyber kill chain. An object could be a network trace, server logs and packet captures. Moreover, the same object can be analyzed at multiple time steps but all the 4 stages are considered concurrently at each time step. Threat actors are capable of incorporating mutation [26] in their attack techniques at each of the 4 stages and therefore, any cognitive security system should also be able to focus on these categories concurrently [268]. In order to analyze a threat object, an analyst will not only look at the current indicators of compromise and indicators of attacks but will also analyze how a threat entered the network and what system/network defenses are compromised. Further, if a threat intelligence expert analyzes possibility of a future attack, then not only the objectives and actions of the threats are analyzed but the method of threat delivery and the techniques of those delivery mechanisms will be investigated as well. Compounding the analysis efforts, threat actors are also changing their techniques by making them stealthy [29]. This is being done to evade cyber defense mechanisms which correlate data anomalies against normal data. In addition, threats are able to spread laterally and thus pose extra challenge of analyzing infection locally and globally both. Therefore, the proposed model depicts an efficient and fast method of analyzing objects which is close in human thought process as well.

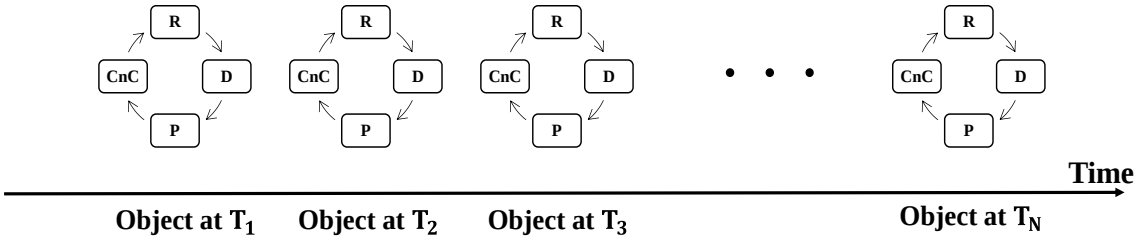


Figure 30: Proposed cognitive analytical kill chain model for simultaneous analysis of data.

It is noted here that the four stages of the proposed cyber kill chain model, R, D, P and CnC are not necessarily evaluated or considered in the order as shown in Figure 30; however, a security expert may use these four stages concurrently to analyze an incident. With the traditional cyber kill chain model, it is observed that forensic analysis should begin with the first stage of reconnaissance, which is not possible without knowing the details of the attack. Further, other stages cannot be analyzed until the malicious activity is analyzed first. It may be argued that traditional cyber kill chain model can be modified for forensic analysis by switching stages according to priority and available evidences. Nevertheless, there are two problems with this approach; (1) with the state of the art available tools for threat activities and the rise of attacks having targeted motivation (political or economic), all the seven stages cannot be differentiated and analyzed separately. Adversaries execute reconnaissance stage keeping in view their weaponization and exploitation capabilities. Therefore, in the proposed model, reconnaissance, weaponization and exploitation stages of traditional kill chain model are grouped in one reconnaissance stage, (2) traditional cyber kill chain treats threat analysis as a sequential analysis model while humans analyze attacks concurrently for all the stages of a cyber kill chain. Therefore, with concurrency, the proposed model more closely complies with a human mental model of analysis.

2.6.2.1 Examples of the Cognitive Analytical Kill Chain

In this section, two examples are presented to elaborate the effectiveness of the proposed cognitive kill chain. These examples demonstrate that the conventional kill chain would be more effective if the proposed concurrency would be added and used.

In almost every organization having a cyber-security team, there are multiple layers of technologies deployed for cyber security. For example, in a hypothetical ecommerce organization, there are network defenses and endpoint defenses. Further, this organization follows an automated mechanism of patching the operating systems and software. There are multiple firewalls deployed for network defenses. Anti-phishing software is also installed over email gateways. There are antimalware systems installed on endpoints with strict domain level access controls. There are various data orchestration and analysis tools which ingests the data coming out of these defenses and provides an aggregated and human comprehendible view for the IR team. As almost all the tools work on known signatures or traces, threat actors look for new ways to enter this organization network consistently to perpetrate a zero-day attack.

Example 1 – Phishing emails

Threat actors craft and send a very deceptive phishing email with a malware attachment disguised as a marketing brochure to the finance department of this organization, alluring them to download this attachment. It is noted that the finance department can be an easy prey for such phishing campaigns, since they are non-cyber-security professionals. Let us assume that the installed anti-phishing tool cannot find any known detectable patterns (signature of known regular expressions) and the email reaches the users' inbox. Unless, a user is intelligent enough to find this email suspicious and convey this to the IR team or the signatures are updated by the security vendors, there is no way that the IR team could know about it. Therefore, this is a zero-day attack. In either case, as soon as the IR team come to know the existence of such emails, they start performing standard preventive actions as follows:

a) They quarantine the infected computers for further forensic analysis.
b) They issue a warning message to everyone in the organization to avoid being a victim of such emails.

It is an established practice in Incident Response team to identify, analyze and respond to the incidence in a timely manner to minimize damage and reduce the associated cost [269]. Therefore, it is of paramount importance for IR teams to monitor the network traffic, computer logs, endpoint activities and other related data to look for attacks. This includes observing traces of reconnaissance, e.g., port scanning activities, DNS traffic, and user behavior analytics. In the event of an attack incidence, the IR team performs forensic analysis of the victimized computers [270], and does not only look for traces of malicious patterns in the quarantined computer, but also analyzes why the email went through their defenses undetected. At this stage, they do want to ensure that such emails should not go through their defenses again; therefore, they also find a way to update firewall rules. Further, based on the type of analysis, experts do want to see how the infected computer is trying to establish communication with outside servers including legitimate and unknown servers. Also, it is investigated to find if the infected computer has communicated internally with other computers and servers of the organization. If this process is mapped with the traditional kill chain model, the experts would be required to look for all the seven stages of the kill chain, sequentially, which, however, is not a cognitive approach. Therefore, the IR team performs a concurrent investigation, as follows:

a) the malicious payload (D),
b) traces of malicious communication with other computers and servers (CnC),
c) analyzing the possible ways of how the phishing email reaches successfully to the finance department bypassing all the defenses (P),
d) and what was the email content that attackers used to lure the users (R).

Example 2 – DNS Denial of Service (DoS) attack

For the next example, let us assume that in the hypothetical ecommerce organization cyber experts observe an abnormally high DNS traffic rate and receive complaints from their users of slow browsing. After initial analysis, it is discovered that the organization's DNS servers are facing

enormous traffic from legitimate internet servers. It could be a signal of a botnet based DoS attack [12]. However, further analysis may be required since the servers host online shopping websites and are connected to the organization for daily business operations. Typically, DNS based rate limiters are applied to reduce anomalously higher traffic; however, it may hurt the business operations if the rise in traffic is due to legitimate reasons, e.g., legitimate increase in traffic due to online shopping during the holiday season. Therefore, security analysts first acquire the traces of the DNS traffic packet capture files/logs, look at the payload and IP addresses (CnC) and try to figure out if the traces conform to normal DNS communication (D), e.g. is there any repeated resolution of DNS name. Further, analyzing the IP address field, they look for the source of traffic and look for any anomalous patterns. For example, if the DNS requests do not have legitimate payload consistently, then the traffic is a DoS attack, because attackers may have used garbage payload or no payload for such DoS attacks. In addition, they will look for potential weaknesses of the system which can be exploited for this DoS attack, e.g., if DNS servers are updated with DNSSEC extension to ensure that valid DNS communication should be passed through the server (R). Further, they will also evaluate if the attack is showing any sign of persistence (P), e.g., if the DNS based DoS attack keeps changing the bot servers, since this will be very hard to stop an attack immediately using firewall black lists. This investigation process to find indicators of threats is an iterative process and involves four distinct stages of finding an attack iteratively as mentioned in this subsection. Traditional Cyber Kill Chain model does not hold valid as it looks for all the seven steps in a sequential and non-iterative manner. Therefore, the proposed concurrent model resembles the cognitive analysis process of cyber experts more closely.

2.6.3 Fractals as a Complexity Measurement Tool

2.6.3.1 Significance of Scale in Complexity Analysis

The quantifiable extent of an object, process or system may be represented and measured in terms of scale. Scale signifies the relative fragility and roughness of various attributes and features of an object. It also determines the resultant selectivity of patterns that can be formed by the observed data. Therefore, scale behaves as a filter, or a window of perceptions which provides an analytical basis for observed data. The larger the window size, the coarser the details will be and vice versa. Moreover, scale is responsible for setting the analytical bounds of an observation; thus expressing the consequential extent to which a data set can be modeled and analyzed. For example, in the domain of cyber-security, a set of network related alerts produced by a learning algorithm can be extended to incorporate host related alerts. It can be scaled to assess emerging attack patterns, or it can be further divided into different categories of attacks to find related mitigation vectors. The relationship among different details with respect to the hierarchy of scales determines the complexity of an object. This scale based relationship depicts the emergence between structures and processes through interactions across a variety of spatial and temporal scales. For instance, the change in the behavior of a network entity under a cyber-attack is influenced by interactions at finer scales of different packet based features e.g. total flow duration and the total amount of bytes exchanged. Typically, malware tends to stay low and slow (stealthy) to evade detection, which implies that only finer scales can reveal this type of interactions and may not

otherwise be observed on coarser scale levels. The concept of scale is useful for the modelling of an observation by scaling the observation at different levels, or it can be considered as the characteristics of a process itself and thus aiding in the system analysis. For example, packet inter-arrival time and total packets exchanged in a flow are two features which can be observed at multiple scales for network based communication. Similarly, to characterize the stealthy malware behavior in a temporal host based process tree, process node based features can be analyzed at multiple scales to observe malware activity pattern which is mimicking legitimate process tree behavior but otherwise executing malicious activities which are different from the legitimate process name misused by the malware. Moving from the coarser to the finer scales, the data samples reveal the delicate differences in benign and malicious samples, which provides underlying patterns and thus helps in modelling them. Otherwise, over single scale analysis, the distribution of the attack samples is indistinguishable from the distribution of normal data samples, as observed in Figure 22 to Figure 29. This is due to the fact that attack samples follow the same behavior as of normal samples. Moreover, this information can be used to deduce inference about the malware detection process itself, which is based on cross-scale interactions.

2.6.3.2 Single Scale vs Multi Scale

Traditional single scale based analysis of a system or process involves measuring the parameters of a system at a global or macro scale. For example, measuring variance of an observable object finds the average squared deviation of object from the mean value. In contrast, multiscale analysis takes into account micro level details from various localized temporal, spatial, and regularity scales. Multiscale analysis combines information within and across different scales of an object. The primary importance of this approach is attributed towards the characteristics of finer scales, which provide granular level details, while coarser scale lacks in providing the sufficient details required for the substantial analysis and modelling of a complex system. Multiscale analysis is computationally more expensive than single scale analysis; however, in the domain of cyber-security, the former is critical for the successful classification of advanced threats, whose features overlap each other in a given feature space, and are, therefore, non-classifiable on a single scale using any linear or non-linear learning algorithm on the available features. In addition, multiscale analysis is significant for the measurement of the nature of cyber data, which is known to be fractal in nature [271] [272] [273] that is characterized by having the scaling property, thus requiring analysis on multiple levels to describe and characterize its complexity, with high fidelity.

2.6.3.3 Complexity Analysis Using Fractals

Fractals are characterized as multiscale objects which are non-differentiable everywhere. They have unique and fascinating scaling properties such that the portion of an entire object like a geometrical figure, a process or a time-series is a scaled down version of the whole. In other words, Fractals are invariant to magnification along multiple scales, which can be either symmetrical or asymmetrical and hence, are referred to as self-similar or self-affine, respectively. Self-similarity (or self-affinity) and long range correlations are properties of fractal objects. Complexity analysis

using fractal theory provides measurable and quantifiable measures of complexity which is applied in wide areas of science and engineering.

Fractals provide a cognitive method of measuring complexity of objects using multiscale analysis and are mathematically elegant in the sense that fractal dimensions are always embedded within the topological dimensions of the multiscale object under study. As it is already established that finding a feature set where data can be uniquely classified for threats is becoming difficult due to advancement in threat landscape, therefore, fractal analysis is a promising candidate in detecting advanced and stealthy threats. This is because fractals are able to find a long term correlation based relationship among various scales of an object and thus provide a unique way to analyze patterns of an attack following behavior of legitimate objects, which is both mathematically tractable and convenient algorithms are available for implementation. For example, the authors in [274] illustrated the fractal dimension of the DNS time series in which DDoS attack pattern clearly follows a change in fractal dimension and hence complexity of the time series. Also, it is possible for humans to visually analyze this discriminating pattern which is not possible through traditional mono-scale machine intelligence tools. Another approach of multiscale analysis is adopted by researchers in [275] [276] [277] where self-constructing and re-organizing neural networks having fractal structures have been discussed. This particular property has resulted in better learning capabilities compared to the traditional neural networks as it is based on the connection in biological systems. Further, a unique multiscale based k-Nearest Neighbor algorithm (k-NN) was proposed in [11] which was able to detect latest advanced persistent threats (APT). Hence, fractal based techniques and algorithms are proving to be more robust and reliable to perform tasks that require cognitive capabilities either because of the presence of multiscale distribution of information or highly complex data analysis requirements.

2.6.3.4 Fractal Dimensions to Measure Complexity

Fractal theory as a subject was introduced by Mandelbrot in late 1970's [278]. Fractals are objects which exhibit self-affinity when viewed or analyzed at multiple scales. Fractals can be categorized as morphological fractals and information based fractals [274]. Morphological fractals are objects which render self-affinity geometrically. They can be viewed visually. However, for entropy based fractals, self-affinity is analyzed statistically only. In this work, we discuss only information based fractal. A detailed description of fractal types is available in [279].

In order to analyze a fractal object, the concept of fractal dimension is necessary [274]. In traditional Euclidean geometry, a line has a dimension of 1 and a plane is represented by 2 dimension. These are also called topological dimensions. Topological dimensions does not take into account the irregularity or complexity of an object and thus remain constant. For example, border of Canada and United States is a 1 dimensional object irrespective of how irregular the border is. Similarly, border of Mexico and United States has a topological dimension of 1 which makes both north and south border of United States similar. However, this is not true.

Fractal dimensions are different from topological dimension and consider the irregularity aspect. For instance, a rectangular box has a topological dimension of 2 but if the box has twists and warps, its fractal dimension is between 2 (area) and 3 (volume). If it has more twists, its

dimension will approach 3, closer to a volume. Fractal dimensions are non-integer and higher fractal dimension represents higher complexity or irregularity of the object.

Mandelbrot [278] defines fractal dimension as; "A fractal will be defined as a set for which the Hausdorff-Besicovitch dimension strictly exceeds the topological dimension". Hausdorff-Besicovitch dimension calculates an exponent of similarity when an object is magnified by a fixed scaling factor multiple times. This similarity exponent is equal to a topological dimension when it is a regular object having no complexity and exceeds the topological dimension when there are irregularities or fractalities [280].

Because self-affinity (self-similarity) and irregularity are related using fractal dimension which is measured at multiple scale, therefore, Hausdorff dimension can be modeled as follows:

$$D_H = \lim_{r_k \to 0} \frac{\log(N_{r_k})}{\log(\frac{1}{r_k})} \quad (1)$$

Subscript "k" is used to signify the importance of multiscale measure. For example, at first scale r_1, divide a curve into $N_{r_1} = r_1$ volume elements (or vels) where each vel will have a size of $\frac{1}{r_k} = \frac{1}{N_{r_k}}$. Then calculate the number of vels which intersect the object at scale k = 1. This is repeated for all scales k =2, 3, 4. If the calculations in equation (1) forms a straight line over a log-log scale, the object is called as a mono-fractal. An example of morphological fractal curve is shown in Figure 31. This is a Minkowski curve generated for a multiscale depth of 5 scales [274]. Figure 32 shows the log-log plot of equation (1) for Figure 31. Slope of Figure 32 is D_H in equation (1). As can be seen, Minkowski curve in Figure 31 is not a single dimensional line in topological sense. It demonstrates irregularity and has a Hausdorff dimension of 1.5 which is also the slope of log-log plot in Figure 32. Therefore, this curve is complex than a single line but simpler than an area (2-dimensions).

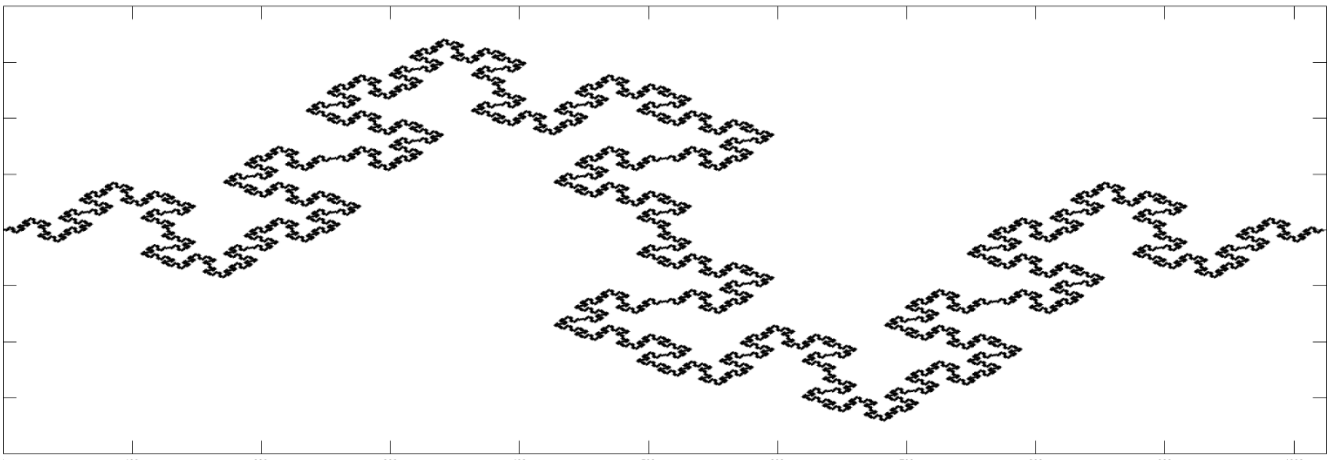


Figure 31: Minkowski fractal curve generated with 5 scales.

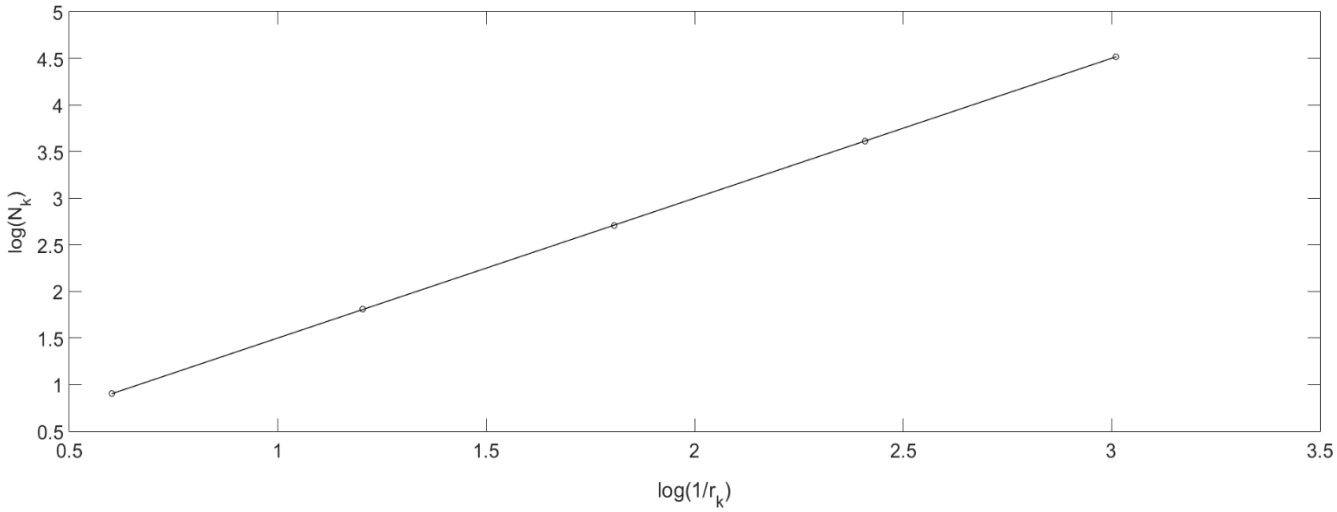


Figure 32: Log-Log plot of Minkowsky fractal curve.

There are many types of morphological fractal dimensions e.g. mass dimension, gyration dimension and Minkowski dimension. However, they are all morphological dimensions and characterize the morphology (shape and geometry) of fractal objects. Information or entropy based dimensions are based on statistical self-affinity of an object e.g. time series. Like Hausdorff dimension for morphological objects, where number of intersecting vels are counted at successive scales, information based fractals utilize the statistical information about the distribution of a measure over spatial fractal or time behavior of a dynamical system [281]. There are many information based fractal dimensions and this dissertation considers Shannon Information fractal dimension, correlation fractal dimension, variance fractal dimension and spectral fractal dimension, In fact, as probabilistic measures are defined by their statistical moment generating function, therefore, there are infinite number of information based fractal dimensions as there are infinite statistical moments.

1) Shannon Information Fractal Dimension

Information based fractal dimension provides Shannon entropy based probabilistic dimension measured at multiple scale using entropy [1]. For a given fractal, probability of intersection of a particular vel at a specific scale is considered in the fractal dimension calculations. Let us define:

$$p_k = N_k r_k \tag{2}$$

where p_k is the probability that a vel of size r_k intersect the object at scale k.

$$N_k \sim \left(\frac{1}{r_k}\right)^{\propto} \tag{3}$$

where $r_k \to 0$, k= 0,1,2,3,…

Therefore, Shannon Information dimension can be defined as:

$$D_I = \lim_{r_k \to 0} \frac{H_k}{\log(\frac{1}{r_k})} \tag{4}$$

where H_k is the Shannon entropy function and is defined as.

$$H_k = p_k \log(p_k) \tag{5}$$

2) Correlation Fractal dimension

Correlation fractal dimension [14] of a fractal object is defined as:

$$D_c = \lim_{r_k \to 0} \frac{-\log(Corr_k)}{\log(r_k)} \tag{6}$$

where, $Corr_k$ is the correlation of samples x_i and x_j at scale level k and is defined as $\lim_{N_{r_k} \to \infty} \frac{1}{{N_{r_k}}^2} \{ \sum_{i,j=1}^{N_{r_k}} \text{HeavisideFunction}(r_k - |x_i - x_j|) \}$ [14] [217]. In order to compute D_c, slope of the least square estimate (LSE) of the log-log plot is computed which represents an estimate of the correlation fractal dimension [217]

3) Variance Fractal Dimension

Variance Fractal Dimension (VFD) is an information based fractal dimension that extracts the variance feature of an object. VFD is calculated by using the Hurst Exponent (also called as Holder exponent) which is characterized by fractional Brownian motion process (fBm). A fBm $\{B_t, t \geq 0\}$ is a self-similar stochastic process that has stationary increments. A fBm is governed by Hurst parameter $H \in [0,1]$. The stationary increments have a normal distribution with zero mean and variance that is dependent on the time step t. As $H = \frac{1}{2}$, fractional Brownian motion process is called standard/ordinary Brownian motion process and the stationary increments also become independent [282].

Let $\{B_t, t \geq 0\}$ is defined as a fractional Brownian motion process of Hurst parameter $H \in [0,1]$ with zero mean and covariance function as follows [12]:

$$E(B_t B_{t+\tau}) = \frac{1}{2}((t+\tau)^{2H} + t^{2H} - |\tau|^{2H}) \tag{7}$$

where $H = \frac{1}{2}$, $E(B_t B_{t+\tau}) = \min(t, t+\tau)$ [283], which is the covariance of a zero mean Gaussian process and represents the independence of increments which is the property of standard Brownian motion process. Also, it can be seen that where $H \neq \frac{1}{2}$, the increments are not independent. VFD calculation is performed using power law relationship between the amplitude increments of the time series. It is imperative to note that the time series is required to be stationary in the statistical sense for the valid calculation of VFD. Therefore, a sliding window of data samples is chosen for VFD calculation such that the stationarity is ensured in the weak sense and a trajectory of the VFD is obtained which varies within the embedding dimensions of the time series. This trajectory is called Variance Fractal Dimension Trajectory (VFDT) [13].

Let x(t) represents a data time series which is sampled at equal intervals. Therefore,

$$\text{Variance} = \text{var}[x(t)] = E[(x - \bar{x})^2] \tag{8}$$

where E(.) is the statistical expectation operator and $\bar{x}$ is the statistical mean (first moment) of the processes x(t). Therefore, according to power law:

$$\text{var}[x(t_2) - x(t_1)] \backsim |t_{2-} t_1|^{2H} \tag{9}$$

$$\text{var}[x(t_2) - x(t_1)] = \text{var}\,[\Delta x_{\Delta t}] \tag{10}$$

Let $$x(t_2) - x(t_1) = \Delta x_{\Delta t} \tag{11}$$

Then $$\log(\text{var}[x(t_2) - x(t_1)]) \backsim 2H\log\,[\Delta t] \tag{12}$$

Therefore, Hurst Exponent (H) is:

$$H = \frac{1}{2} \lim_{\Delta t \to 0} \frac{\log[\text{var}(\Delta x_{\Delta t})]}{\log(\Delta t)} \tag{13}$$

The variance dimension (D_σ) is calculated using H as:

$$D_\sigma = E + 1 - H \tag{14}$$

where E is the embedded Euclidean dimension.

In the case of single Euclidean dimension, i.e. single independent variable, we will have $E = 1$. Therefore,

$$D_\sigma = 2 - H \tag{15}$$

So for a data time series with one measurable parameter (feature), D_σ varies between 1 and 2. If D_σ=1.5, the process will represent standard fractional Brownian motion (fBm) [283]. When D_σ=1, the process is not showing any multiscale complexity and can be referred as a mono-fractal. When, D_σ = 2, the process is equivalent to a white noise process.

4) Spectral Fractal Dimension

Spectral fractal dimension analysis [7], which is an extension of variance fractal dimension analysis [279], is a class of statistical/information based fractal dimension analysis where second order frequency analysis using power spectral density (PSD) is performed at multiple scales and a relationship among those scales is found simultaneously using log-log relationship of multiple scales [279] [284].

If a time series is a self-similar (or self-affine) fractal, the power spectrum density satisfies the following power law [7] [284] [281] [285]:

$$P(f, T) \sim \left(\frac{1}{f}\right)^d \tag{16}$$

$P(f, T)$ represents the power spectrum density of the time series as a function of the frequency and the window time T of the time series over which power spectrum density is calculated. Exponent **d** represents the slope of the least square fit of the line over power spectrum density plot. As shown in Figure 33, a line of slope 1 represents a negative dimension over a PSD plot. This happens because, one sided PSD plot is considered to estimate the best least square fit which is a negative slope line. Therefore, it is required to reverse the sign in our calculations to ensure that dimensions remain positive. It is equivalent of considering the single sided negative frequency spectrum e.g. Figure 35 and Figure 36.

As shown in Figure 33, lines having varying slopes over a log-log plot of PSD are shown [7] [286] [279]. If the exponent of the equation (1) is −1, then the resulting PSD would be of blue noise where higher frequency components are amplified. Similarly, if d=0, then the resulting PSD would result due to white noise. If the frequency exponent is 1 then it represents PSD of a pink noise. For d=2, PSD is generated from brown noise or standard Brownian motion process. For d=3, it becomes black noise. Also increasing d from 1 till 3 will result in increasing attenuation of higher frequency components and the correlation will increase. Black noise is also called as broadband noise.

Moreover, this noise phenomenon is also called integer noise [7] [287]. There are fractional noises that are not integer and lie between these integer limits. For example, if the exponent lies between 1 and 3, it is called fractional Brownian motion process [287]. As an example, Figure 34 shows a PSD plot of a Gaussian pulse while Figure 35 shows a one-sided plot of the same PSD plot. In order to find the spectral fractal dimension, Figure 36 shows a linear fit of the log-log plot of single sided PSD. Slope of this line is the magnitude of the exponent of equation 1. As there is only a single slope of the log-log plot of single sided PSD, this process is called a mono-fractal.

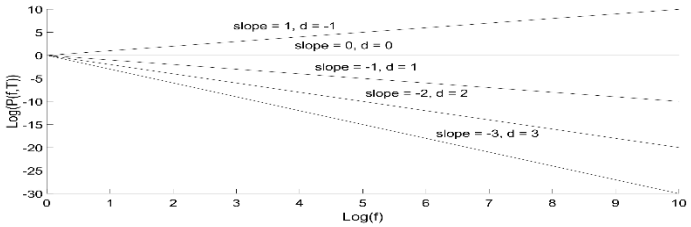


Figure 33: Slopes representing various spectral fractal dimensions (SFD).

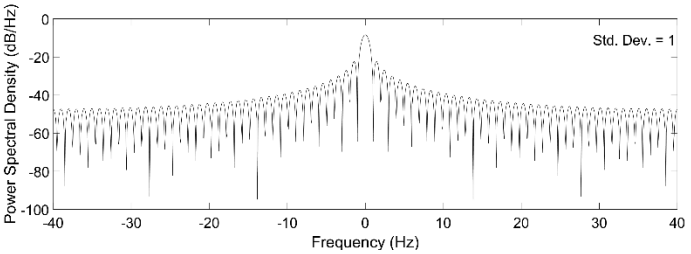


Figure 34: A double sided Power Spectral Density (PSD) of a Gaussian pulse.

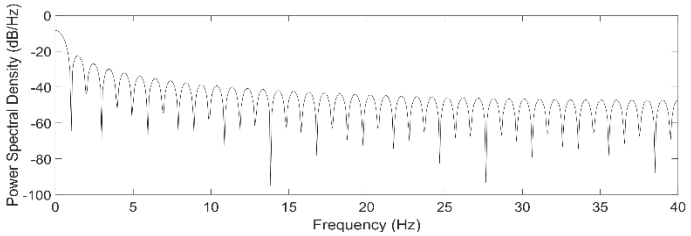


Figure 35: A single sided Power Spectral Density (PSD) of a Gaussian pulse.

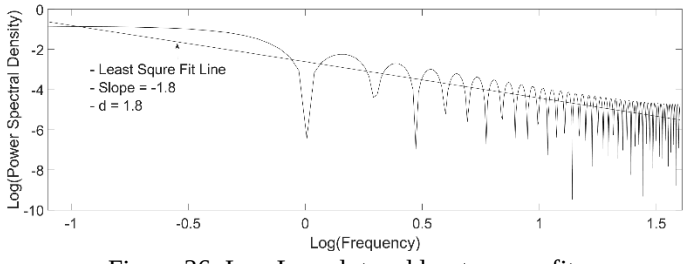


Figure 36: Log-Log plot and least square fit.

In order to find the spectral fractal dimension, following is the relationship between slope and the fractal dimension [286] [284]:

$$D_s = E + \frac{3 - d}{2} \tag{17}$$

where E is the number of dimensions or number of features represented by the time series. In this work, E =1, since there is one feature of the time series i.e. DNS packet count. Therefore, equation (17) is reduced to:

$$D_s = \frac{5 - d}{2} \tag{18}$$

Therefore, in this work, if spectral exponent is in the range $1 < d < 3$, then the spectral fractal dimension accordingly falls in the range $1 < D_s < 2$.

2.7 Application of Graph Theory in Malware Characterization

Graph theory deals with the collection of objects and their relationship. In graph theory, objects are called as nodes and the relations are represented using edges. Graph structure is a natural candidate in cyber security, where dependencies among various attributes of data can be analyzed. In this work, host based operating system process tree structure is transformed into graph nodes and edges to characterize the malware behavior. This subsection provides a brief overview of graph theory and literature survey of available graph based malware characterization techniques.

2.7.1 Graph Theory Definitions

A ***graph***, G, is defined as a pair of set of vertices (nodes) and edges. Mathematically, it is denoted as follows:

$$G = (V, E) \tag{19}$$

where, V is a non-empty set of vertices and $\boldsymbol{E}$ is the set of edges which is also a two element subset of $\boldsymbol{V}$ [288]. The total number of vertices in a graph, which is also the cardinality of the set $\boldsymbol{V}$, is referred to as the ***order*** of the graph [289]. Moreover, the number of edges incident on a vertex in a graph is called the ***degree*** of the vertex

If the set of edges, $\boldsymbol{E}$, consists of ordered pair of elements of $\boldsymbol{V}$ i.e. vertices set, then such graph is called ***directed graph or digraph*** [290]. On the other hand, ***undirected graphs*** are characterized by having a set of vertices V and an unordered set of edges, $\boldsymbol{E}$ [290]. Directed graphs (Digraphs) are signified by edges having particular orientation which implies that the possible traversable path is from origin to destination and not the other way round. Also, these digraphs are used to represent hierarchy in objects. For example, when a user opens up an application, a process $\boldsymbol{p}$ initiates which later may access a particular module $\boldsymbol{m}$. So, the communication between process and module can be represented with a directed graph depicting the hierarchy in invoking procedure.

Further, if a graph consists of exactly one edge between each pair of distinct nodes then it is considered a ***complete*** graph [291]. However, if it has repeated elements in its set of edges, then such type of graph is called ***multigraph***. Basically, these graphs have two or more edges between a pair of vertices. If the edges are directed these are called **directed multigraphs** in which case, the edges have the same origination and destination vertices. While, the edges in the multigraphs are simply arcs i.e. they do not have an orientation. Also, sometimes the graphs have edges that connects a node to itself thus, forming a ***loop*** [292]. Some texts consider loop as part of the multigraph while others call such graphs ***pseudographs*** [292]**.**

Before actually navigating a graph, it is important to understand its connectivity. A graph is considered ***connected*** if a path exists which connects every pair of its distinct vertices [293]. This scenario can be observed in a set of computer nodes which can only communicate if they are connected. On the other hand, an ***unconnected*** graph is a union of two or more connected sub-graphs such that each of them has no pair in common [294]. Moreover, a graph can be traversed in a number of ways. One of this traversal method is called ***walk*** which is defined as a sequence of vertices i.e. $v_1, v_2, v_3, \dots, v_n$ where $v_i, v_{i+1} \in E$ for $i = 1, 2, \dots, n-1$. Also, a walk with distinct vertices is called ***path*** and that with a distinct edges is called ***trail.*** A path that begins and ends at the same vertex is called a ***closed path*** or ***cycle*** and the one that does not exhibit this property is considered ***acyclic*** in nature [295]. Similarly, a trail which exhibits this property i.e. its starting and ending vertices are same then it is known as ***closed trail*** or ***circuit*** [292]**.** Graph traversal concept is widely used in modeling scenarios such as the routing of a network packet on internet.

There are many different methods of representing a graph, the simplest of which is to list all the edges. For instance, using adjacency list is a way of describing the connections in a graph. This is tabulated by listing all the vertices adjacent to each of the vertex in the graph. However, this approach becomes impractical for larger graphs. Therefore, matrix based representations like **adjacency matrix** and **incidence matrix** are more widely used.

Consider a graph $G = (V, E)$ having n number of distinct vertices enlisted as $v_1, v_2, \dots, v_n$. The ***adjacency matrix*** A of G is a $n\,x\,n$ zero-one matrix, such that each of the $(i,j)th$ entry is determined mathematically as [296] [297],

$$a_{ij} = \begin{cases} 1 & if\ \{v_i, v_j\}\ is\ an\ edge\ of\ G \\ 0 & Otherwise \end{cases} \tag{20}$$

There are $\boldsymbol{n}!$ different ways of ordering the vertices and hence, $n!$ various adjacency matrix are possible. Also, for an undirected graph which does not have a loop, the adjacency matrix is symmetric.

Another interesting approach of representing the graph is through incidence matrix. Consider a graph $G = (V, E)$ having n number of distinct vertices enlisted as $v_1, v_2, \dots, v_n$ and m number of edges enumerated as $e_1, e_2, \dots, e_m$. The incidence matrix M of the graph G is a $n\,x\,m$ zero-one matrix such that each of the $(i,j)th$ entry is determined mathematically as [296] [298],

$$m_{ij} = \begin{cases} 1 & when\ edge\ e_j\ is\ incident\ with\ v_j \\ 0 & Otherwise \end{cases} \tag{21}$$

It is possible to represent multiple edges and loops using incidence matrix. The columns which have similar entries in an incidence matrix represent multiple edges while loop is designated with a column having exactly one entry as 1.

Another important concept related to the adjacency relationship of the graph is ***isomorphism*** where two graphs are characterized as having a one-to-one correspondence between their vertices and are

thus, termed as isomorphic. Formally, it is defined by comparing two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ such that a one-to-one and onto function f exists from V_1 to V_2 which preserves the adjacency for all $a, b\ in\ V_1$ [276].

The isomorphism of a graph G to itself is called ***automorphism*** [299]. In other words, it is a type of symmetrical transformation such that the vertex set of the graph is mapped onto itself which preserves the edge-vertex relationship. Formally, automorphism of a graph $G = (V, E)$ is defined as a permutation $\boldsymbol{f}$ on the vertex set $\boldsymbol{V}$ such that an edge is formed by the pair of vertices (a, b) if and only if the pair of vertices $(f(a), f(b))$ also form an edge. For an ***asymmetric*** graph, any other automorphism does not exist. On the other hand, a graph is considered ***symmetric*** if it is both vertex and edge transitive [300]. However, there are graphs which are sometimes vertex and edge transitive but are not arc-transitive. Therefore, graph is considered symmetric if the automorphism set is transitive for edges having direction.

A special type of connected graph which does not have a cycle is called ***tree*** and a disjoint set of trees is called ***forest*** [294]. The edges of a tree are called ***branches*** [297]**.** Also, a tree is characterized as a connected graph which has $\boldsymbol{n}$ vertices and $\boldsymbol{n - 1}$ edges. Sometimes, one of the node of a tree which does not have a parent but may have child nodes connected to it is designated as the ***root*** of the tree. In such root based trees, every edge is directed away from the root. Also, every node has only one parent node which is the vertex closest to the root. A node may have zero or many child nodes which are adjacent vertices farthest from the root. The node without a child which is usually the terminal node and has a degree zero is called a ***leaf*** [301] while the one which is not a leaf is called ***interior node.*** All the vertices which share the same parent node are called ***siblings***. In a rooted tree, the ***depth or level*** of a vertex is its distance from the root which is described as the length of its unique path from the root. The root itself has a depth of zero. In addition, the greatest depth of a tree which is the longest path from the root to the leaf is called tree ***height***. All the nodes along the path from the root to a particular node v are considered the ***ancestor*** of node v. Similarly, all those nodes which are along the path from a particular node v to the terminal node are called ***descendants***. Further, if the children of each internal node in a rooted tree have fixed ordering, then such trees are called ***ordered rooted tree.*** Generally, the ordering is from left to right which implies that an ordered binary tree has a left subtree and a right subtree [302].

2.7.2 Graph Theory in Malware Characterization and Detection

The abundance of internet based devices and the resultant growth of the internet traffic in terms of Volume, Velocity, Veracity and Variety [219] is responsible for creating complex datasets which are difficult to represent, observe and analyze. This difficulty serves as an opportunity for the threat-actors to invade the computing devices and obscure the execution of their malicious plans. However, the malevolent activities also leave some data footprints which gets mixed up with the data generated by legitimate activities both on the network and the computing node thus

creating a multi-dimensional dataset which has intricate hidden patterns referring to the inter-dependence of various underlying entities. To detect a malicious activity, these inherent relationships are evaluated for which graphs are used that are powerful mathematical tools for capturing interdependence structure in the dataset [303] [304]. To elaborate, consider the user-activity graph data generated in a corporate firm to detect an attack that depends on whether the malicious action was caused by an insider or an outsider. This is also linked to the type of attack, since if it is an outsider attack usually, the target will be a complete disruption of network resource accesses, while an insider may launch an attack through internal computing node. In addition, it is also related to the target and the time of the attack which in case of an outsider will probably be during the peak business hour to cause maximum damage but for an insider an attack outside the regular office hours is more anticipated. Moreover, it is connected with the statistics of user vs. operating system activities both on the node and the network which in turn depends on the usage of administrative privileges. This is further dependent on the accessed resources and so on.

Using graphs for the characterization and detection of regular and irregular patterns in different fields of study is considered reliable and robust because of the following reasons [303] [305] [306] [307]:

In the presence of complex relationships between multi-dimensional dataset, as discussed above, graphs can capture the long-range linkages thus, revealing the hidden patterns. These datasets are not only limited to the cyber-space, rather are omnipresent in our surroundings as well. For example, social networks, human brain structure, electrical power grids, and internet [308] [309].

Graph is a powerful representation tool it captures the relationships using node and edges that depicts the connections between entities. Often, the directions and labels associated with the edges unveil the possible flow of information between nodes.

It provides a holistic view of the entire problem domain by connecting seemingly unrelated local entities together to form a global link which is helpful in tracing atypical patterns. Thus, graph provides a balance between the local and global analysis of the data.

A variety of basic and advanced graph related algorithms are available that can be used for the understanding and analysis of the graph. These algorithms have been implemented in different computing languages and therefore, can be used off-the-shelf. Further, graphs are represented as matrices which can be manipulated in an efficient manner using the available mathematical knowledge and computing tools.

Although, graph is considered a very useful machinery for representation, characterization and detection of anomalies, it has its fair share of challenges. The first one is attributed directly to the dependent nature of the graph structure which makes the odd configurations difficult to be separated from the regular ones, whereas, traditionally, the outlier data point are considered independent and identically distributed [303]. The graphical modeling of the problem plays a key role in such situation as the correct representation can easily accumulate anomalous samples into distinct graph substructures. Further, the complexity involved with the searching of graph space is huge because the possible solutions require a combinatorial investigation approach. Therefore, the efficiency and scalability needs to be carefully evaluated when applying graph based algorithms.

Also, the dynamic updates in time based graph require considerable memory space which means offline evaluation and analysis is much more typical with graph based approached [310]. In addition, with the growing sophistication in the development of cyber-threats, it is getting difficult to distinctly mark a behavior as anomalous as many of the advanced malware morph their behavior to that of the normal activity and hence, become difficult to be detected [311].

Detection of malicious activity using graph based techniques can be broadly divided into two main approaches i.e. static and dynamic depending on the type of underlying graph. The static methodology deals with determining the malignant graph entity i.e. node, edge or a subgraph in the entire network under consideration. In other words, due to the static nature of the graph only the intra-graph comparison of entities is possible. The graphical network can be labelled or unlabeled and leverages the patterns in (i) structural units or (ii) neighborhood/community of the graph to determine the anomalous objects [312] [313]. If the graph does not have attributes attached to it, then the major tactics of finding the structural patterns include, (i) using graph organization/anatomy based features, or (ii) graph proximity based features. The graph structure centric features involve using measurement data associated with edges, nodes or other substructures of the graph [314]. For example: degree of the node, eigenvector, diameter, common neighbors count, and reciprocity [315] [316] [317] [318]. On the other hand, the proximity based features exploit the relative closeness or similarity of objects in the graph. It encompasses the correlation of graph entities with each other to combine them in similar groups or classes. For instance: Jaccard proximity, page rank [319].

The neighborhood or community based alternate strategy to determine the malicious events in graphs deals with the spotting of nodes and edges that do not belong to a particular group but have rather connection with the other sub structures [316] [320] [321]. In this situation, the determination of malignant activities can be viewed as finding the bridge node or edge between different groups which serves as a building block to form intrusive connections. An example of such scenario exists in the cyber-space where the attacker morphs and tries to blend its malicious actions with the normal activities by establishing connections which appear to be legitimate. This gives rise to the relationships among graphical groups which appear to be connected but are not. So, these bridge nodes/edges can be interpreted as an attacker in disguise.

Similarly, for a labelled graph the techniques for defining a malevolent activity exploit either the structural or the neighborhood patterns. Generally, the substructures which happen to be present infrequently in terms of their connections or attributes are evaluated to find irregularity [322]. An interesting application of this approach is found in program execution flow graphs that can be used to determine the presence of malicious software on a computer system [323]. However, high false positive rates and specification of the application based threshold are the shortcoming of this techniques. Alternatively, the neighborhood based techniques are built upon the concept of clustering the nodes with respect to the correlation in the attributes and then finding the deviations in each group. Some of the algorithms consider performing the graph clustering and abnormality detection in an integrated way while others prefer it separately as a post-processing step [317]. Also, the advanced classification algorithms like neural networks are also based on graphical models and are able to reveal infer more intricate relationships among the entities using complex correlation techniques. Usually, the goal for these systems is to assign the data sample to a

particular class based on learnt linkages. For instance, this classification is useful in categorizing an incoming email as spam or not depending on the sender address, the email subject, words in the body, attachment details, and the size of the email. These convoluted features may have an underlying relation that can be inferred using these complex network models [324].

Graphs that evolve with respect to time are considered dynamic in nature and are basically a sequential array of static graphs [325] [326]. Detection of malicious events in such graphs involves determining the exact instance in time when the anomalous activity took place. This means finding the time when the graph appears to be different from its previous and following snapshots. Also, it includes finding all those nodes, edges, and substructures which contributed most towards the successful execution of events i.e. change detection. These graph structures often help in characterizing the evolutionary behavior of normal and suspicious activities in the graphical network. It is important to note that the occurrence of event in time is considered an isolated incident, while, a change point in the graph is the instance where the entire graph patterns alters and is continued till the next change point is observant [312] [327]. There are four different approaches to diagnose irregular activities in a dynamic graph which are discussed as follows.

The first one is based on the extraction of suitable features from each of the consecutive graph occurrences which are then compared using a similarity metric to generate a time-series [328]. Then a threshold based anomaly detection mechanism that may be manual or automatic is defined to characterize malicious events. Some commonly used graph similarity measures includes hamming distance, λ distance, median graph distance, vertex/edge overlap distance, and graph diameter [303]. An interesting application of this approach has been investigated in the study of changes occurring the communication network for performance monitoring. Similarly, to characterize a particular graph structure as anomalous its behavior over time is extracted and the moment it deviates from its usual behavior, it is categorized as anomalous. This behavior is established by extracting suitable features like node degree, and neighbor count from each of the consecutive graph instances. Then, these raw features are converted into a meaningful mathematical pattern that can convey information about the graph structure's behavior over various time windows. The values for these structures are typically computed using averaging concept which are then compared using a similarity metric to determine anomaly by assigning a score to each node [329] [330].

The second technique for finding malicious activity can be considered an enhancement of the first one which as discussed above requires features extraction as its first step. In this approach, the extracted information from the dynamic graphs is decomposed into a form which can be manipulated from a matrix or tensor perspective, for example, Eigen-value decomposition or Singular Value Decomposition (SVD) of graph features [331] [332]. A popular application of this method is found in the monitoring of multi-tier web-based systems. Further, tensors can also be used to represent the graph which are then decomposed and manipulated accordingly to detect unusual behavioral patterns at particular time [333].

Another important methodology in the context of detecting oddness in dynamic graphs is rooted in neighborhood or cluster based procedures which does not take into account changes in the entire network rather consider monitoring clusters over time for structural or contextual changes [334].

This is often related to the evolution of the cluster with respect to time that indicated the triggering of an event [335]. These techniques creates partitions of similar graph structures like nodes which are updated iteratively till until the optimum cost of the network is achieved [336]. In case of an attack, the new points in the cluster causes dissimilarity that lead to the creation of a new partition and hence, the possibility of an event. Research efforts to use the probabilistic models for the change detection has been explored. One such example is the usage of likelihood ratio test to determine the event instances which are characterized as causing serious alteration in the parameters of the fitted model for a cluster [337].

The final approach for the identification of a malicious event in time based graph sequences utilize the concept of time-windows to figure out the distinct behavioral pattern. The basic idea is to use the previous snapshots as a tool to establish normal behavior with which each incoming graphical instance is compared to be marked as regular or odd. A moving window analysis approach is utilized here that works by computing the statistics of each window under consideration [338]. This is then compared with the maximum value which if exceeded indicates the presence of an anomaly in the time frame [339]. An implementation of this concept has been explored in determining anomalies in computer network where various shapes reveal the networks under attack [311]. The selection of the suitable analysis method is a challenging task and requires consideration from the perspective of application domain, the type of the graph data, the availability of ground truth, the required output format and the target problem.

2.7.3 Summary of Graph Techniques Used

In this dissertation, graphs of tree types (processes and modules are considered as graph nodes) are considered to analyze the changes in graph structure using various node and edge based features. Time based graph is considered to aid the cyber expert in detecting the time instance so that malicious events and activities involving various nodes and edges can be localized and analyzed. This method will help the cyber experts in analyzing the semantic behavior of the process tree evolution where malware renders advanced persistent behavior by mimicking legitimate processes and modules e.g. malware is using the same node name as the legitimate node use. As mentioned earlier, there are four major time based dynamic analysis techniques for graphs and this work evolves through these techniques to overcome the inherent weaknesses and improve cognitive characterization of advanced malware.

Following is the summary of graph techniques used for malware characterization using cognitive complexity in an operating system process tree:

1) Windows 7 operating system based process tree is converted into acyclic, directed and connected graph structure.

2) This work combines static and dynamic graph analysis techniques such that the dynamic graph is used for time instance (time window) detection having malicious object e.g. node, while static in the sense that the features are extracted based on graph structural units and neighborhood i.e. nodes, edges and their neighboring information.

3) Time based graphs are employed using equal interval time samples and various sampling intervals are tested using mathematical concepts of stationarity and Nyquist sampling criterion to ensure generalization.

4) In this work, malicious nodes, edges and the time windows containing these nodes and edges are labelled a-priori to aid in characterization of anomalies and measuring the relative improvement in performance. However, the labelled data is not used for supervised training however, an unsupervised clustering mechanism is used with validation testing using this labelled data.

5) In this work, the first, third and fourth methodologies of subsection 2.7.2 to diagnose irregular activities in a dynamic graph are combined. As in the first approach, which deals with characterizing the anomalous behavior of a particular graph over time, graph structures and neighborhood based features have been extracted from the consecutive time graph snapshots e.g. CNTS and TSNN, among others . These features are then converted into time based mathematical patterns to depict graph behavior using time windows e.g. information based fractal dimensions of each feature. Further, with respect to graph cluster approaches, unsupervised clustering mechanism over graph features is proposed which characterizes the time instances having malicious objects. This is required since the malware nodes and edges show inseparability over features and therefore, direct graph clusters cannot be used. Finally, statistics of each time window in graph are calculated for every feature which corresponds to the fourth approach.

2.8 Heavy Tailed Distribution and Statistical Distribution Tests

In the domain of probability and statistics, there are two major types of distributions; light tailed and heavy tailed [340]. The heaviness of the tail of a distribution indicates that the probability distribution function on large random values is not exponentially bounded. In other words, the tails are heavier than the exponential distributions, which are considered light tailed. Heavy tailed distributions tend to have many outliers with high probability.

Mathematically, for a heavy tailed distribution function F(x) on a random variable x,

$$\int_{-\infty}^{\infty} e^{\alpha x} F(x) dx = \infty \quad \forall \alpha > 0 \tag{22}$$

Equation (23) implies that all statistical moment generating function of heavy tailed distribution are infinite. For any light tailed distribution, moment generating functions shows finite values.

Heavy tailed distributions are divided into three subclasses: fat tailed, long tailed and sub-exponential distributions. These subclasses are divided based on relative heaviness in the tails of distribution and are based on empirical observations, which are not rigorously defined. However, all heavy tailed distributions show power law relationship and the magnitude of the power law delineates the classifications between these subclasses i.e. large outliers occur with non negligible probability. In this work, there are various statistical tests performed to estimate the distribution type (heavy or light), without considering the exact type. For a detailed description of heavy tailed distribution, readers are encouraged to refer to [340].

In order to analyze feature sets for malicious behavior characterization, it is important to perform the statistical evaluation first as it provides valuable mathematical information about the required data analysis and applying suitable technique to ensure minimum performance errors. For example, if the data set reveals the presence For example, if a data set indicates the presence of underlying normal distribution then first and second order moments (mean and variance) are sufficient to characterize the data set. However, if the data set shows signs of heavy tailed distribution, then third and fourth order moments (Skewness and Kurtosis) are also required. Further heavy tailed distributions renders lot of outliers which makes traditional light tailed distribution analysis (e.g. normal and exponential) invalid. In the case of heavy tailed distribution, goal should not be to avoid outliers rather outliers play an important role in shaping the analysis towards cognitively inferable results. Further, heavy tails provide significantly important information of the intrinsic behavior of data set which shows long range correlation and self-similarity at multiple scales and thus begs the use of more advanced analytical techniques i.e. multiscale and fractal analysis.

There are numerous statistical tests to validate the statistical distribution of a given data set empirically. In order to test the validity of features, four statistical significance tests and a fourth moment Kurtosis test are used and are defined as follows:

2.8.1 Kolmogorov–Smirnov test

Named after Andrey Kolmogorov and Nikolai Smirnov, the Kolmogorov-Smirnov test [341] is used to determine if two data samples belong to the same distribution. In other words, it is a non-parametric hypothesis test which compares the cumulative distribution of two data sets. The major advantage of this test comes from the fact that the distribution of data is not assumed and hence, renders it extremely useful for real-world applications where much is not known about the distribution of data at hand. Also, there is no restriction on the sample size which indicates that a smaller set of values can also be used to execute the test [342] [343]

Let's consider that we have a dataset with samples $X_1, X_2, \dots, X_n$ which belong to some unknown distribution P, often known as Empirical Distribution Function or EDF, and the aim is to test the hypothesis that P is equal to a particular distribution P_0. Mathematically, the null and the alternate hypothesis are defined as follows:

$$H_0: P = P_o \qquad (23)$$
$$H_1: P \neq P_0$$

This test enumerates the largest vertical distance between the EDF of the sample $F_n(x)$ and CDF of the referenced theoretical distribution, $F(x)$. The test statistic is mathematically represented as,

$$D = sup_x |F_n(x) - F(x)| \qquad (24)$$

The basic idea is that if the sample belongs to the distribution $F(x)$, then D goes to 0 in probability when $n \to \infty$. A detailed discussion is available in [342] [343].

For two-sample Kolmogorov-Smirnov test, the test statistics is defined as,

$$D = sup_x \left|F_{1,n}(x) - F_{2,m}(x)\right| \qquad (25)$$

where, $F_{1,n}(x)$ and $F_{2,m}(x)$ are the EDF of the first and the second sample. The null hypothesis is rejected, if the value of D exceeds the critical value for which the tables are available at [344].

One of the limitation is that the assumed distributions in null hypothesis are continuous in nature and hence, is not recommended for discrete distributions. Also, it is mandatory to specify the scale, shape and location parameters. These should not be calculated from the data itself. Further, the test is more sensitive towards the median of the sample values compared to the tails [345] [346].

2.8.2 t-test

Commonly known as Student's t-test, this test is used to compare two population means to determine their statistical difference. It was developed by William S. Gossett and verifies if under the null hypothesis, the test statistics follow the student's t-distribution [347]. Alternatively, if the value of the spread parameter i.e. the scaling term is known, the test statistic would assume a

normal distribution. However, if it is unknown and required to be estimated from the data itself, the test statistics follow student's t-distribution. The t-test basically indicates the probability of repetition of results given their average values [348]. The test statistics used in the t-test is called a t-value which very similar to the z-scores. The t-value quantifies the difference between the two sample means. Mathematically, t-value is defined as [349] [347],

$$t = \frac{\bar{X} - \mu}{(\sigma/\sqrt{n})} \tag{26}$$

where, $\bar{X}$ is the mean of samples consisting of $X_1, X_2, \dots, X_n$. μ is the population mean and σ is the standard deviation of the population. The term in the numerator signifies the difference in the two means while the denominator indicates the spread of the scores which is also known as the standard error. It is basically a ratio between the two samples and the difference within the samples. A larger value for the t-score indicates that the considered sample groups are different. Further, the values will be affected by the degrees of freedom which is mathematically represented by $n - 1$

There are three different types of t-tests which are [349]: (i) one-sample, (ii) dependent (related) samples, and (iii) independent (unrelated) samples. The one-sample test compares the mean of the sample with a pre-known value. The data should come independently and randomly from a normal. On the other hand, the dependent or paired samples t-test compares mean of the same sample group under different conditions. While the independent samples t-test deals with the comparison of two different groups

2.8.3 Chi Square Test

Proposed by Karl Pearson [350], the Chi Square goodness of fit test determines if a data sample matches the population. Simply, it is used to validate the hypothesis regarding the nature of the distribution of observation in different groups. For this purpose, it utilizes the frequency values of a data sample to validate the proportion of a population distribution. The frequency in this test refers to the sample count in each category. The null hypothesis states the categorization of the population group with respect to the frequency which is then used to compute the expected frequency. Simply, the null hypothesis checks if the observed and expected frequencies are equal [351]. Mathematically, the null and the alternate hypothesis are defined as follows:

$$\begin{aligned} H_0 &: f_o = f_E \\ H_1 &: f_o \neq f_E \end{aligned} \tag{27}$$

where, the total count in each category is called observed values, f_o, while the expected one, f_E, is the frequency which is predicted under the null hypothesis. The expected frequency for each group is calculated by,

$$f_E = N_p \tag{28}$$

where p is the size from the null hypothesis and N is the sample size. The Chi-Square statistics identifies the extent to which the data samples fit a hypothesized distribution. It is computed as follows:

$$\chi^2 = \sum \frac{(f_o - f_E)^2}{f_E} \tag{29}$$

A large value of the Chi Square statistics reveals a discrepancy between the observed values and the fitted model indicating that the null hypothesis should be rejected. A lower value indicates higher correlation between the observed and expected group and theoretically, the Chi Square statistics should be zero if the two match perfectly. In addition, we have to compute the degree of freedom by subtracting one from the total number of groups or categories. This value is used to lookup the correct significance value from Chi Square distribution table.

2.8.4 Lilliefors test

Developed by Hubert Lilliefors [352] [342] and Van Soest, the Lilliefors normality test is a modification of the Kolomogorov-Smirnov (K-S) goodness of fit test which is used to test the assumption that the samples belongs to a normal distribution. This particular test corrects one of the limitations of the K-S test which requires that the parameters of the normal distribution i.e. the mean and variance to be known apriori. However, this is not the case in most of the real world scenarios and hence, the parameters can be estimated from the sample data itself which in case of K-S will lead to erroneous results. Thus, the preference of Lilliefors test over K-S test [353].

The null hypothesis for this test states that the error is normally distributed or in other words, the difference between the error distribution and normal distribution is zero. The null and the alternate hypothesis are defined as follows:

$$\begin{aligned} H_0 &: S_n(x) = F^*(x) \\ H_1 &: S_n(x) \neq F^*(x) \end{aligned} \tag{30}$$

where, $F^*(x)$ is the cumulative normal distribution function with $\mu = \bar{X}$ the sample mean and s^2 the sample variance. Also, $S_n(x)$ is the estimated cumulative distribution function of the sample. The statistics for the test is defined as,

$$D = max_x |F^*(x) - S_n(x)| \tag{31}$$

If the value of D is greater than the critical value (in the table), the null hypothesis is rejected. These tables can be found in [354].

2.8.5 Kurtosis

To test for the normality of the sample data, kurtosis and skewness are computed. These two values are smaller for a normal distribution which means if the data sample has values closer to zero then, a standard bell curve will be a good fit for distribution in this case. Specifically, kurtosis indicates the height and sharpness of the central peak. The higher values of kurtosis signifies a higher and sharper peak whereas the smaller values indicate a flat and short peak. Another interesting way of interpreting kurtosis is that it is associated with the shift of probability mass from the center of the distribution towards the tail [355] which means that the probability of having outlier is highly likely. It is important to note that kurtosis has no unit and is merely a number. The standard value of kurtosis for normal distribution is 3 (generally, excess kurtosis is reported which is defined as: $kurtosis - 3$). A distribution with kurtosis approximately equal to 3 is called mesokurtic. The one which is greater than 3 is called leptokurtic and is characterized as having higher and sharper peak with longer and dense tails, for example, Laplace distribution. On the other hand, platykurtic are distribution with kurtosis less than 3. Their peak are relatively lower compared to a normal distribution and the tails are quite short and thin, for instance, uniform distribution.

Kurtosis is the fourth standardized moment. For the univariate data,$X_1, X_2, \dots, X_n$, it is mathematically defined as,

$$Kurtosis = \frac{\sum_{i=1}^{n}(X_i - \overline{X})^4/n}{(\sum_{i=1}^{n}(X_i - \overline{X})^2/n)^2} \tag{32}$$

where, n is the total number of data samples and $\bar{X}$ is the sample mean. The denominator term refers to the square of the variance. The lower bound of the kurtosis is given as,

$$Kurtosis \geq (skewness)^2 + 1 \tag{33}$$

and is realized by the Bernoulli distribution. However, there is no upper limit for the kurtosis of a probability distribution and it can be infinite. Kurtosis is a useful method to determine the presence of outlier indicated by its higher value and thus is an indicator for the heaviness in tails.

2.9 K-means Based Unsupervised Clustering Approach

K-means is a clustering algorithm which is widely used in data mining to reveal inherent data structures and patterns based on similarity measures. It is distinctly different from supervised classification techniques, e.g., neural networks and SVM which use offline training to generate classification boundaries to distinguish competing hypotheses. Clustering is an unsupervised machine learning technique that uses a measure of similarity to cluster data samples into discrete and disjoint sets. Clustering does not require any pre-defined labelled data, and, therefore, is a natural candidate for categorizing new cyber threats. Supervised machine learning techniques are insufficient for detecting mutating malware based cyber threats due to the challenges of data re-learning by the algorithm with the new labelled samples, which are generally not available a-priori and thus zero-day threats including new signatures of the previously known malware would have higher probability of being missed, e.g. false alarms.

2.9.1 Clustering Types

Formally, clustering is a method to partitioning an n-dimensional data set containing m samples into k sets or k clusters, such that data samples in one cluster are relatively more similar than samples into another cluster [356]. There are many types of clustering algorithms and a detailed discussion on their types, strengths and weaknesses of various clustering algorithms is discussed thoroughly in [357] [358] [359]. Based on these studies, clustering algorithms can be categorized into following four major categories:

1) Centroid based
   Algorithms in this category iteratively calculate optimum centroids of the data samples and partition them based on their similarity metric e.g. Euclidean with these centroids. K-means algorithm belongs to this category and requires a-priori input of total number of clusters required at the end of iterations. Therefore, knowledge of the dataset is needed to analyze and decide the number of clusters. Further, these algorithms find a local optima in the search space of the data set similarity measure. Centroid based algorithms are efficient in implementation due to their quick convergence to the local optima. Main disadvantage of centroid based algorithms is their sensitivity to the outliers which tend to move the cluster centroid towards the outlier.

2) Connectivity based
   These algorithms create hierarchical connectivity in data points and can iteratively cluster data in two ways; (1) agglomerative: start algorithm assuming all data points as separate clusters and then aggregate them iteratively by increasing the radius of similarity between points, or (2) divisive: start with one cluster and then partition as the distance increases (or similarity measure decreases). These algorithms are efficient and effective in handling data set with varying granularity based on the similarity measure but do not revisit the previous visited data

sample and thus each successive iteration of the algorithm considers only the current data in estimating the cluster skipping the previous results.

3) Distribution based
   These models are based on testing the hypothesis iteratively (or finding a probability) that all data samples in a cluster belongs to a particular distribution. Expectation-Maximization (EM) is a popular clustering technique in this category. These models do not require a-priori knowledge of the number of clusters but suffer from over-fitting problems.

4) Density based
   Algorithms in this category cluster data samples based on their closeness to each other, i.e., finding nearest neighbours based on spatial arrangements such as circular radius. These algorithms keep away outliers from a cluster and provide better approximation based on a similarity measure. However, these algorithms do not scale well with the increasing dimension of data and thus suffer from the so-called curse of dimensionality. DBSCAN [357] and OPTICS [357] are well known density based clustering algorithms.

2.9.2 Clustering Similarity Measures

In order to characterize and analyze malware behavior inside an operating system, clustering mechanisms have been tested and labelled data sets are used to evaluate the clustering performance. As there is no supervised learning to guide the algorithm on the characteristics of malware samples, it is required to understand the effects of different similarity metrics in finding the suitable clustering technique to detect new malware from previous malware family or a new family. Similarity measures can be divided into two major types; (1) single scale, and (2) multi scale [360]. Single scale measures include but are not limited to Euclidean distance, Manhattan distance, Cosine measure, Minkowski measure, and entropy measures [361]. Multiscale similarity metrics measure similarity at each scale and transforms them into a contextual coefficient which represents the variations of the data set from a macro to micro scale. It is important to mention that the variations at multiple scales can be of any type and represent the intrinsic details of how different samples are related to each other, e.g., correlation, variance, spectral, and structural.

2.9.3 Significance of K-means

In this dissertation, a single scale Euclidean similarity measure and three fractal based multiscale similarity measures are implemented in a centroid based k-means algorithm to study and characterize the behavior of different malware samples in a host operating system. Centroid based k-means algorithm is chosen for the following reasons:

1) In a data set having light tailed distribution (low number of outliers), k-means may not be an effective clustering algorithm. However, as estimated and shown in section 2.5 and experiments, host based operating system data set of time graphical model shows heavy tailed distribution and therefore, it would be significant to take into consideration the effects of many outliers in calculating clustering centroid.

2) The reason for not selecting connectivity based clustering algorithm is that they do not consider the previously iterated points in their calculations to find the local optima. Therefore, with each successive iteration, connectivity based algorithms chose new samples skipping the clustered samples in previous iterations and thus ensures convergence to local optima in a limited sense. Connectivity based algorithms can be considered as "cluster and forget" algorithms and therefore, statistical significance of the clustering results is not strong. This implies that law of large numbers will not be applied uniformly in all iterations and therefore this type of closeting is not suitable to be used in this work.

3) Distribution and density based clustering algorithms are closely related in the sense of extracting the closeness of samples either structurally (density) or through estimated probability distribution functions. However, these algorithms do not consider outliers and are not suitable for heavy tailed distributions.

As the features show significant overlap among normal and malicious samples, fractal based similarity methods are incorporated in the k-means algorithm to characterize and validate the performance over single scale similarity based clusters.

2.10 Performance Evaluation Metrics

In order to test the performance of a prediction algorithm, following basic evaluation metrics are used to test the binary hypothesis, where a positive represents malicious sample and a negative represents normal sample [362].

1) True Positives (TP) = Sample to be predicted is Positive and resultant prediction is Positive.

2) True Negative (TN) = Sample to be predicted is Negative and resultant prediction is Negative.

3) False Positive (FP) = Sample to be predicted is Negative and resultant prediction is Positive.
    a. Missing a Negative and wrongly considering it a Positive.
    b. An efficient metric to measure a missing normal sample
    c. In the domain of security world, this is considered a nuisance for security experts and creates possibility of missing a true positive due to cognitive bias if there is a FP overload.

4) False Negative (FN) = Sample to be predicted is Positive and resultant prediction is Negative.
    a. Missing a Positive and wrongly considering it a Negative.
    b. An efficient metric to measure missing a zero-day cyber threat.

These basic evaluation parameters can be used further to derive following statistical measures bounded in the interval [0, 1]:

1) True Positive Rate (Sensitivity or Recall or Probability of Detection)

    This measure defines the degree or extent over which a positive is not missed and thus false negatives are minimized.

$$\text{True Positive Rate (TPR)} = \frac{TP}{TP + FN} \tag{34}$$

2) True Negative Rate (Specifity)

    This measure defines the degree or extent to minimize false positives and not missing the detection of negatives.

$$\text{True Negative Rate (TNR)} = \frac{TN}{TN + FP} \tag{35}$$

3) False Positive Rate

    This measure quantifies the degree of missing a negative sample.

$$\text{False Positive Rate (FPR)} = \frac{FP}{FP + TN} = 1 - TNR \tag{36}$$

4) False Negative Rate

This measure quantifies the degree of missing a positive sample.

$$\text{False Negative Rate (FNR)} = \frac{FN}{TP + FN} = 1 - TPR \tag{37}$$

5) Precision (Positive Predicted Value)

This measure provides a metric on the correct identification of the proportion of positives. High precision means the variance of predicted positives is low while low precision means that the prediction of positive value has a large spread. Precision is not accuracy, rather a way of knowing how close the predicted results are (may or may not be close to the actual values).

$$\text{Precision} = \frac{TP}{TP + FP} \tag{38}$$

6) Accuracy

Accuracy measures the overall performance of how closely the predicted values (both positive and negative) agree with the known values. High accuracy means the results are low biased. A high accuracy model can only be useful when there is a class balance.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{39}$$

7) F1 score

F1 score is a statistical harmonic mean and represents the weighted average of the precision and recall. This metric is a measure of knowing how good a predictor is in correctly identifying the positives and negatives. This metric provides a way to measure precision vs. recall. This metric has significance when there is a class imbalance e.g. cyber security data sets.

$$\text{F1} = 2.\frac{Recall\,.\,Precision}{Recall + Precision} = 2.\frac{TPR \cdot \frac{TP}{TP + FP}}{TPR + \frac{TP}{TP + FP}} \tag{40}$$

It is worthwhile to mention that in the domain of cyber security, having a problem of class imbalance due to intelligence and mutating malware/threat factors, prediction power of an algorithm requires metrics of sensitivity, accuracy and F1 score altogether to understand how reliable the prediction is in terms of performing true detection of threats. However, sensitivity and accuracy are found to be complementary. If sensitivity increases, accuracy decreases and vice versa. Further, having a good accuracy model does not work when the data set has asymmetric

balance of normal vs. malicious samples. Therefore, F1 score helps in finding the average performance of algorithm in predicting both classes correctly [363].

3. Design of Experiments and Algorithms

In this section, details of the experimental framework and algorithms is provided. Further, this section describes the threat model used in this work. Following are the subsections:

Subsection 3.1 Threat Model

This subsection describes the threat model used in this research. This threat model is based on five different assumptions and provide a scope of the experimental framework.

Subsection 3.2 Sandbox - Data Collection and Processing

In this subsection, details of the system and software architecture are provided. Further, the methodological approach carried out to collect, process and curate the data set is also provided. In order to provide similar environment and operating system behavior, a simulation of user behavior is also mentioned. Finally, observation details of each of the ten malware instances is enumerated for a detailed and systematic cognitive analysis.

Subsection 3.3 Malware Data Set

In this subsection, experimental details of the execution of each malware instance is provided. It includes how each malware behaves inside an operating system process tree and what can be observed as a data attribute.

Subsection 3.4 Algorithms

This subsection provides algorithmic details of the time and space graphs, and cognitive complexity based fractal algorithms i.e. VFD, SFD, IFD, and CFD. Further, algorithms of standard and the proposed fractal based k-means algorithms is also mentioned.

3.1 Threat Model

Before characterizing advanced and persistent malware inside an operating system using cognitive semantic approach, a threat model is presented which is a collection of following assumptions:

Assumption 1: Malware (threat) is delivered successfully.

The threat model assumes that the adversary is successful in executing the first four stages of the traditional cyber kill chain model and the payload, which is an advanced persistent malware, is ready for installation followed by establishing CnC communication and subsequently performing the required malicious objectives. This assumption is believed to be realistic because many organizations have recently reported data exfiltration attacks where intellectual and confidential data has been stolen over a course of many years and none of their existing defenses were able to detect it on time [30] [364]. Therefore, it suggests that threat actors have the required skills to penetrate large and complex organizations, secured with multiple line of defenses, and therefore, it is necessary to adopt a threat hunting (in addition to reactive threat detection methods) approach assuming the existence of threat. Also, the initial four stages of traditional cyber kill chain does not generate sufficient host based evidential data that can be used for malware characterization and subsequent detection.

Assumption 2: Host based malware analysis.

This dissertation focuses on analyzing and characterizing malware behavior inside an operating system using the temporal dynamics of its process tree. Further, the experiments and analysis activities are limited to the malware which are able to exfiltrate data by establishing CnC channel(s) with the malicious remote servers and are used for targeted attacks [31]. The analysis does not consider the network communications and assumes that the malware is or will communicate to its servers. Nevertheless, in order to establish the communication channels, the malware process must first attach itself to the process tree to spawn required modules and interact with operating system objects. Therefore, this work focusses on this local behavior of the malware which is a pre-requisite step for the malware to commence any CnC communication. This is a realistic assumption and simplifies the analysis because analyzing network communication typically requires a suite of firewalls and IDS/IPS devices which are mostly based on signature based detection and are limited in performance due to the large volume of data from multiple hosts and network devices. The proposed Malvidence framework can be applied to individual host operating system. Further, the eventual purpose of malware based attacks is to target hosts and therefore, warrants the validity of this assumption.

Assumption 3: Malware hunting (threat hunting) approach using binary hypothesis.

As this work studies the behavior of targeted malware which exfiltrates data and are capable of mimicking the legitimate process objects, therefore, a binary hypothesis is chosen to characterize the objects either as legitimate or malware. Multiple hypotheses are used in reactive cyber security operations where threat intelligence feeds are used to add situational awareness about certain families of malware [365] and therefore, a categorization of malware is required to subjectively analyze the behavior related to a particular category of threats. However, this work conjectures to analyze process tree behavior for the characterization of advanced persistent malware, without considering any a-priori knowledge including but not limited to situational awareness, and therefore, it is realistic to use binary hypothesis [366]. Further, in the context of practical cyber security operation centers, the first step in threat analysis requires the alerting of an anomaly first before finding a particular category of threat, therefore, this assumption is not far from practical use case.

Assumption 4: Malware has no knowledge about the virtualization setup.

It is assumed that the malware is not able to sense the presence of any virtualization or sandboxing mechanism. Advanced persistent and stealthy malware can detect the presence of any detection mechanism including virtualization framework, which are used to trap malware to render their true behavior for collecting signatures. However, it is assumed that the proposed characterization framework will run in actual servers, computers and production machine which are the actual target for adversaries. Due to limited resources and policy restrictions at University of Manitoba, it was not possible to run malware over actual computing machines, and therefore, an open source virtual machine setup was used for the experiments. With the increasing use of virtual machines over actual computing hardware such as computers and servers, this assumption is not far from practical use cases.

Assumption 5: Malware persistence and survival.

This work assumes that the malware renders persistence after a machine reboot or after a removal of the malware by killing its process node manually [367]. For advanced persistent threats, it is common to deploy multiple copies of the malware with different file names, memory locations and process tree activities so that even after the removal of one copy, another copy get activated and performs the malicious function [368]. Further, malware are intelligent enough to get reactivated after a machine is rebooted because they modify Windows registry to ensure their persistence as well. Moreover, this behavior is attributed due to the malware getting the administrative privilege of the operating system to perform its operations without hindrance.

3.2 Sandbox - Data Collection and Processing

3.2.1 System Architecture

As shown in Figure 37, a conceptual experimental setup is shown which also serves as the high level visual representation of the malware testing sandbox [1]. Following is the configuration of the host machine in Figure 37:

1) Server: Dell PowerEdge R730 server rackmount server machine.
2) Processor: Intel Xeon E5, 2.3 GHz, 25M Cache, 10/20cores.
3) RAM: 32 GB.
4) Storage: 40 TB SATA 5400 rpm.
5) Operating System: Windows 2012 R2 Server.

Over this host machine, open source software for creating and managing virtual machine i.e. Oracle virtual box is installed [369] and two Windows 7 (service pack 1) virtual machines (VM) instances (VM guest 1 and VM guest 2) are created with following configuration for each VM:

1) Operating System: Windows 7, 64 bit, Service Pack 1.
2) Virtual RAM: 8 GB.
3) Virtual Storage: 25 GB HDD.
4) 2 virtual network adapters.

MySQL Server 5.7 [370] is installed on VM guest 1 and two virtual network adapters were created. One adapter is used to communicate with the host to share MySQL tables for further processing by software running on the physical host machine. On VM guest 1, sharing was disabled during malware execution to avoid any malicious leak. The second virtual network adapter is used to collect SQL table entries from VM guest 2 where malware is executed. There is no possible communication between the two instances, except for the SQL query information using the specific port; all other ports are blocked. This is done in order to ensure that the malware is not able to propagate to the VM guest 1 instance or to the host machine and remain quarantined in its VM instance. Also, in the second VM instance having malware executed, there is a secured internet communication allowed via the host machine.

For the cases of malware bots like Zeus and Citadel, where relevant malware builder kit is available, a Linux (Fedora) based VM is used to build a malware command and control (CnC) server which serves as the mother-ship for controlling the bot's activities and also for the storage of exfiltrated information. Over this machine, a LAMP (Linux, Apache, MySQL and PHP) package is installed to assist in preparing the malware control panel. Also, for some malware samples, CnC is outside of our domain.

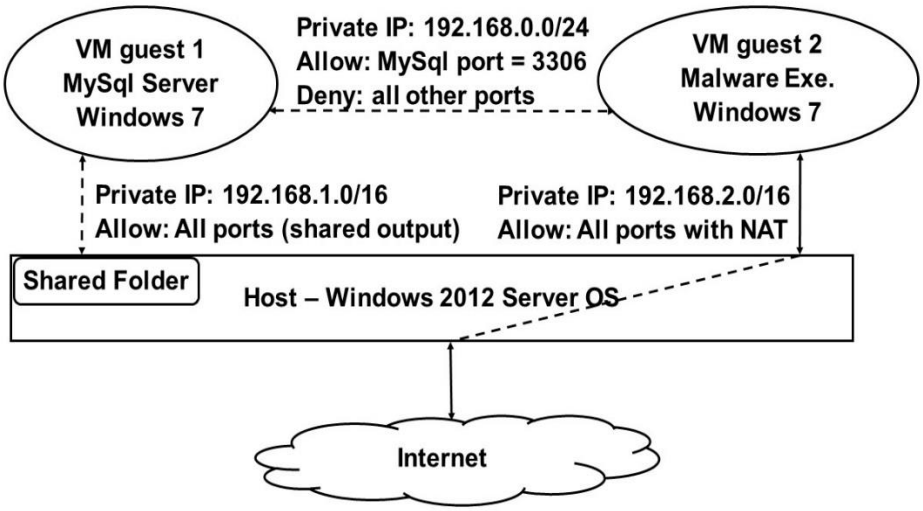


Figure 37: System diagram showing experiment setup on a Host machine with Virtual Machines (VM).

3.2.2 Software Details

The following Windows 7 operating system process tree attributes are extracted using C based programming module:

1) Universally Unique Identifier (UUID) based on Process ID – UUID.
2) Process ID – PID.
3) Process Name – PRN.
4) Process Creation Time – PRT.
5) Parent Process ID – PPID.
6) Module Name – MODN.
7) Module Create Time – MODT.
8) Module Executable Location – MODL.
9) Process Memory Size – PRM.
10) Module Memory Size – MODM.
11) Thread Count – THC.

3.2.2.1 A Brief of Microsoft MSDN Windows APIs

Following major Windows API functions are used in this C function – GetProcess():

1) UuidCreate() [371].
    a. UuidToString.
2) CreateToolhelp32Snapshot () [372].
    a. Takes a snapshot of the process and its opened modules and threads.
3) OpenProcess () [373].

a. GetProcessMemoryInfo ().
b. ListProcessModules ().
c. ListProcessThreads ().

3.2.3 Description of Data Collection Program

The following steps are mentioned here to provide a logical flow of the programming steps. These steps represent the C code where modular functions are created using Windows API. Cygwin programming platform, GCC compiler and GDB debugger are used to create the C program .exe files over Windows 7 operating system.

3.2.3.1 Preprocessing

1) Configure MySQL server and client.
    a. Client should have write access (this experiment uses privileged access).
    b. Server IP must be allowed for opening connection in the client Windows firewall.

2) Create MySQL template.
    a. *endpointProcessTable.* (Table for endpoint process data).
    b. *endpointModuleTable.* (Table for endpoint module data).
    c. *endpointThreadTable.* (Table for endpoint thread data).

3.2.3.2 Collect Data

1) Main() function
    a. Open MySQL Connection.
        i. Select database.
        ii. Open connection.
        iii. Open process table.
    b. FOR Loop.
        i. GetProcess(handle *MySQL tables*);
2) GetProcess() function.
    a. Handle hProcessSnap = CreateToolhelp32Snapshot().
        i. save all running processes in a structure pointer.
    b. DO-WHILE (till the end of hProcessSnap which is indexed based on processes).
        i. OpenProcess().
        ii. UuidCreate (PID).
        iii. malloc() - Allocate memory according to the size of [UUID+PID+PRN+PRT+PPID+MODN+MODT+MODL+PRM+MODM+THC].
        iv. Use MySQL database table handle to store database information.

3.2.3.3 Curate Data

1) Data Consolidation Step.
   a. Join *endpointProcessTable*, *endpointModuleTable* and *endpointThreadTable* using UUIDs.
2) Create a CSV file of the data attributes and sort them according to increasing timestamps.
3) Label the CSV file (binary where 1 is for malware and 0 for all else).
4) The CSV file contains the attributes as mentioned in Figure 38.

As shown in Figure 39, an abstract view of the collected templates is shown to represent the temporal collection of data.

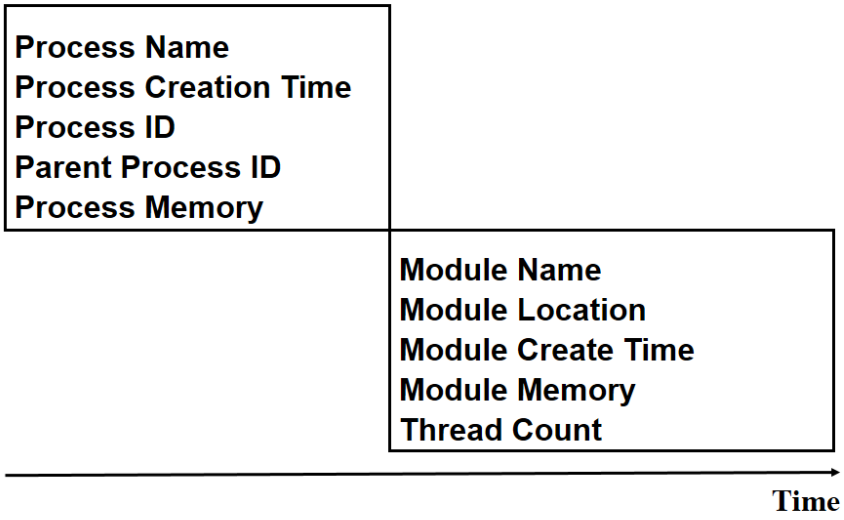


Figure 38: Template of information collected for each process tree.

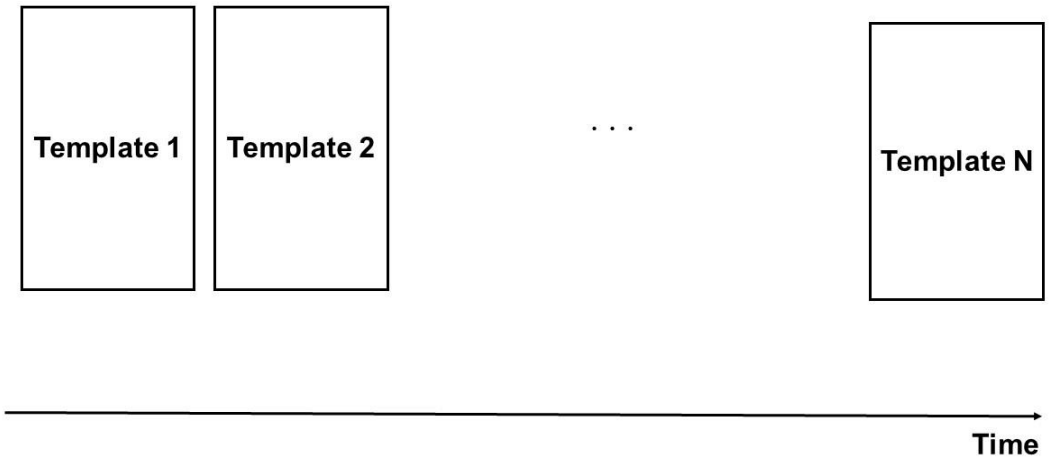


Figure 39: Time series showing the abstract collection of template samples.

3.2.4 Simulating User Behavior

In order to simulate the user behavior (a typical office computer) over Windows 7 operating system, two methods are employed:

1) Sikulix [374] software is used to automate Windows desktop activities. Sikulix is a Python based program that uses OpenCV based image recognition tools to automate Windows desktop activities. Sikulix was programmed to open multiple websites with predefined varying time intervals. Also, reasonable sleep intervals were introduced to ensure that the resultant host based activity mimic human interaction and not an automated program such as bots and crawlers. Further, it is also programmed to create new files, edit existing file, play audio, write notepad files, load and save files and login to dummy social media accounts with varying time intervals. Sikulix software is used because it is an open source software having an interactive user interface and is a light weight package consuming relatively low computing resources making it an ideal choice for this work.
2) Activities using these programs and websites were carried out manually for the entire duration as well.

It is noted here that there was switching between the above mentioned activities to mimic human like behavior, such as, a typical human working on a desktop application, would have opened many website in a browser along with social media interaction and possible audio or video streaming. Further, above 2 methods of simulating user behavior using both Sikulix and manual human activities is employed to ensure that the host behavior of legitimate activities remain same throughout the experiments on various malware execution VM instances and thus analyze the

malware actions manually for data validation purpose. Also, Sikulix appeared in the process tree as an artifact and is filtered out of the data set during the pre-processing stage.

Following is a visual time flow of a typical lifecycle of the experimental virtual machine (which was used for malware detonation):

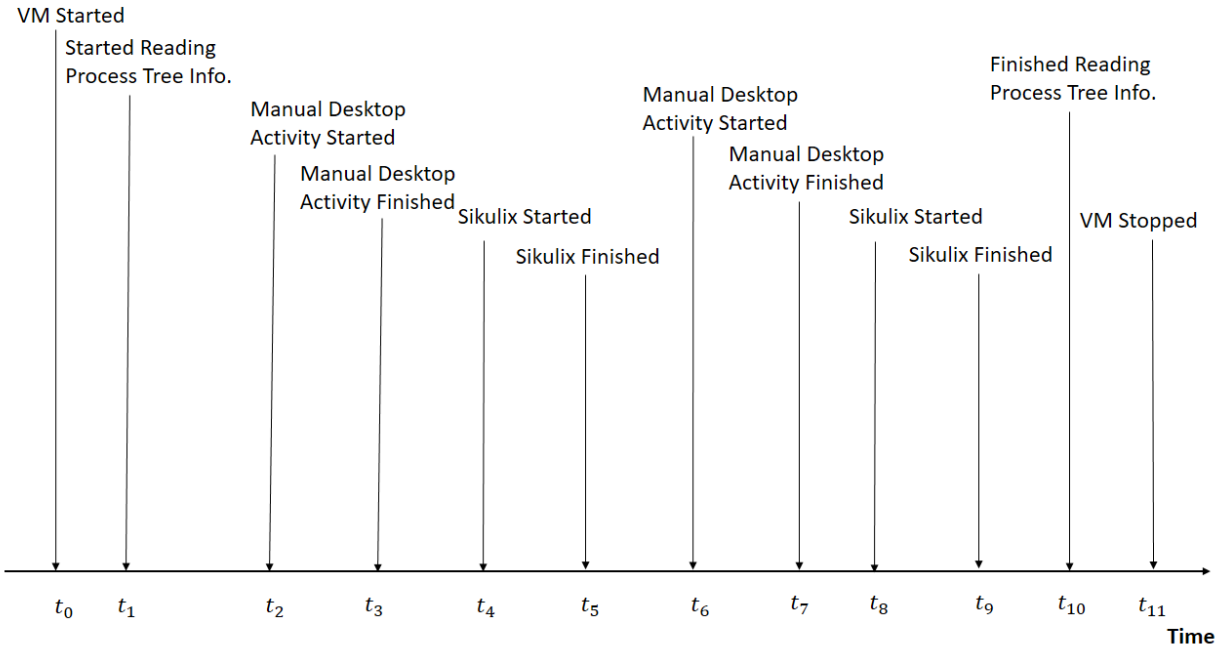


Figure 40: A timeline of the experimental virtual machine.

t_1 - t_0	=	time duration between the initialization of the operating system. startup and the commencement of process tree acquisition.
t_3 - t_1	=	manual desktop activities initiated and then stopped.
t_5 - t_3, t_9 - t_7	=	Sikulix started and then stopped.
t_7 - t_5	=	manual desktop activities initiated and then stopped.
t_{11} - t_9	=	Stopped process tree acquisition and then stopped the VM.

3.2.5 Observation Details for Each Malware

As shown in Table 2, a comparative view of the collected data from each malware sample execution on Windows 7 VM is presented. There are two instances of each sample with varying acquisition time. This acquisition time is based on the fact that whenever a malware sample enters a host machine successfully, it takes some time to establish itself within the operating system environment. Typically, it senses the existing defenses, analyzes the behavior of operating system and then does decrypts the mutated payload. This payload either connects with the remote CnC server successfully to start getting commands or exfiltration or detonates while damaging the system completely (e.g. virus and worms). In the first case, it may look for other ways to communicate with the CnC using alternate set of IP addresses or domains. During the experimental

execution of selected malware samples, which are CnC based, it is ensured that the sample gets established inside the host and starts communicating with the CnC server. Wireshark based packet capturing on guest operating system was observed manually to ensure that the sample has started communicating to the CnC IP address. To ensure that each malware sample renders its inherent persistence and is subsequently captured by the process tree acquisition program, the VMs were rebooted and the malware processes were terminated manually. Following this, the malware samples re-initiated and are captured in the acquisition system. Therefore, the acquisition duration of 2500 loops of C program is chosen as an upper limit based on multiple experiments on each malware instance and the duration varied accordingly. It is noted in Table 2 that the acquisition time varies with each VM which is due to the non-real time nature of the operating system whereby multiple operating system schedules tasks with random assigned priorities for user space.

Table 2: Data acquisition and collection details for each malware instance.

No.	Malware	Instance	Acquisition Loops	Acquisition Duration	Total Records	Unique Records
				minutes	No. of Rows	No. of Rows
1	Zeus	1	2500	85	421576	230381
2	Zeus	2	2500	165	433910	254679
3	Citadel	1	2500	85	427287	232208
4	Citadel	2	2500	105	398624	249443
5	Hupigon	1	2500	87	401581	217837
6	Hupigon	2	2500	92	407021	227097
7	Zurgop	1	2500	84	417158	213574
8	Zurgop	2	2500	83	391426	201132
9	Carberp	1	2500	87	424015	232659
10	Carberp	2	2500	86	429322	227104
11	Alina	1	2500	99	397202	225677
12	Alina	2	2500	99	491544	273751
13	Proteus	1	2500	92	461594	250376
14	Proteus	2	2500	93	532657	340784
15	Stabuniq	1	2500	95	576776	339724
16	Stabuniq	2	2500	149	564771	334570
17	Nivdort	1	2500	94	443117	251784
18	Nivdort	2	2500	139	375903	235487
19	Poweliks	1	2500	132	417859	251284
20	Poweliks	2	2500	93	547777	310833

As shown in Figure 41, a comparative analysis of the count of number of rows acquired for each data as per Table 2 is presented. It is observed that the row duplication occurs in the range of 34% to 44%, which is attributed by virtue of the acquisition software's functionality to capture the state of all process information in the memory. Therefore, it is necessary to remove the duplication for further analysis. Also, Figure 42 shows the acquisition speed of each malware data set as per Table 2. Although, this research work does not stipulate improvement in the efficiency of data acquisition, however, Figure 42 provides a rough estimate of the acquisition speed which is mostly in the range of 80 to 100 rows per second.

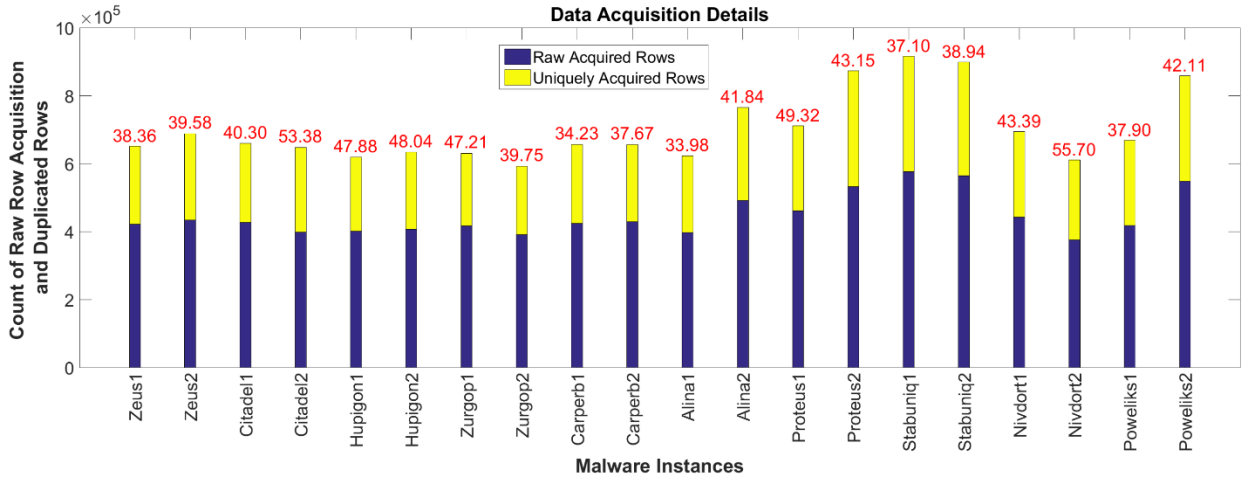


Figure 41: Data acquisition analysis for each malware data set.

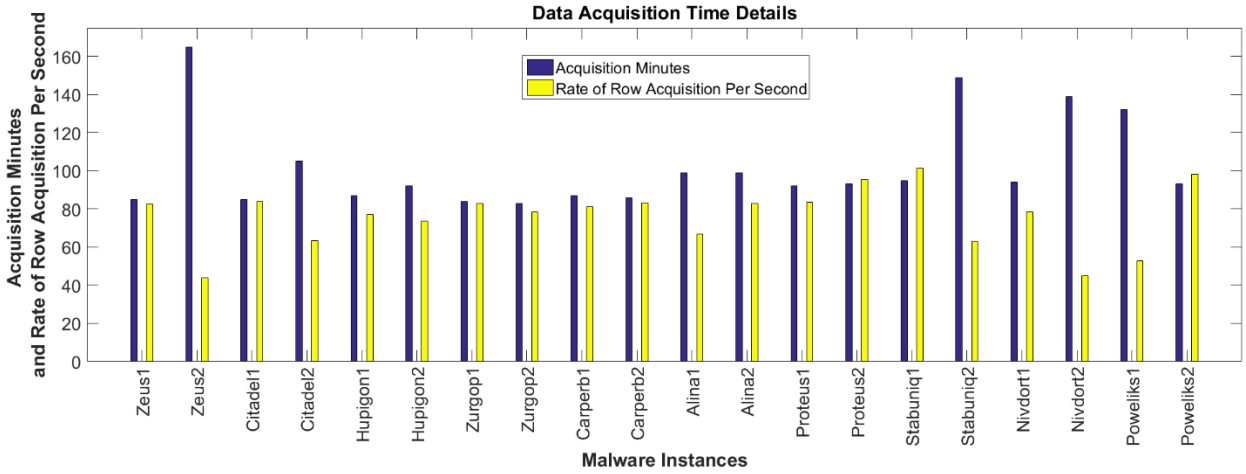


Figure 42: Data acquisition time analysis.

3.3 Malware Data Set

This subsection describes details of the data set which is collected and processed for malware characterization. Ten different samples of mutating malware with 2 instances of each are tested in a virtual machine (VM) based Windows 7 operating system. All selected malware samples exfiltrate victim's data to the outside server and are able to mimic operating system process tree behavior as described in Table 1.

3.3.1 Malware Samples and Related Information

In order to extract process tree information of a Windows 7 based virtual machine infected by a mutating malware, a clone of a clean Windows 7 based virtual machine with similar virtual resources (memory, processor and hard drives) is used for every new malware instance tested. The configuration of this clone is kept same for all instances to avoid any operating system based artifacts due to change in configurations and settings.

In order to understand the data set, it is worthwhile to note that the data capture program written in C programming language described section 3.2 uses Microsoft MSDN libraries to capture a snapshot of the process tree residing in the main memory of the Windows 7 based endpoint system. There is a loop based C program that acquires the process tree information and then parse it further for creating MySQL queries at every loop step. This program executes 2500 times and therefore the process tree data set contains copies of previously observed process information as well. For example, if a process of Mozilla Firefox opened a PDF document and it was kept open for an extended amount of time, then it will appear in many successive loops.

The selected malware samples show behavioral mutation as already described in section 2.2.3 and Table 1. The dynamic changes are observed to be; (1) change in the process name of the malware executable, (2) changes in parent and child processes of the malware process, and/or (3) changes in the type of the operating system file formats.

The following subsection defines the details of observations collected over the sandbox for individual malware. Particularly, it addresses: (1) how did we ensure that the sample in hand belongs to a particular malware family? and (2) how did we label the individual dataset?

3.3.2 Malware Execution and Data Collection

As discussed in Section 3.2 the malware sandbox consists of three different VMs; (1) a Windows 7 guest for executing the malicious executable, (2) a Fedora/Kali Linux based command and control server to direct the malicious activities and gather exfiltrated data and (3) a Windows 7 based MySQL system where the collected data is stored and processed. It is important to note that Zeus and its variant Citadel, which are used in this research study, are constructed from malware kits which were downloaded from [375] and their corresponding CnC server was built on virtual Linux machines. The rest of the malicious samples were obtained in the form of Windows

executable from [376]. As the builder kits for Zeus and Citadel were available, different instances of the malware were generated using various configurations. However, the same malicious sample was executed twice for other malware samples. To keep the nature of this research experiment as close to the real world scenario as possible, both host and network based activities were performed and the resultant data was collected in a database. Nevertheless, as this work is only focussed towards host based analysis, therefore, only host based operating system process tree data analysis is analyzed and retained.

To initiate the research investigation, the malware executable is manually delivered to the Windows host. In case of a real world cyber-attack, this is usually achieved with the help of a dropper or downloader stage of kill chain. But, to focus the efforts on the actual data collection and analysis process, this step was simplified with an assumption that the threat actors use certain vulnerability of the system or network to deliver the malware payload successfully. Moreover, the malware samples were executed with administrative privileges as they require access and modification rights for operating system resources and components like Windows operating system based registries, memory, directories and processes. Upon execution, the copied malicious file automatically and expectedly disappeared from its folder and some or all of the following behaviors were observed on the host machine:

1. The malware executable file was copied under all or some of these directories: Windows HOME directory, SYSTEM directory and the USER profile.
2. The file was copied to the STARTUP folder or a registry is created to ensure persistence after reboot.
3. Communication with the command and control server was initiated and established.
4. The binary configuration file was downloaded from the command and control server, which has rules regarding the logging format and frequency, data capture, URL filtering, web injections and form grabbers.
5. A new folder was created under the Windows HOME directory or USER profile where stolen data was kept before exfiltration.
6. Some of the files from Windows HOME or SYSTEM directory were replaced by the infected files.
7. New operating system processes were created, most of which mimic the standard Windows processes like svchost.exe.
8. Registry values were created and modified on the fly.

On the command and control server side of the Zeus and Citadel bot, the information about the infected host was logged. This included the operating system information, local date, time and IP addresses, cookies, username/passwords, screenshots, browsing information, installed software. Also, some changes were made in the configuration file, which was updated on the host and the corresponding changes were reflected in the bot behavior. Further, the bot control panel provided options to execute commands remotely and send files on the infected machine, view desktop screenshots, activate/deactivate bot, reboot machine and connect to the infected system via VNC.

Also, during the experiment, before and after detonating the malware, normal host activity was performed manually for a few minutes; creating MS office file, browsing internet, playing music, and checking email. In addition, SikuliX based scripts [374] were executed on the infected host to automatically perform activities like creating documents, editing them, browsing internet, and logging to email services. Further, details on the SikuliX script is available in section 3.2.4. This is done in order to ensure that a balance in the generated data for both malware and normal data is maintained. Further, this will provide a common denominator to analyze the malware effect after it infects a clean operating system. Also, it is close to the usage pattern of a general user. This also simulates the case if a malware samples tries to evade the system if they detect that they are under scrutiny. Also, to ensure the persistence of a malware, the infected virtual machine was rebooted and the corresponding details of new malicious processes were recorded. It is important to note that two samples of each malware family were executed in a different virtual machines and their behavior was observed.

Detailed information of the observed malicious processes, files and directories is discussed in the following subsections for each malware sample. Although network level information is collected by the sandbox, they are not included in this work because the purpose of study is to analyze the host level behavior only.

3.3.2.1 Zeus Malware – Instance 1

Process Name and ID

When initialized, the Zeus bot [377] [378] [379] [380] [381] started with the name ***bot.exe*** with a process ID 6480; however, after few minutes this process vanished and a new process with the name ***xusa.exe*** appeared with the process ID 6484. Also, bot.exe was a name given to the bot executable generated using the kit for this experiment only. However, in a real world cyber-attack scenario this name is generally kept similar to that of a legitimate file.

Directories and Files

The bot copied the executable to the USER profile with a random folder and file name as:

C:\Users\<user_name>\AppData\Awovcu\xusa.exe

3.3.2.2 Zeus Malware – Instance 2

Process Name and ID

For the second instance, the Zeus bot [377] [378] [379] [380] [381] initialized as the process ***bot.exe*** with a process ID 5224, however, after few minutes this process disappeared and a new process with the name ***voed.exe*** appeared with the process ID 5236. Also, consider that the bot.exe

was a name given to the bot executable generated using the kit but it can be changed while making sure that the configuration file is correspondingly updated. However, in a real world cyber-attack scenario this name is generally kept similar to that of a legit file to evade detection.

Directories and Files

The bot copied the executable to the user profile with a random folder and file name as:

C:\Users\<user_name>\AppData\Ogbia\voed.exe.

3.3.2.3 Citadel Malware – Instance 1

Process Name and ID

When initialized the Citadel bot [381] [382] started with the name ***soft.exe*** with a process ID 5724 which was given for simplification and identification purpose. However, after few minutes this process vanished and a new process with the name ***puxa.exe*** appeared with the process ID 6632.

Directories and Files

The bot copied the executable to the user profile with a random folder and file name which for this Citadel instance was:

C:\Users\<user_name>\AppData\hpwm\puxa.exe.

3.3.2.4 Citadel Malware – Instance 2

Process Name and ID

The Citadel bot [381] [382] was initialized with the name ***soft.exe*** with a process ID 4432 which was simplified the process identification in the process tree. However, after few minutes this process exit and a new process with the name ***ahce.exe*** appeared with the process ID 4444.

Directories and Files

The bot copied the executable to the user profile with a random folder and file name which for this Citadel instance was:

C:\Users\<user_name>\AppData\ykuq\ahce.exe.

3.3.2.5 Hupigon Malware – Instance 1

Process Name and ID

This malicious backdoor executable [383] [384] created two processes with the name ***cmd.exe*** one of which belonged to the user and other to the SYSTEM with the corresponding process IDs of 6336 and 6392 respectively. Attached to each of these were two ***conhost.exe*** processes separately with the process ID 6400 (for SYSTEM) and 6344 (for USER). Another process with the name ***Hacker.com.cn.exe*** and process ID 6384 was also spawned by this malicious executable.

Directories and Files

The backdoor copies itself to the Windows system directory with the following name:

C:\Windows\SysWOW64\Hacker.com.cn.exe.

3.3.2.6 Hupigon Malware – Instance 2

Process Name and ID

Similarly, for the second instance [383] [384], the malware sample created two processes with the name ***cmd.exe*** one of which belonged to the user and other to the SYSTEM with the corresponding process IDs of 6780 and 6820 respectively. Attached to each of these were two ***conhost.exe*** processes separately with the process ID 6828 (for SYSTEM) and 6760 (for user). Another process with the name ***Hacker.com.cn.exe*** and process ID 6872 was also spawned by this malicious executable.

Directories and Files

The backdoor copies itself to the Windows system directory with the following name:

C:\Windows\SysWOW64\Hacker.com.cn.exe.

3.3.2.7 Zurgop Malware – Instance 1

Process Name and ID

The Zurgop sample [385] [386]created a new process with the name ***svchost.exe*** and ID 6344. The important catch is that Windows has a legitimate process with this name as well. To check for the persistence, the system was restarted and the malicious ***svchost.exe*** process with a new ID 2468 was present.

Directories and Files

To ensure persistence, the executable upon installation copies itself to the Windows STARTUP folder with the name ***dxdiag.exe.***

C:\Users\<user_name>\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\dxdiag.exe.

3.3.2.8 Zurgop Malware – Instance 2

Process Name and ID

Again, in the second instance [385] [386], the Zurgop sample created a new process with the name ***svchost.exe*** and ID 6296. The notable point is that the process name is among the list of authentic Windows processes. To further analyze the behavior, the system was restarted and the malicious ***svchost.exe*** process with a new ID 2456 was found to be present on the system.

Directories and Files

To ensure persistence, the executable upon installation copies itself to the Windows startup folder with the name ***dxdiag.exe.***

C:\Users\<user_name>\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\dxdiag.exe.

3.3.2.9 Carperb Malware – Instance 1

Process Name and ID

When executed, Carberp banking Trojan [381] [387] created two processes with the name ***svchost.exe*** having process IDs 6508 and 6516. It is important to note here that svchost.exe is a legit Windows process as well. Therefore, identifying this malware from process list alone is quite difficult.

Directories and Files

The malicious executable copied itself with the name ***igfxtray.exe*** to the Windows startup folder to ensure its presence after reboot.

C:\Users\<user_name>\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\igfxtray.exe.

Further, it created the following folders as well:

C:\O0oSmLwBgnUZBIX\wndsksi.inf.

C:\Users\<user_name>\AppData\Roaming\MicroST.

3.3.2.10 Carperb Malware – Instance 2

Process Name and ID

Two processes with the name ***svchost.exe*** having process IDs 6420 and 6428 were created when the malware was executed for the second time. Identification of this malware from process list is quite difficult because of its similarity in term of its name with the genuine Windows process [381] [387].

Directories and Files

The malicious executable copied itself with the name igfxtray.exe to the Windows startup folder to ensure its presence after reboot.

C:\Users\<user_name>\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\igfxtray.exe.

Further, it created the following folders as well:

C:\O0oSmLwBgnUZBIX\wndsksi.inf.

C:\Users\<user_name>\AppData\Roaming\MicroST.

3.3.2.11 Alina Malware – Instance 1

Process Name and ID

The sample from Alina family of malware [388] [389] displayed a unique behavior upon execution where multiple processes were created upon reboot. First, a malicious process with a name ***3_4.exe*** and process ID 6816 was observed which after initialization vanished and a new process with the name ***dwm.exe*** and process ID 6880 was created. To verify the persistent behavior, the system was rebooted and the ***dwm.exe*** process with the ID 2532 was observed. This however, changed into ***adobeflash.exe*** with an ID 2568. To further investigate the behavior, the system was restarted again and this time two process with the same previous name i.e. ***adobeflash.exe*** and ***dwm.exe*** with their respective IDs 2372 and 2348 were observed. After sometime, both of these processes vanished and a new process with the name ***desktop.exe*** and ID 944 surfaced.

Directories and Files

The malware copied itself to the following directory after installation:

C:\Users\<user_name>\AppData\Roaming\dwm.exe.

3.3.2.12 Alina Malware – Instance 2

Process Name and ID

For the second run as well, the sample from Alina family of malware [388] [389] displayed a unique behavior upon execution in terms of spawning multiple processes. First, a malicious process with a name ***3_4.exe*** and process ID 5444 was observed which after initialization disappeared and a new process with the name ***jusched.exe*** and process ID 5516 was created. To investigate the behavior further, the system was rebooted and the ***jusched.exe*** process with the ID 2452 was present. This however, changed into ***win-firewall.exe*** with an ID 2800 after the complete initialization. To further understand the malware characteristics, the system was restarted again and this time two process with the same previous name i.e. ***jusched.exe*** and ***win-firewall.exe*** with their respective IDs 2368 and 2356 were observed. After sometime, both of these processes vanished and a new process with the name ***jucheck.exe*** and ID 2032 surfaced.

Directories and Files

The malware copied itself to the following directory after installation:

C:\Users\<user_name>\AppData\Roaming\jusched.exe.

3.3.2.13 Proteus Malware – Instance 1

Process Name and ID

Proteus bot sample [82] [85] was downloaded as a Google chrome executable and upon execution ***gchrome.exe*** process was immediately visible in the process list with the ID 6804. However, this process exit and three process with the name ***chrome.exe*** and IDs 6876, 7000 and 7068 were created.

Directories and Files

This bot copied an illegitimate **chrome.exe** to the following folder:

C:\Users\<user_name>\AppData\Roaming\.

3.3.2.14 Proteus Malware – Instance 2

Process Name and ID

Proteus sample [82] [85] appeared to be a Google chrome executable and therefore, when executed, a process with the name ***gchrome.exe*** with the ID 6332 is observed in the process list. However, this process exit after installation and three process with the name ***chrome.exe*** and IDs 6848, 6800 and 7024 appeared. For this instance, the malware process was killed manually,

however, it immediately spawned back with the same process name but different IDs i.e. 10836, 10932, and 11352.

Directories and Files

This bot copied an illegitimate **chrome.exe** to the following folder:

C:\Users\<user_name>\AppData\Roaming\.

3.3.2.15 Stabuniq Malware – Instance 1

Process Name and ID

For this experiment, the Trojan horse Stabuniq [390] [391] executable sample was named as ***svchost.exe*** which upon execution created a process with the same name and ID 6844. Along with that, another malicious process was spawned with the name ***issch.exe*** with the ID 6916. Also, it was observed that the Trojan copied its code to two ***iexplore.exe*** processes with the ID 6940 and 6956. For further verification of its persistence, the system was rebooted after which two ***iexplore.exe*** processes with the ID 912 and 2124 were present in the process list.

Directories and Files

The Trojan horse copied itself to the following location:

C:\Program Files\ GrooveMonitor Utility\Update\issch.exe.

3.3.2.16 Stabuniq Malware – Instance 2

Process Name and ID

In this run, the Stabuniq Trojan horse [390] [391] sample was named as ***svchost.exe*** which upon execution created a process with the same name and ID 7548. Along with that another malicious process was spawned with the name ***issch.exe*** with the ID 7268. Also, it was observed that the Trojan copied its code to two ***iexplore.exe*** processes with the ID 7680 and 7628. For better understanding of malware behavior, the system was restarted after which two ***iexplore.exe*** processes with the ID 15232 and 15316 were present in the process list.

Directories and Files

The Trojan horse copied itself to the following location:

C:\Program Files\ GrooveMonitor Utility\Update\issch.exe.

3.3.2.17 Nivdort Malware – Instance 1

Process Name and ID

The Nivdort Trojan sample [392] [393] was named as ***sample.exe*** for the purpose of data simplification which when executed created a process with the same name and ID 1300. Once installed, it created multiple process IDs with two distinct names i.e. ***tdtxjtat.exe*** and ***ylxgpkkuii.exe.*** The observed process IDs for each of these processes is listed below:

tdtxjtat.exe: 1556, 7036, 7316, 7396, 8460, 11992, 13424, 15660, 18128, 18788, 22008.

ylxgpkkuii.exe: 2388, 2636, 9244, 9628, 11492, 13340, 14580, 16816, 19028, 19892, 23544.

Directories and Files

The trojan drops its copies in the system root folder as follows:

C:\tdtxjtat.exe.

C:\ ylxgpkkuii.exe.

3.3.2.18 Nivdort Malware – Instance 2

Process Name and ID

The Nivdort Trojan sample [392] [393] was named as ***sample.exe*** for the purpose of ease in identification in the process list which when executed created a process with the same name and ID 8012. Once installed, it created multiple process IDs with two distinct names i.e. ***tdtxjtat.exe*** and ***ylxgpkkuii.exe.*** The observed process IDs for each of these processes is listed below:

tdtxjtat.exe: 9908, 10024, 14968, 18952, 29036, 33464, 36648, 39712, 42064, 46284, 49300, 52328, 55504.

ylxgpkkuii.exe: 2388, 2636, 9244, 9628, 11492, 13340, 14580, 16816, 19028, 19892, 23544.

Directories and Files

The Trojan drops its copies in the system root folder as follows:

C:\tdtxjtat.exe.

C:\ ylxgpkkuii.exe.

3.3.2.19 Poweliks Malware – Instance 1

Process Name and ID

This special file-less Trojan [394] [395] when executed is extremely difficult to catch. It created two processes ***cmd.exe*** and ***powershell.exe*** with IDs 8856 and 8588 immediately. Due to its fileless nature, it executes its code from rundll32.exe which is a legit Windows program for executing java code. However, it was observed that after the execution of Poweliks sample, a ***rundll32.exe*** process with process ID 8552 and a ***cmd.exe:0*** process with ID 1536 was initiated and thus noted as malicious. A corresponding ***conhost.exe*** with ID 8600 and ***dllhost.exe*** with ID 8864 was also found to be malignant after analysis. To further verify the persistence, the process was killed and it automatically resumed with names ***cmd.exe, cmd.exe:0,*** and ***dllhost.exe*** with IDs 14332, 13464, and 13372 respectively.

Directories and Files

It is a fileless Trojan and therefore, does not copy anything on disk rather it creates a registry containing its malicious code which gets executed upon each reboot.

3.3.2.20 Poweliks Malware – Instance 2

Process Name and ID

This special file-less Trojan [394] [395] when executed created two processes i.e. ***cmd.exe*** and ***powershell.exe*** with IDs 6752 and 7108 immediately. Due to its fileless nature, it executes its code from rundll32.exe which is an authentic Windows program for executing java code. However, it was observed that after the execution of Poweliks sample, a ***rundll32.exe*** process with process ID 6196 and a ***cmd.exe:0*** process with ID 6808 was initiated and thus noted as malicious. A corresponding ***conhost.exe*** with ID 6692 and ***dllhost.exe*** with ID 6844 was also found to be malignant after analysis.

Directories and Files

It is a fileless Trojan and therefore, does not copy anything on disk rather it creates a registry containing its malicious code which gets executed upon each reboot.

3.4 Algorithms

3.4.1 Process Tree Relationship Algorithm

3.4.1.1 Pre-Processing

1) Read **N** rows of the process tree file and sort it in ascending order based on process create time with resolution of 100 nano second (ns) per unit of time. It is important to know that graph generation requires process creation time and module creation time information. Sorting the file based on process create time will automatically sort module creation time since process create time is always greater than or equal to its spawned module creation time.

2) After sorting, **N** rows of a process tree file are read and the following information is extracted in individual array data structures:
    a. **pid** - Process ID.
    b. **procNm** - Process Name.
    c. **procCTm** - Process create time in MS Windows timestamp (100 nano second).
    d. **ppid** - Parent Process ID of the pid.
    e. **procMemSz** - Process Memory Size in bytes.
    f. **threadCnt** - Number of threads opened by the module.
    g. **modNm** - Module opened by the process.
    h. **modPth** - Module Path in Windows directory structure.
    i. **modBaseSz** - Module memory in bytes.
    j. **modCTm** - Module create time in MS Windows timestamp (100 nano second).
    k. **label** - Label (normal = 0, malware = 1).

3) Concatenate **modNm** and **modPth** into another array data structure called **mod**.

4) Concatenate **pid** and **procNm** into another array called **pidNode**.

3.4.1.2 Extract Process Tree Relationship

```
1       /*
2       Purpose:        Develop process tree relationship in the process tree data file.
3       Input:          ppid(Parent process ID), pid(Process ID), procNm(Process Name)
4       Output:         Data structure having concatenated PID and process name.
5       Example:        '444,winlogon.exe'    OR      '0,xxx'
6       */
7
8       Function pTree = procRelation (ppid, pid, procNm)
9               // Find array of unique ppid
10              unqPPID  ← unique(ppid);
11              FOR Loop: i = 1 till size(unqPPID)
12                      // Find index of given unqPPID in array of pid
13                      ind1 ← find(pid , unqPPID(i));
14                      IF isempty(ind1)
15                              /* Find index of given unqPPID in array of ppid if unable to find
16                              in pid such as pid = 0 and 4 */
17                              ind2 ← find(ppid , unqPPID(i));
18                              // For pid not having ppid and process name, assign 'xxx'
19                              ppidNode(ind2) ← concatenate( unqPPID(i) , ',' , 'xxx' );
20                      ELSE
21                              // Find index of ppidNode (found in previous step) in ppid array
22                              ind2 ← find((ppid , ppidNode(i));
23                              // Concatenate pid with procName
24                              ppidNode(ind2) ← strcat( pid( ind1 ) , ',' , procNm( ind1 ) );
25                      END IF
26              END FOR
27      END procRelation()
```

3.4.2 Time and Space Graph Algorithm

This function will create ten different groups of time based graph structures. Each such structure will have time based graphs from t_{min} till t_{max} where t_{min} is the smallest process timestamp and t_{max} is the largest process timestamp in the data set. Each group will have adaptive and sliding sampling time windows having minimum lag. Details of adaptive and sliding time window mechanism is provided in subsection 4.2.5.1. Increasing group number is equivalent to increasing time sample window lag size from 10^1x100ns per window till 10^{10}x100 ns per window.

```
1    /*
2    Purpose:    Generate time and space graph of the process tree data file.
3    Input:      Process tree data file.
4    Output:     Time and space graph data structures.
5    */
6    Function main()
7        // --- Generate space graph of the data file. ---
8        G = gph(ppid, pid, procCTm, procMemSz, threadCnt, modNm, modBaseSz,
9            modCTm, label );
10       // --- Generate Time Graph of the data file. ---
11
12       // Creating adaptive sliding time samples for each group of sample window size.
13       FOR Loop: windowLag = 1 till 10
14           // Initialization.
15           i := 1;
16           s := 10;
17           tmWindowLag ← 10^windowLag;
18           beginTm(i) ← procCTm(1);
19           endTm(i) ← procCTm(1);
20           tmBeginIndArray(i) ← 1;
21           tmEndIndArray(i) ← 1;
22           minTm ← min(procCTm);
23           deltaTm ← procCTm – minTm;
24
25           // Loop through N rows to find indices for stationary sampling intervals.
26           FOR Loop: ind =1 till N
27               tmTemp ← deltaTm(tmBeginIndArray(i) : ind);
28               isStationary = vfd(tmTemp, s);
29               IF isStationary ≥ 1 & isStationary ≤ 2
30                   tmEndIndArray(i)  ← ind;
31                   endTm(i) ← procCTm(ind);
32                   indTemp ← tmBeginIndArray(i);
33                   i++;
34                   tmBeginIndArray(i) ← tmWindowLag + indTemp;
35               END IF
```

```
36                  END FOR
37              // Assign tmIndBeginArray and tmIndEndArray to relevant time sample window
38              data structure.
39              tmSample(windowLag). tmBeginIndArray = tmBeginIndArray;
40              tmSample(windowLag). tmEndIndArray = tmEndIndArray;
41              END FOR
42              // Creating time graph structure in each group of time sample windows.
43              FOR Loop: ind1 = 1 till 10
44                      // Accessing tmIndBeginArray and tmIndEndArray corresponding to the
45                      relevant time window.
46                      tmpValBegin ← tmSample(ind1). tmIndBeginArray;
47                      tmpValEnd ← tmSample(ind1). tmIndEndArray;
48                      // Loop through each sample in tmIndArray.
49                      FOR Loop:  ind2= 1 till size(tmpValBegin)
50                              // Assign window start index to x.
51                              x ← tmpValBegin (ind2);
52                              // Assign window end index to x.
53                              y ← tmpValEnd (ind2);
54                              //  Initialize structure s and assign corresponding arrays to it.
55                              // Parent Process ID array assignment.
56                              s.ppid ← ppid(x:y);
57                              // Process ID array assignment.
58                              s.pid ← pid(x:y);
59                              // Process create time array assignment.
60                              s.pct ← procCTm (x:y);
61                              // Process memory size array assignment.
62                              s.pcm ← procMemSz (x:y);
63                              // Thread count array assignment.
64                              s.tc ← threadCnt(x:y);
65                              // Module name accessed by the process array assignment.
66                              s.m ← modNm (x:y);
67                              // Module memory array assignment.
68                              s.mdm ← modBaseSz(x:y);
69                              // Module create time array assignment.
70                              s.mct ← modCTm(x:y);
71                              // Label assignment.
72                              s.lb ← label(x:y);
73                              // Generate graph for each sample in the time window array.
74                              gT(ind1).G = gph(s.ppid, s.pid, s.pct, s.pcm, s.tc, s.m, s.mdm, s.mct,
75                                              s.lb );
76                      END FOR
77              END FOR
78      END main()
```

```
1   /*
2   Purpose:    To create space graph data structure.
3   Input:      ppid(Parent Process ID), pid(Process ID), procCTm(Process create time),
4               procMemSz(Process memory size), threadCnt(Thread Count),
5               mod(Module name), modBaseSz(Module memory), modCTm(Module
6               Create Time), label(label).
7   Output:     G(Directed Acyclic Graph data structure).
8   */
9
10  Function G = gph(ppid, pid, procCTm, procMemSz, threadCnt, mod, modBaseSz,
11              modCTm, label)
12          // Initialization of G i.e. a Directed Acyclic Graph (DAG).
13          G.Nodes ≔ ∅;
14          G.Edges ≔ ∅;
15          G.Edges.EdgeCnt ≔ 0;
16          G.Edges.TimeCnt ≔ 0;
17          G.Edges.Mem ≔ ∅;
18          G.Edges.ThreadCnt ≔ 0;
19          G.Edges.Label ≔ ∅;
20          // Loop through N rows.
21          FOR LOOP: i = 1 till N
22                  /* This condition executes when given ppidNode is included in the graph
23                  Nodes. */
24                  IF  ppidNode_i ∈ G.Nodes
25                  /* This condition executes when given pidNode is included in the graph
26                  Nodes. */
27                          IF  pidNode_i ∈ G.Nodes
28                                  // Update graph with the ppid, pid and module info.
29                                  G ← gphForm(G, ppidNode_i, pidNode_i ,
30                                  mod_i,procCTm_i, procMemSz_i);
31                          ELSE
32                                  // Add given pidNode to the graph node structure.
33                                  addNode(G, pidNode_i);
34                                  // Update graph with the ppid, pid and module info.
35                                  G ← gphForm(G, ppidNode_i, pidNode_i ,
36                                  mod_i,procCTm_i, procMemSz_i);
37                          END IF
38                  /* This condition executes because given ppidNode is not included in the
39                  graph nodes. */
40                  ELSE
41                          // Add given ppidNode to the graph node structure.
42                          addNode(G, ppidNode_i);
43                          // Add given pidNode to the graph node structure.
```

```
44                              addNode(G, pidNode_i);
45                              // Update graph with the ppid, pid and module info.
46                               G ← gphForm(G, ppidNode_i, pidNode_i , mod_i, modCTm_i,
47                              modBaseSz_i);
48                      END IF
49              END FOR
50      END gph()
```

```
1     /*
2     Purpose:     To augment process details in the graph edges.
3     Input:       G(Graph structure), ppidNode (Graph node of PPID), pidNode (Graph
4                  Node of PID), mod(Graph Node of module), crtTime(Process or module
5                  create time), memSz(Process or module memory size).
6     Output:      G(Updated graph data structure).
7     */
8
9     Function G = gphForm (G , ppidNode , pidNode , mod, crtTime, memSz)
10          /* This condition executes when directed edge of considered ppidNode and
11          pidNode is not included in the graph edges list. */
12          IF [ppidNode→pidNode] ∉ G.Edges
13                // Add edge in the graph between ppidNode and pidNode.
14                addEdge(G, ppidNode, pidNode);
15                // Update graph edges with the process information.
16                G ← procInfo(G, crtTime, memSz, G.Edges.ThreadCnt, G.Edges.Label);
17          ELSE
18                // Update graph edges with the process information.
19                G ← procInfo(G, crtTime, memSz, G.Edges.ThreadCnt, G.Edges.Label);
20          END IF
21          // This condition executes when module name is not included in the graph nodes.
22          IF  mod ∉ G.Nodes
23                // Add node with the module name in the graph.
24                addNode(G, mod);
25                // Add edge in the graph between pidNode and mod.
26                addEdge(G, pidNode, mod);
27                // Update graph edges with the module information.
28                G ← modInfo(G, crtTime, memSz, G.Edges.ThreadCnt, G.Edges.Label);
29          ELSE
30                /* This condition executes when directed edge of considered pidNode and
31                mod is not included in the graph edges list. */
32                IF  [pidNode → mod] ∉ G.Edges
33                      // Add edge in the graph between pidNode and module.
34                      addEdge(G, pidNode, mod);
35                      // Update graph edges with the module information.
36                      G ← modInfo(G, crtTime, memSz, G.Edges.ThreadCnt,
37                      G.Edges.Label);
38                ELSE
39                      // Update graph edges with the module information.
40                      G ← modInfo(G, crtTime, memSz, G.Edges.ThreadCnt,
41                      G.Edges.Label);
42                END IF
43          END IF
44    END gphForm ()
```

```
1       /*
2       Purpose:        To augment process details in the graph edges.
3       Input:          G(Graph structure), procCTm(Process create time), procMemSz(Process
4                       Memory size), threadCnt(Thread count), label(label).
5       Output:         G(Updated graph structure).
6       */
7
8       Function G = procInfo(G, procCTm, procMemSz, threadCnt, label)
9               // Update the corresponding edge fields in the graph structure for processes.
10              G.Edges.EdgeCnt++;
11              G.Edges.TimeCnt ← procCTm;
12              G.Edges.Mem ← procMemSz;
13              G.Edges.ThreadCnt ← threadCnt;
14              G.Edges.Label ← label;
15      END procInfo ()
```

```
1       /*
2       Purpose:        To augment process modules in the graph edges.
3       Input:          G(Graph structure), modCTm(Module create time), modBaseSz(Module
4                       Memory size), threadCnt(Thread count), label(label).
5       Output:         G(Updated graph structure).
6       */
7
8       Function G = modInfo(G, modCTm, modBaseSz, threadCnt, label)
9               // Update the corresponding edge fields in the graph structure for modules.
10              G.Edges.EdgeCnt++;
11              G.Edges.TimeCnt ← modCTm;
12              G.Edges.Mem ← modBaseSz;
13              G.Edges.ThreadCnt ← threadCnt;
14              G.Edges.Label ← label;
15      END modInfo()
```

3.4.3 Variance Fractal Dimension (VFD) Algorithm

```
/*
Purpose:    Compute Variance Fractal Dimension (VFD) [12] [217] [13].
Input:      Y (Feature array), s (Scaling depth).
Output:     D_V (VFD of Y).
*/

Function D_V = vfd(Y, s)
    // Size of input feature array Y.
    szY := size(Y);
    // Loop through each scale.
    FOR Loop: k =1 till s
        // Radius of vels at k^th scale.
        velR_k ← 2^k;
        // No. of vels at k^th scale.
        vel_k ← szY / velR_k;
        // Loop through each vel of the scale k.
        FOR Loop: i = 1 till vel_k
            // Difference of max and min values of the vel covering Y_ik.
            ΔY_ik ← max(Y_ik) − min(Y_ik);
        END FOR
        // Compute variance at scale k.
        Var_k ← 1/(N_k − 1) [ Σ_{j=1}^{vel_k} (ΔY_jk)^2 − 1/N_k (Σ_{j=1}^{N_k} ΔY_jk)^2 ]
    END FOR
    // Storing variance at each scale in an array.
    Var ← [Var_1, Var_2, Var_3, ... Var_k];
    // Vector of vel radius.
    V ← [2^1, 2^2, ... 2^s];
    // Fit a polynomial of first degree.
    h ← polyfit(log[V] , log[Var]);
    // Find the slope of h which is an estimate of VFD.
    D_V ← slope(h) / 2;
END vfd()
```

3.4.4 Spectral Fractal Dimension (SFD) Algorithm

```
/*
Purpose:    Compute Spectrum Fractal Dimension (SFD) [7].
Input:      Y (Feature array), N(sampling time window size), s (Scaling depth), p
            (order of Autoregressive series AR) [396]
Output:     D_S (SFD of Y).
Supporting Functions:
*/

Function D_S = sfd(Y, N, s, p)
        // Estimate PSD using Yule-Walker model.
        Y: = [Y_0, Y_1, Y_2, ... Y_{N-1}];
        // Create a polynomial using unknown ∅_i's to be estimated.
        Y_{i+1} ← ∅_1 Y_i + ∅_2 Y_{i-1} + ∅_2 Y_{i-2} + ∅_p Y_{i-p+1};
        // Estimating second order expected value.
        r_ip ← Σ_{j=1}^{p} ∅_ij . Corr(Y_{i-p+1} Y_{i-j+1});
        // Matrix manipulations.
        [r_1; r_2; .; .; r_p] = [r_0 r_1 . . . r_{p-1}; r_1 r_2 . . . r_{p-2}; . . . . . .; . . . . . .; r_{p-1} r_{p-2} . . . r_0] . [∅_1; ∅_2; .; .; ∅_p]  => r̄ = R̄ . ∅̄;
        // Looping through each p to estimate ∅_i's.
        FOR Loop i = 1 till p
                ∅̂_i ← R̄_i^{-1} . r̄_i ;
        END FOR
        // acf is an autocorrelation function acf.
        acf : = ∅̂ ;
        /* power spectral density (PSD) using Fast Fourier Transform FFT and
        corresponding frequency components.*/
        [psd , freq] ← fft(acf);
        // Fit a polynomial of first degree.
         h ← polyfit(log[psd] , log[freq]);
        // Find the slope of h which is an estimate of SFD.
         D_S ← slope(h);
END sfd()
```

3.4.5 Information Fractal Dimension (IFD) Algorithm

```
/*
Purpose:    Compute Information Fractal Dimension (IFD) [258] [1].
Input:      Y (Feature array), s (Scaling depth).
Output:     D_I (IFD of Y).
*/

Function D_I = ifd(Y, s)
    // Size of input feature array Y.
    szY ≔ size(Y);
    // Loop through each scale.
    FOR Loop: k=1 till s
        // Radius of vels at k^th scale.
        velR_k ← 2^k;
        // No. of vels at k^th scale.
        vel_k ← szY / velR_k;
        // Loop through each vel of the scale k.
        FOR Loop: j=1 till vel_k
            // Estimating vel probability.
            p_jk ← (vel_ik == ∅) ? 1 / vel_k : 0
        END FOR
        // Compute Shannon's entropy at scale k.
        H_k ← −∑_{j=1}^{vel_k} p_jk . log(p_jk);
    END FOR
    // Storing entropy at each scale in an array.
    H ← [H_1, H_2, H_3, ... H_k];
    // Vector of vel radius.
    V ← [2^1, 2^2, ... 2^s];
    // Fit a polynomial of first degree.
    h ← polyfit(log[V] , log[H]);
    // Find the slope of h which is an estimate of IFD.
    D_I ← slope(h);
END ifd()
```

3.4.6 Correlation Fractal Dimension (CFD) Algorithm

```
/*
Purpose:    Compute Correlation Fractal Dimension (CFD) [14].
Input:      Y (Feature array), s (Scaling depth).
Output:     D_C (CFD of Y).
*/

Function D_C = cfd(Y, s)
    // Size of input feature array Y.
    szY := size(Y);
    // Loop through each scale.
    FOR Loop: k=1 till s
        // Radius of vels at k^th scale.
        velR_k ← 2^k;
        // No. of vels at k^th scale.
        vel_k ← szY / velR_k;
        // Compute correlation at scale k.
        C_k ← 1/(N_vel_k)^2 [∑_{i,j=1}^{N_vel_k} heavisideFunction(velR_k-|Y_i − Y_j|)];
    END FOR
    // Storing correlation at each scale in an array.
    C ← [C_1, C_2, C_3, ... C_k];
    // Vector of vel radius
    V ← [2^1, 2^2, ... 2^s];
    // Fit a polynomial of  first degree.
    h ← polyfit(log[V] , log[C]);
    // Find the slope of h which is an estimate of CFD.
    D_C ← slope(h);
END cfd()
```

3.4.7 Standard and Proposed Fractal based K-means Clustering Algorithm

3.4.7.1 K-means Lloyd's Algorithm:

```
/*
Purpose:    Assign input samples to the clusters based on similarity metric [356].
Input:      k (No. of clusters – default value is 2 for legitimate and malicious samples),
            X ((m x n) dimensional data set; [x1 x2 x3 ... xm] T, where each x_i is an n
            dimensional feature array).
Output:     V (Cluster labels estimated for each sample and is an m-dim array),
            C_k (Array of centroids).
*/

Function [V, C_k ] = kmeansLloyd(k, X, iter)
        // Looping through iterations.
        FOR Loop : z = 1 till iter
                // centroid assignment is random from X.
                C_k ← x_j;        ∀ k ∈ {0,1}, j ∈ {1, 2, 3, … , m} and (C_0 ∩ C_1 = ∅)
                FOR Loop : i = 1 till m
                        // Compute distance between sample x_i and each centroid.
                        ϵ_ik ← min_k(distance( x_i, C_k )) ∀ (x_i ∩ C_k = ∅);
                        // Assign k with minimum ϵ_i to x_i.
                        V_i ← arg min_k(ϵ_ik);
                END FOR
                // Update centroids with average distance between samples in each cluster.
                C_k ← 1/size(ϵ_k) Σ_{j=1}^{m} ϵ_jk;
        END FOR
END kmeansLloyd ()
```

3.4.7.2 K-means Fractal Algorithm:

```
/*
Purpose:    Assign input samples to the clusters based on similarity metric.
Input:      k (No. of clusters – default value is 2 for legitimate and malicious samples),
            X ((m x n) dimensional data set; [x1 x2 x3 … xm] T, where each xi is an n
            dimensional feature array).
Output:     V (Cluster labels estimated for each sample and is an m-dim array),
            Ck (Array of centroids).
Note:       Computation of fractal dimension (FD) uses the fractal algorithms as per
            subsections 3.4.3, 3.4.4, 3.4.5, and 3.4.6 e.g. VFD, SFD, IFD and CFD.
*/

Function [V, Ck ] = kmeansFD(k, X, iter)
    // Estimate fractal dimension (FD) of each n-dimensional point in X.
    FDX ← [fdx1, fdx2, fdx3, … , fdxm];
    // Looping through iterations.
    FOR Loop : z = 1 till size(FDX)
        /* Assign first centroid to xi having maximum value FDX and the
        second centroid to xi having minimum value of FDX. */
        C0 ← max(FDX);
        C1 ← min(FDX);
        FOR Loop : i = 1 till size(FDX)
            // Compute distance between sample xi and each centroid.
            ϵik ← mink ( distance( fdxi, Ck ) ) ∀ (fdxi ∩ Ck = ∅);
            // Assign k with minimum ϵi to xi.
            Vi ← arg mink(ϵik);
        END FOR
        // Update centroids with average distance between samples in each cluster.
        FDX ← FDX – max(FDX);
        FDX ← FDX – min(FDX);
    END FOR
END kmeansFD ()
```

THIS PAGE INTENTIONALLY LEFT BLANK

4. Experiments, Analysis and Results

This section describes the extraction of graph theoretical features from the collected and transformed process tree data set. Also, each data set is labelled for malicious and normal nodes and edges, respectively. This labelling is done to validate the characterization performance and is not intended for training or learning purpose. Thirteen different node and edge based features are manually analyzed and subsequently selected using a parsing program.

Subsection 4.1 Data Features vs. Data Attributes

In this subsection, a prologue on the difference between features and attributes for empirical data is provided. Further, feature selection criteria is also described in the context of cognitive machine intelligence and mathematical validity.

Subsection 4.2 Graph Theoretical Characterization

This subsection provides a detailed study and analysis of the collected data attributes and extracted features. Further, a description of converting the data set into space based time graphs is mentioned which is labelled with the presence of malware nodes and edges. This analysis is carried over further by converting the space graphs into 10 time graphs having separate time sampling intervals. This sampling is done using adaptive and sliding time window mechanism and is entailed by the need of statistical validation. Further, these ten time graphs are analyzed to find out optimum time series that can provide unique and sufficient features for characterization. These ten different time graphs are based on ten increasing timestamps using a variable, adaptive and sliding time window algorithm to find a statistically valid time window showing weak sense stationarity. This is followed by extracting node and edge based features for cognitive analysis and an example is illustrated to emphasise the role of these extracted features in cyber security cognitively.

Subsection 4.3 Fractal Characterization and Validation by K-means Clustering Algorithm

In this subsection, cognitive complexity based fractal characterization using mathematical fractional Brownian motion process and clustering approach using k-means algorithm is provided.

Subsection 4.4 Feature Characterization and Clustering Performance Results of Malware Data Set

In this subsection, performance of the characterization is compared with traditional single scale methods followed by a discussion.

Subsection 4.5 Analysis of Results

This subsection provides further details of the proposed Malvidence characterization framework using multiple features in such a way that each feature is analyzed for its performance towards reducing a particular false alert. A preliminary characterization using mathematical tests is provided which is followed by unsupervised cognitive characterization using complexity based fractal analysis on individual features. A detailed discussion on the performance is also followed. Afterwards, significance of the proposed characterization framework is provided followed by two use case examples to elaborate the implementation feasibility of using Malvidence framework in a practical CSOC environment.

4.1 Data Features vs. Data Attributes

In order to analyze the process tree of a Windows 7 operating system, a graph theoretical model is used to extract features from the raw process tree data. Particularly, a time based graph model is used, where graph is generated for each time window from the data set and the minimum time window sliding size (lag) is varied from 1 microsecond to 1000 seconds. Therefore, there are ten time series showing variations in graph structures and subsequently their features accordingly. These ten time series are used to analyze and subsequently decide a statistically optimum time series for further analysis.

It is important to signify the difference between data attributes and features. According to [397], an attribute represents the observation of raw data, which may or may not be complete. More precisely, a data model describes an attribute as an instance of data and is not necessarily what a human may perceive. Therefore, a feature is a derived human perception from observable raw data [397]. The terminology of "attribute" is also used to represent a property or characteristic of a data model. Typically, in the theory of Artificial Intelligence, attribute and features are used interchangeably. There has been intensive research work [398] [399] [400] carried out in the domain of image processing, where the terminology "attribute" is used to define an intermediate feature, while the terminology "feature" is reserved for the cognitively derived knowledge from those attributes. For example, in Artificial Neural Network applications, attributes are used as the input to the first neural layer and the hidden layers are used to extract features by transforming attributes using a linear or nonlinear weighted function [29] [113] [401].

However, the terminology "feature" is significantly differentiated from the terminology "attribute" in the context of cognitive intelligence. In the theory of machine intelligence [402] [403], an attribute represents human observation about the data while feature is a transformation (interpretation) of that observation into a meaningful recognition. It can be modeled as:

$$F = f(attributes) \tag{41}$$

where F is a feature derived from a set of data attributes through some functional mapping f(). Therefore, using mathematical notation:

$$F: Domain(Attribute) \rightarrow S \tag{42}$$

where S is the set of all possible functional values of the attribute [397].

In this work, the terminology "feature" is used as an extension of the definitions of equations (41) and (42). This work conjectures that, cognitively speaking, a feature represents a semantic value of some aspect(s) of the data, which is a transformation of syntactic representation of data called attribute. It can be viewed as an analogical difference between the terminologies of "information" and "message" in the domain of Shannon information theory. A message represents raw bit(s) of digital data while information represents a meaningful probabilistic transformation of raw bit(s). A stream of raw bits does not represent anything unless an information theoretic transformation is applied to encode/decode bits into a meaningful recognition such as statistical probability. Likewise, feature is a meaningful recognition of the raw data attributes and thus bears a semantic value through feature transformation mapping.

4.1.1 Feature Selection Criteria

In this work, features are selected based on the following rules of thumb and cognitive aspect of utilizing domain knowledge [9] [404] [405]:

a) Features should not be correlated. There should be at least weak sense independence among the selected features. Independence is required in order to avoid any bias towards a particular feature during the learning process. For example, statistical features of nodes are different from edge in a graph based process tree operating system data. Multiple paths can exist between a particular parent and child nodes, in which case, it is redundant to consider node based features as many times as the edge based paths are. This is necessary to avoid data bias towards nodes while under fitting towards edges.

b) Features should be representative of the overall data set. This is necessary to ensure that the results follow generalization principles and should avoid *over*- or *under*- fit. For example, node of a process tree graph should consider not only the processes, but the modules as well. However, module is a different entity representing a child originated from a certain process. Further, processes always have a process identifier while module does not have. However, considering both process and module as nodes of a graph not only provide a cognitive tree sense of the process dynamics, but also ensures generalization because any program running in an operating system can be represented as a combination of processes and modules altogether.

c) Similar nodes can generate parallel paths from parent to child node and thus create a process tree of similar parent and child node for each new edge based feature which would add redundancy, and will subsequently bias the statistical analysis towards either nodes or edges.

d) It is necessary to ensure that the features must represent the dynamics of the system under consideration. For example, if the features are extracted from a host based process tree, then those features should represent modifications/dynamics (e.g. addition, removal and accessing of different processes/modules) with respect to time.

e) Features should be unique and represent a data set uniquely which is attributed to the statistical independence of features. There should not be any overlap. For example, in a host based process tree data set, number of child nodes spawned by the parent process would be similar to the number of new edges created under the same parent process. However, if the objective for edge based feature is to find number of paths, then they should be used in conjunction with number of nodes and should not be used separately as edges.

4.2 Graph Theoretical Characterization

4.2.1 Collected Data Attributes

In this work, host based data is collected and the 11 data attributes are shown in Table 3. The first and 11th attribute are not acquired but appended. Label is a binary value and is considered 1 for malware and 0 for normal using the knowledge of the executable of each malware sample.

Table 3: Collected attributes from Windows 7 Operating System (OS).

No.	Acronyms	Attributes	Example Values
1	UUID	Unique User ID	009a0542-ccec-4580-a018-5a0898e2cd6c
2	PID	Process ID	4
3	PRN	Process Name	winlogon.exe
4	PRT	Process Create Time	1.31478E+17
5	PPID	Process Parent ID	0
6	MODN	Module Name	authz.dll
7	MODL	Module Path Location	C:Windowssystem32authz.dll
8	PRM	Process Memory	1502964962
9	MODM	Module Memory	192512
10	THC	Thread Count	4
11		*Label*	*1*

This data has timestamps with Microsoft Windows timestamp resolution of 100 nano-second (one timestamp is equal to 100 nano-second). A sample of the data set CSV (comma separated value) file is shown in Table 4.

4.2.2 Transformation of Data Set into Spatially Labelled Graph

The node of the graph represents a string which depicts the following information:

"*PID, Process Name*" OR "*Module Name, Module Location*"

A graph edge will have a parent node and a child connected via an edge. It can be either:

"*PID, Process Name*" → "*PID, Process Name*"

Or

"*PID, Process Name*" → "*Module Name, Module Location*"

In this work, the process tree data set is converted into a directed acyclic graph using algorithm defined in subsection 3.4 where nodes represent the process or module information, while edge represents their inter dependency.

Table 4: Sample Data Set - A Comma Separated Value (CSV) file containing acquired host data.

UUID, PID, PRN, PRT, PPID, PRM, THC, MODN, MODT, MODL, MODM,

.
.
.

ebab22f7-031b-4367-8fd3-41e043424aa2,896,svchost.exe,131490088834343750,504,105164800,18,credssp.dll,C:WindowsSystem32credssp.dll,896,40960,

ebab22f7-031b-4367-8fd3-41e043424aa2,356,svchost.exe,131490088843109375,504,20459520,14,WINSTA.dll,C:Windowssystem32WINSTA.dll,356,249856,

ebab22f7-031b-4367-8fd3-41e043424aa2,1228,spoolsv.exe,131490088851112321,504,12156928,14,netutils.dll,C:WindowsSystem32netutils.dll,1228,49152,

ebab22f7-031b-4367-8fd3-41e043424aa2,1256,svchost.exe,131490088851370135,504,12742656,20,WINSTA.dll,C:Windowssystem32WINSTA.dll,1256,249856,

.
.
.

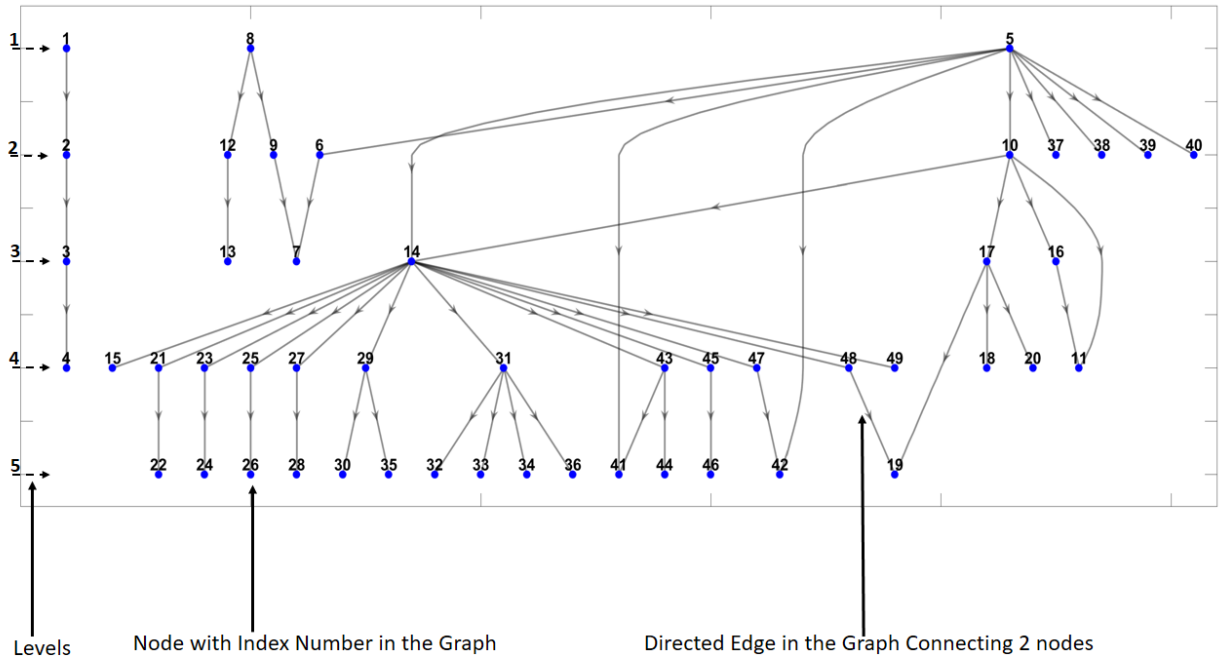


Figure 43: Zeus Malware - Instance 1 - Sample graph of a Windows 7 host having 49 nodes and 52 edges before the execution of malware.

In order to explain the methodology of process tree data transformation into graph structure, an example of Zeus Malware – Instance 1 is presented in this section (data set is available in appendix 7). This transformation process is applied to all malware instances and is not mentioned for each instance for brevity.

The analysis of the process tree graph in Figure 43 for a Windows 7 host before the execution of Zeus Malware- Instance 1 reveals the following significant observations as per subsection 2.7.1:

1) It is an acyclic graph which is a property of tree based graphs having nodes 1, 8 and 5 as root nodes as shown in Figure 43.

2) It is a directed graph where every edge is directed away from the root.

3) It is an unconnected graph as it is a union of multiple connected sub-graphs without having common nodes. For example, sub-graph 1->2->3->4 and sub-graph formed by rest of the nodes.

4) As observed, the process tree graph is found to be a complete graph at any instance of time and only one edge exists between two distinct nodes.

5) There are various depths associated with nodes in the graph. For example, node 17 is at depth of 2 while node 20 is at depth 3.

6) The height of the tree graph is 4 which corresponds to the longest path from the root to the leaf.

7) Also as observed, multiple sibling nodes exist in the graph, for instance, node 12 and node 9 are the sibling nodes having node 8 as their parent.

8) As observed in Figure 44, root node may have either zero or multiple children.

9) The root nodes 1, 8 and 5 represent the first processes initiated when Windows 7 operating system starts. Node 1 represents PID 0 having no process name. Similarly, node 8 has PID 412 having no process name. However, PID 356, which is the node 5 is a svchost.exe process (as presented in subsection appendix 7.2.1).

10) A process can spawn multiple processes which create sub-graph. For example, node 1 (*'0,XXX'*) spawns node 2 (*'4,System'*) which subsequently spawns node 3 (*'288,smss.exe'*) and finally node 4 (*'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'*). This shows the inherent dependencies of Windows 7 operating system on multiple libraries and modules such as smss.exe and system32ntdll.dll.

11) A node can have several incident edges. For example node 19 is represented by *'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'* has incoming edges from nodes labelled as 48 ('1380,svchost.exe') and 17 ('520,lsass.exe') . It shows that node wldap.dll library is used by both svchost.exe and Isass.exe files.

4.2.2.1 Malware Nodes and Edges in the Space Graph

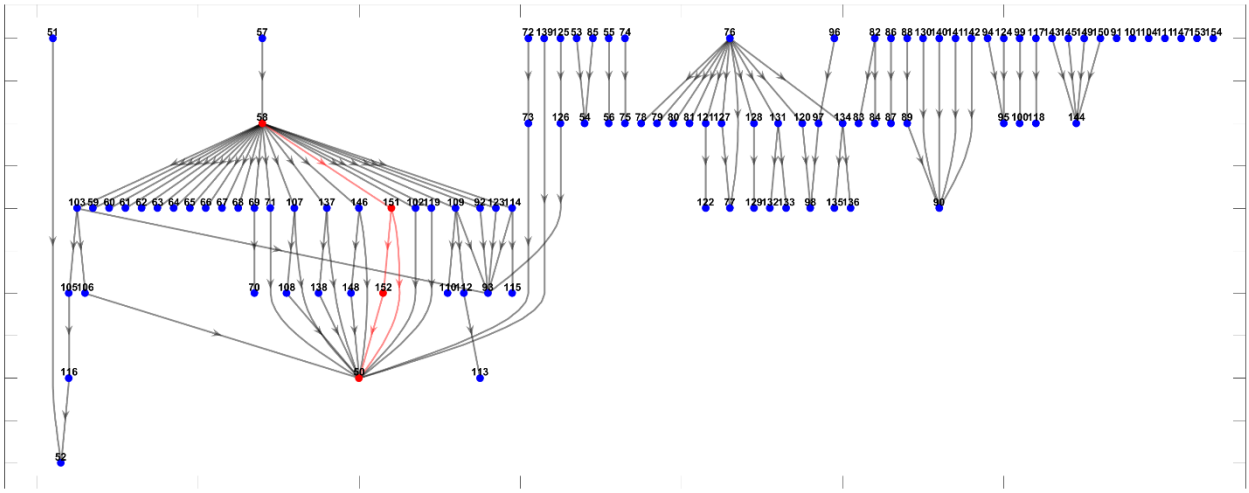


Figure 44: Zeus Malware - Instance 1 - Sample graph of a malware infected Windows 7 host having 154 nodes and 102 edges.

Figure 44 is a continuing graph of Figure 43 which illustrates that the nodes continue to spawn from 50 till 154 with additional 102 edges in total. Node details are presented in subsection appendix 7.2.1 with malware nodes and edges highlighted in red color. Root node 57 ('*1096,xxx*') spawned node 58 ('*1340,explorer.exe*') which is an *explorer.exe* process. Node 151

('*6480,bot.exe'*), which is a true malware process has multiple siblings which are legitimate processes and have node 58 as its parent node. Further, node 151 spawned leaf node 50 ('*wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll*') directly which denotes the accessing of required Windows 7 DLL file used to execute the malicious purpose. Then, node 151 spawned node 152 ('*6484,xusa.exe*'), which is yet another malware process which in turn accessed leaf node 50 and thus creating a parallel path. The reason for this activity in the process graph is due to the inherent Zeus Malware - Instance 1 operation as discussed in subsection 3.3.2.1.

Each malware instance has various PIDs and malware processes/modules, therefore, every node that is either a malware process or module is labelled as positive (label 1). Also, the descendants of the malware node are labelled positive. This is because the descendent node(s) which represent either child process(es) or a module(s) help in completing the malicious intent of the executable. However, it should be noted that a particular module or process may or may not be malicious itself. For example, malware executable may use legitimate Windows 7 module like *wow64cpu.dll* which itself is benign but can be exploited by the threat actors for illegitimate activities. As shown in Figure 44, node 50 ('*wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll*') is considered positive as it is used by malware nodes 151 and 152. However, it is also used by legitimate processes depicted as nodes 108, 138, 148. Since node 50 represents both benign and malicious entities in Windows 7 process tree, it is considered indistinguishable and overlapping node and hence, poses a classification/detection challenge as discussed in detail in subsection 2.5.1. In addition, the malicious process names have been chosen as such to simplify the controlled experiment process, however, in real-world targeted attacks, all the selected malware samples mimic legitimate process names and thus are indistinguishable by their syntactical names (sub-section 2.3).

Further the graph edge, that is a directed path from one node to another, is labelled positive if it contains the malicious node either at one end or both ends. As shown in subsection appendix 7.2.1, the edge number 134 (which connects nodes 58 and 151) is labelled positive because although node 58 represents a benign processes and spawns other benign nodes such as 146 and 107, the edge itself is unique to malware path as well. Further, the edge number 255 (which connects nodes 151 and 50) and edge number 257 (which connects nodes 152 and 50) are labelled positive although node 50 is not a malware node itself. Edge 256 is the malware edge with both parent and child nodes as true malware nodes.

4.2.3 Need of Time Graph

As in any computer operating system generally and Windows 7 operating system particularly, dynamic behavior of a process tree corresponds to continuous update and alteration in its process tree structure due to the creation, removal, and accessing of various other processes and modules. It is therefore, imperative to apply a tool which is able to capture this dynamic behavior with respect to time. In other words, using a single snapshot of the process tree is not enough to characterize the overall behavioral changes in the process tree rather a continuous sequence of process tree graph snapshots are required to depict the run-time evolution in processes and modules

relationship. Therefore, as already discussed in subsection 2.7.3, the selected time graphs act as a convenient tool to study and characterize the temporal progression of process tree states.

Further, using time graph based transformation of process tree, it is also easier to extract meaningful features which can semantically represent the time based progression and evolution effectively. For instance, as discussed in the subsection 4.2.2.1 regarding the Zeus Malware - Instance 1, the process *bot.exe* vanishes after initiating another process with the name *xusa.exe* which indicates that time based features are required to not only capture the dynamic behavior of *bot.exe* process but also characterize its very existence in an evolving time-series of interdependent process tree structure.

Moreover, in the context of existing cyber-security technologies employed in cyber-security operation centres (CSOC) where cyber experts are required to cognitively analyze the heterogeneous network and endpoint data for incidence response and threat-intelligence functions, a time graph based theoretical tool will help them with the data visualization in elegant graph structure format on a time scale [406]. Due to big data challenges, cyber experts are facing an issue of information overload and researchers have begun to find ways to reduce this cognitive load on human experts by proposing new and effective visualization techniques [407]. In this work, it is emphasized that visualization should be supported by convenient characterization methodology to reduce further analytical load on human experts by providing semantic tools using the time based graphical methods.

Further, it is necessary to select time windowing technique that is statistically valid and thus can be generalized. Therefore, an adaptive and sliding time windowing algorithm is used to create ten different time series of the datasets and statistical validity tests are applied to evaluate statistically optimized time series.

4.2.4 Extracting Features from Time Graphs

In this research work, thirteen different nodes and edges based features from time graphs are extracted systematically by preserving the unique graphical characteristics [408] which may act as indicator of exploits for the CSOC team as discussed below. The criteria for the selection of following graph based features for Windows 7 process tree is already described in subsection 4.1.

4.2.4.1 Edge Features

1) Edge Count (ECTS): An edge represents an interconnected link between parent/child processes and process/module. The feature *edge count* indicates the presence of an edge in a time window. It means that if an edge exists between two nodes in a time window state then it will be assigned a value of 1 and if it disappears in any future window this feature will hold a value of 0. Assume, there are four nodes *A, B, C,* and *D* in a graph such that an edge exists between A→B, A→C, and C→D. If for instance, the edge A→ B is present in

window 1 and 5 while disappeared in the other windows and the edge A→ C exists for window 2, 3 and 4, and the edge C→D is observed in all 5 windows then the feature *Edge count* will hold a value of 1 in time windows 1 and 5 corresponding to the edge A→ B. Similarly, this feature will be 1 for edge A→C during time windows 2, 3 and 4. However, for edge C→D the feature *edge count* will hold a value of 1 throughout all time windows indicating its presence of the entire time span.

2) Edge Memory (EMTS): This feature represents the total amount of memory allocated by the parent node to a child process or a module in the relevant time window which is illustrated as an edge between parent and child process/module in the graph. It means that if a node does not have an edge associated with it then this feature will be considered non-existent (zero). Also, if a node has two child nodes then an edge memory feature will be associated with each of them which denotes the memory consumed by that particular module/process as allocated by the parent process. For example, consider that six nodes exist in a particular time window such that one of the parent node *X* does not have any child and while the other two parent nodes *A* and *B* have one and two child nodes forming the edges A→C, B→D, and B→ E such that each have corresponding memory bytes *m1, m2*, and *m3* associated with them respectively. Suppose, the edges B→D, and B→ E appear in time window 1 only while the edge A→C exists for time window 3 and 4. In this case, the feature *edge memory* will have non-zero values of *m2* and *m3* corresponding to edges B→D, and B→ E respectively for time window 1. Whereas, the value of *m1* will appear for the edge A→C for time window 3 and 4 and will be zero otherwise.

3) Edge Time (ETSD): The relationship between a parent-child process nodes and process-module nodes is represented by an edge that evolves with respect to time in a process tree time graph. It implies that these interconnections may form or die over time due to dynamic changes in the process tree graph. The *edge time* feature captures this dynamic aspect by recording the total time for which the edge exists in terms of 100 nano-second ticks in each time window. It is measured as a time difference from the minimum time of the process tree (the time when the operating system starts). To further elaborate, consider a graph with four nodes *A, B, C*, and *D* having edges A→B, B→C and A→D in a time-window. Let us assume that the edges A→B and A→D appear immediately in the process tree having zero time difference with the minimum time of the process tree while the edge B→C appears after *t1* time ticks with respect to the minimum time. Then, in this case, the feature *edge time* associated with edge A→B and A→D will be 0 for that particular time window while it will be *t1* for edge B→C.

4) Edge Thread Count (ETTS): A thread is created by the operating system when a module is accessed by a process node in a Windows 7 based process tree graph. This is re-enforced with the observation that the thread count is non-zero only when a process tree graph leaf is reached otherwise this value remains zero. Generally, the leaf in a particular path in process tree graph represents a module. Therefore, this feature keeps a track of total number of threads created during the retrieval of a module in a particular time-window. So, for example if process node *X* spawns a child process node *Y* which then eventually accessed

module *A*, then there will be two edges in the graph (i.e. X → Y and Y → A) such that each of them will carry a value corresponding to *edge thread count feature*. However, it is important to note that ETTS will be non-zero only for the edge between *Y* and *A (*Y → A). Also, any update in terms of increment or decrement in the thread count is reflected by this feature as long as the edge exists in that particular time window. However, the value is reset to zero if the edge disappears from a time-window.

5) Number of Edges per Timestamp (TSNE): As the presence of an edge in a process tree graph represents the existence of either a parent-child process relationship or a parent-module relationship, this feature aggregates presence of all edges in a particular time window. This means that this feature will keep a count of total edges which exist in a particular time window. For example, if there are 5 time windows of process tree graph such that each of them has total edges count of 3, 7, 9, 2, and 15 respectively then, these values will be stored as the feature *number of edges per timestamp* corresponding to each time window.

6) Edge Repeat (TSER): An edge represents a relationship between a particular parent process and its spawned child process or the accessing of module by the parent process. In a time graph having multiple time windows, this feature depicts a repetition count for all the edges which exist for the entire time span. It implies that when an edge exists in a time window for the first time, then it is assigned a count of 1 which is incremented with its presence in future time-windows, if it appears. To further elaborate, consider that an edge exist between hypothetical process node *A* and *B* for time window 1 till 6. Therefore, the edge repeat will be 1 for window 1, incremented to 2 if it exists in window 2 and so on and so forth until time window 6 when counter will reach a value of 6, if the edge exists in all time windows. Also, if an edge does not exist for a time window although it was present in the previous time window, the count will not be incremented but will retain its previous value. This means that if this particular edge appears again in any future time window, the counter will increment again from its previous value, keeping a time based information about the inter-process and process-module based relationships. It is important to note that a counter is attached to individual edges and therefore, the feature of e*dge repeat* represents edge count for each edge ever appeared in the process tree for the entire time span.

7) Number of Edge Memory per Timestamp (TSEM): As discussed, a parent process is responsible for the allocation of memory for child process or the module which in this work is represented by an attribute attached to the edge between the nodes. However, there are processes which may not have a child process/module attached to it and therefore, the edge will carry a zero memory value (or, an edge will not exist) which indicates an unallocated memory space. This particular feature counts the number of times all such processes (where the memory has been allocated which is indicated by the presence of an edge in a particular time window) repeat for the entire time span. For instance, consider that there are four hypothetical process nodes in a time-window where one of them i.e. node *X* has no child and the other one i.e. node *A* has two child nodes *B* and *C* (forming edges A→ B and A→ C). Suppose, all of these nodes along with their edge relationships exist for three future

time-windows then the *number of edge memory per time stamp* for each of the edge i.e. A→ B and A→ C will be 3.

8) Number of Edge Time per Timestamp (NTSE): The dynamic inter-process and process-module relationship which evolves with respect to time in terms of addition and removal of edges/nodes on graph is captured by measuring the time difference between the time of the first appearance of an edge in a particular time window and the minimum time of the process tree graph. The feature *number of edge time per timestamp* represents an accumulation of the count over all time windows for which the time difference was non-zero with respect to each edge. Let us assume that there are three nodes *A, B,* and, *C* such that an edge exist between A→B and A→C. Say, A→B has an edge time of *t1* in time window 4 while A→C has an edge time of *t2* in time window 1. Then the feature *number of edge time per timestamp* will have a value of 1 corresponding to each of the mentioned edges over the entire time span.

9) Number of Edge Thread per Timestamp (TSET): The creation of a thread corresponds to the accessing of a module by the process node and is reflected in the graph as the presence of an edge. This feature accumulates over time, the count of all such edges which connect a process node with a module node and therefore, possess a non-zero thread count. So, for example, consider that there are six nodes present in a graph such that two of them are parent nodes. The first parent node *X* has one child node *Y* which retrieves another module node *Z*. Similarly, the other parent node *A* has a child process node *B* which is linked with a module node *C* by an edge. There are total four edges in the graph i.e. X→Y, Y→ Z, A→B and B→ C such that the edges Y→Z and B→ C will have a non-zero thread count value. Assuming, edge Y→Z repeat itself only twice while edge B→C is present for the next four time-window out of total seven time windows then, the feature *number of edge thread per time stamp* will have a value of 2 for Y→Z, 4 for B→ C and zero for the other two.

4.2.4.2 Node Features

10) Node Count (CNTS): The node in the process tree graph represents a string tuple formed by the combination of either a PID and parent/child process name or a module name and its location. It is important to keep track of the nodes that appear in each time window to define the birth and death of the processes and modules in a time graph. The feature *node count* verifies the presence of a particular node in a fixed time window. If the node is present the feature is assigned the value of 1 otherwise, it is 0. For example, if there are two nodes *X* and *Y* in a graph such that node *X* appears in time windows 1, 2 and 3 while node *Y* appears in time windows 3 and 4. Then, in this scenario the feature *node count* will have a value of 1 for node *X* corresponding to time windows 1, 2 and 3 and zero otherwise. Similarly, node *Y* will be assigned a *node count* value of 0 initially for time-windows 1 and 2 but later it will have a value of 1.

11) Node Neighbor Count (TSNN): A neighboring node signifies an immediate process or a module spawned or accessed by the parent node. In terms of graph, keeping track of neighbors helps form unique path from root to the leaf in a tree which depicts the spatial evolution and often aids in determining the originating point of an activity. The feature *node neighbor count* sums up all the nodes which are at a distance of one edge from a particular node in a time window. Assume there are five nodes in a graph such that node *A*, *B*, *C*, *D*, and *E* are connected by edges A→B, B→C, A→D and A→E in a particular time window. So, the feature *node neighbor count* will have values of 3, 2, 1, 1, and 1 for nodes *A*, *B*, *C*, *D*, and *E* respectively in that time window.

12) Number of Nodes per Timestamp (TSNC): As mentioned, the presence of a node indicates a new process or a module and the count of all such nodes in a particular time window is stored in the feature *number of nodes per timestamp*. So, this feature keeps a track of the evolution in the nodes which may be an indication of a change or activity. Consider that there exist 3 time windows each having a total node count of 14, 25, and 9 respectively, then these values will be assigned to the feature *number of nodes per timestamp.*

13) Node Repeat (TSNR): The process/module node count over the entire time window span is kept as a feature *node repeat*. It determines the number of times a particular node exists in a process tree graph. This count is initiated with 1 when the first node is encountered. The value is incremented after every appearance of the node in any of the future time windows. Therefore, if a node is present in the current time window but is not found in the next time window then the *node repeat* will retain the last count value. If the node is present in any of the future time window, the count will start from its previous value. So, for example if a node *X* exists in time window 1 and 2, but vanishes from time window 3 and re-appears in time window 4 and 5. Then, the feature *node repeat* will have a value of 4 at the end of time window 5.

Table 5: Summary of time graph features.

No.	Feature Definition	Feature Notation	Notation Definition
1	Edge Count	ECTS	**E**dge **C**ount vs. **T**ime **S**tamp
2	Edge Memory	EMTS	**E**dge **M**emory vs. **T**ime **S**tamp
3	Edge Time	ETSD	**E**dge **T**ime **S**tamp **D**uration
4	Edge Thread Count	ETTS	**E**dge **T**hread vs. **T**ime **S**tamp
5	Number of Edges per timestamp	TSNE	**T**ime **S**tamp vs. **N**umber of **E**dges
6	Edge Repeat	TSER	**T**ime **S**tamp vs. **E**dge **R**epeat
7	Number of Edge Memory per timestamp	TSEM	**T**ime **S**tamp vs. **E**dge **M**emory
8	Number of Edge Time per timestamp	NTSE	**T**ime **S**tamp vs. **E**dge **T**ime
9	Number of Edge Thread per timestamp	TSET	**T**ime **S**tamp vs. **E**dge **T**hread
10	Node Count	CNTS	**C**ount of **N**odes per **T**ime **S**tamp
11	Node Neighbor Count	TSNN	**T**ime **S**tamp vs. **N**ode **N**eighbor
12	Number of Nodes per timestamp	TSNC	**T**ime **S**tamp vs. **N**ode **C**ount
13	Node Repeat	TSNR	**T**ime **S**tamp vs. **N**ode **R**epeat

4.2.4.3 Significance of Selected Features

In the context of graph based cyber security model, cognition is defined in terms of change detection such that the change should correspond to the existence or activity of an anomalous object that may or may not be legitimate (true positive or false positive where positive represents malware object or its characteristics). Therefore, an advanced feature extraction based on fractal complexity measures is employed on each of the above individual features for cognitive characterization of malware and is discussed in subsections 4.4 and 4.5.

An operating system (OS) requires resources such as memory and CPU cycles to carry out system operations and execute application programs. The consumption of these resources by the OS is through the creation, deletion, modification and/or retrieval of processes and modules, which represent a systematic execution of files and their dependent libraries. A time based representation and analysis of the utilization of these resource provides an in-depth information of the dynamic behavior of the operating system which aids in characterizing any peculiar changes in the system. A change essentially signifies the deviation of the operating system and its resources from the a-priori behavior observed over a course of time and is an indication of the presence of anomaly which is a relative concept and requires cognitive attributes to be attached to it. In the domain of cyber security, these cognitive attributes should be able to sufficiently differentiate threats from normal behavior. To detect a change point in this research work, thirteen different features derived from the time based graph structure are combined together in the following categories with respect to the computing resource consumption:

1) Statistics of graph nodes (process/modules).
2) Statistics of graph edges (process to process or process to module relationship).
3) Statistics of Threads.
4) Statistics of starting time for nodes and edges.
5) Statistics of memory consumption.

The statistics of graph nodes which represent a module or a process denote changes in the process tree graph as a result of any modification in these entities. Precisely, it captures the birth and death of the processes and modules consumption which can act as an indicator of compromise in case of a cyber-threat. From the perspective of threat-actor who intends to invade a system to execute the malicious intent by exploiting operating system resources, this group of feature (graph nodes) will depict a change in its statistics like an increment or decrement in count e.g. malware Stabuniq and Proteus (subsection 2.3). For example, to successfully execute a malicious executable, an attack should be curated such that it creates a number of legitimate processes by executing various applications and modules while introducing a single malicious process with a legitimate name (mimic legitimate process behavior) within these normal processes. This characteristic will help to hide the malicious process from the cyber-security expert who may be observing the system process tree logs at that moment. The proposed system however, can generate

an anomaly flag in such situation while providing the identification of time window in which the change appears that can speed up and ease the analysis efforts of a cyber-security expert.

Moreover, the establishment of relationship between nodes illustrated by edges in the graph indirectly represents an increase in utilization of operating system resources. In other words, the measurement of node and edge statistics can indicate the occurrence of a stealth activity hidden in the intricate neighborhood updates or in a process tree path from root to the leaf. This is observed for advance malware which themselves do not utilize system resources to appear as an innocent object and rather offload their malicious tasks to their child process which can in turn carry out the malign objectives e.g. malware Zeus and Citadel (subsection 2.3). Hence, the presence of a node which tends to have numerous relationships with other nodes/modules or the occurrence of multiple parallel paths from a particular root node to the leaf node can indicate a change event which may correspond to an anomaly. Hence, these combined node/edge statistics can act as an indicator of compromise helping the cyber-threat defender team in their investigation of suspicious observations.

Further, it is important to keep a record of the statistics related to the process/module activity with respect to the initial operating system time. This is because such measurements help reveal the behavior of anomalous processes which may initiate at the boot time but remain dormant before finally beginning to fulfill the malign objectives. This time delay is often introduced by the malware authors in the malicious code to give an impression of legitimate behavioral patterns by the executable. Simply, these delays morph the behavior of malware in such a way that they appear to be benign and are able to evade detection. Also, recent advanced malware are able to detect the presence of surveillance which require the execution of actual piece of code to be delayed that can be captured with this attribute e.g. malware Alina and Zurgop (subsection 2.3). In addition, the exfiltration from a system often takes place at regular time intervals and is usually controlled by the threat actor from the command and control server. The time difference parameter of the system can also reveal the occurrence of such activities in the system. Therefore, the time delta related feature is extremely important to be included in the set of concurrent system observations [409] by the security experts to detect any change point which may lead to the discovery of a true anomaly.

Likewise, the statistics about the thread and memory utilization depict the granular level resource consumption like the CPU load and storage changes. It is important to log the patterns shown by these operating system resources as a number of latest malware are fileless and complex in structure e.g. malware Poweliks, Hupigon and Nivdort (subsection 2.3). Being fileless means these exist only in the memory and are not apparently visible in the process tree graph. So, the activities of these malicious software can be characterized by a sudden change in the memory state or a continuous memory engagement without the presence of corresponding process/module nodes in the system indicating an irregular pattern. Moreover, malware with large number of modules create multiple corresponding threads which is an indication of intricate structure of the malicious code which in turn can act as an indicator of compromise for targeted attacks which are often state-backed and are sophisticated.

Usually, a valid change in the system is retracted when the particular user-initiated process/module is removed and does not re-appear without manual intervention (execution). Contrarily, mutating malware display a persistent behavior in the sense that when their corresponding process/module is manually (by a cyber-defender) or automatically (by an antivirus) deleted, it resurfaces in the process tree graph mimicking the behavior of system processes. This pattern is also observed upon the system reboot where the malignant node/edge recur. Therefore, to support the threat-investigation process, binary node/edge features along with other statistical properties of edges/nodes are also evaluated in this study which indicate the presence and absence of an entity (node) or a relationship (edge). The analysis of these indicators of exploits (IoE) over time with respect to different time-windows clearly shows a differentiating behavior for false and true anomaly. In case of the former, the node/edge once erased never re-appears in the future time-windows whereas for a sophisticated attack it returns causing modified node/edge statistics.

It is worth-mentioning that due to the complex and refined modular code structure of mutating malware which gives rise to the multifaceted behavior, it is necessary to consider a set of different graph based features at any instance of time. This is because none of the features alone can accurately and completely characterize every possible malware behavior [9] which often consists of highly varying activity patterns in a system and thus depend on human cognition for detailed manual analysis after alert (positive or negative) generation. The dependence on human cyber threat-defenders refers to the requirement of continuous manual threshold modification which is different for each malware samples within and across malware families [410] [8] [411] [412]. This challenge was also faced during the execution phase of this research work. As a result, a second set of fractal features derived from these primary graph related features are proposed and their viability was experimentally tested using all the ten malware samples considered in this dissertation as mentioned in the sub-section 2.3. Through this different ensemble of various advanced malware samples, it is possible to attach a high confidence level for an empirical cognitive characterization of threats. On a side note, in a practical environment these statistics can be of any order including but not limited to mean, variance, and standard deviation which depends on the requirements of necessary details by the cyber threat team to characterize a threat. Therefore, the set of features discussed in this thesis are expected to serve as a foundational ground for the cognitively derived features in the domain of host operating system process tree based cyber-security.

4.2.5 An Example Illustrating Extraction and Characterization of Proposed Time Graph based Features

In this subsection, extraction of thirteen time based graph theoretical features from raw data attributes as mentioned in subsection 4.2.1 is described. In particular, an example of Zeus Malware – Instance 1 is used to elaborate the data sampling process, where a fixed sliding and non-overlapping time window resolution (called as lag) increases by an order of 10 factor gradually from 1 microsecond time lag to 1000 second time lag for each time series respectively. For example, for the first time series, the starting sample of each consecutive fixed sliding window increases by 10 samples and for the second time series, the fixed sliding window increases by 100 samples and so on. However, the finish time of each sliding time window in each time series is based on the validity of time window local stationarity using identification of valid fractal dimension, therefore, the individual window size is not fixed.

4.2.5.1 Adaptive and Sliding Time Window

As shown in appendix 7.1, for each of the 13 features of all malware instances, the data set shows high sparsity, which necessitates the requirement of irregular and sparse time sampling [413] [414] using adaptive and sliding window mechanism. For brevity, a plot of the percentage of non-zero data of the 6 features from appendix 7.1 for each malware data set is shown in Figure 45. As can be seen, the minimum and maximum ratios of the non-zero values is shown in each data set which is bounded below 10% and mostly reside within less than 8%. Therefore, all data set are highly sparse and require sparse sampling methods. Sparse time sampling does not assume that the time series shows uniform and non-overlapping time samples and therefore, the time windows are not the same size and do overlap. Further, as mentioned in subsection 4.5, data set for each malware shows heavy tailed distribution, that indicates the presence of many outliers. Therefore, due to these challenges, it is not possible to use regularly spaced and non-overlapping (windows) time sampling where each window has uniform size. In order to capture the dynamics of a sparse and heavy tailed distribution time series, an adaptive and sliding window algorithm is suitable, which will capture the dynamic changes more effectively and meaningfully.

Time series analysis is based on stochastic stationarity principle [12]. Without establishing the stationarity of time series [330], it is not possible to infer meaningful analysis of time series dynamics. Sampling of time series requires that the sampled time window should at least show statistical weak sense stationarity which is akin to finding the optimal time window size [415]. Therefore, in this work, time graphical models are validated against weak sense stationarity locally (due to being heavy tailed) using variance fractal dimension algorithm as defined in sub-section 3.4.3. This algorithm is used to extract valid multiscale fractal dimension based on statistical variance and provides an elegant mechanism to validate the stationarity of selected time sample window [12].

In order to find an appropriate adaptive time window that renders weak sense stationarity in a continuous fashion, it is necessary to divide the time series in windows of variable data samples where each window size should be selected such that stationarity of chosen samples is preserved. As defined in sub-section 2.6.3.4 and [12], variance fractal dimension is mathematically based on Hurst parameter and for a single measureable parameter, the valid variance dimension varies between 1 and 2. Any value greater than 2 or less than 1 is considered an effect of non stationarity since it does not represent the valid mathematical bounds of 1 and 2 [12]. Therefore, using this method, an adaptive time window can be selected where the time window size is dependent on the valid values of variance fractal dimension calculations. It is noted that this adaptive time window selection constitutes overlapping time windows since the consecutive time windows will have variable size and may overlap the previous window based on the number of samples in that window [416].

Based on earlier work in [12], the adaptive time window algorithm is already mentioned in the subsection 3.4.2. A pictorial representation of the time sampling procedure is shown in Figure 46 where discrete samples are divided into variable width time windows based on stationarity calculations and also have fixed sliding lags for the consecutive increments in the time windows. As can be seen, the width of windows (e.g. $\mathrm{Window}_1, \mathrm{Window}_2$) is dependent on finding the valid fractal dimension that should lie between 1 and 2. For example, after executing Window_1, the Window_2 starts at Δ_1+1 sample and then it keeps incrementing for each sample. While incrementing, it will estimate the VFD per increment and if VFD is found between 1 and 2, then it will stop at that sample to finish the width of the Window_2. It should be noted that this window estimation is adaptive in the sense of finding VFD based local stationarity, that takes into account removing noise and saturation during fractal dimension estimation [12]. Further, this window width estimation takes into account the samples from previous window size and is therefore, overlapping.

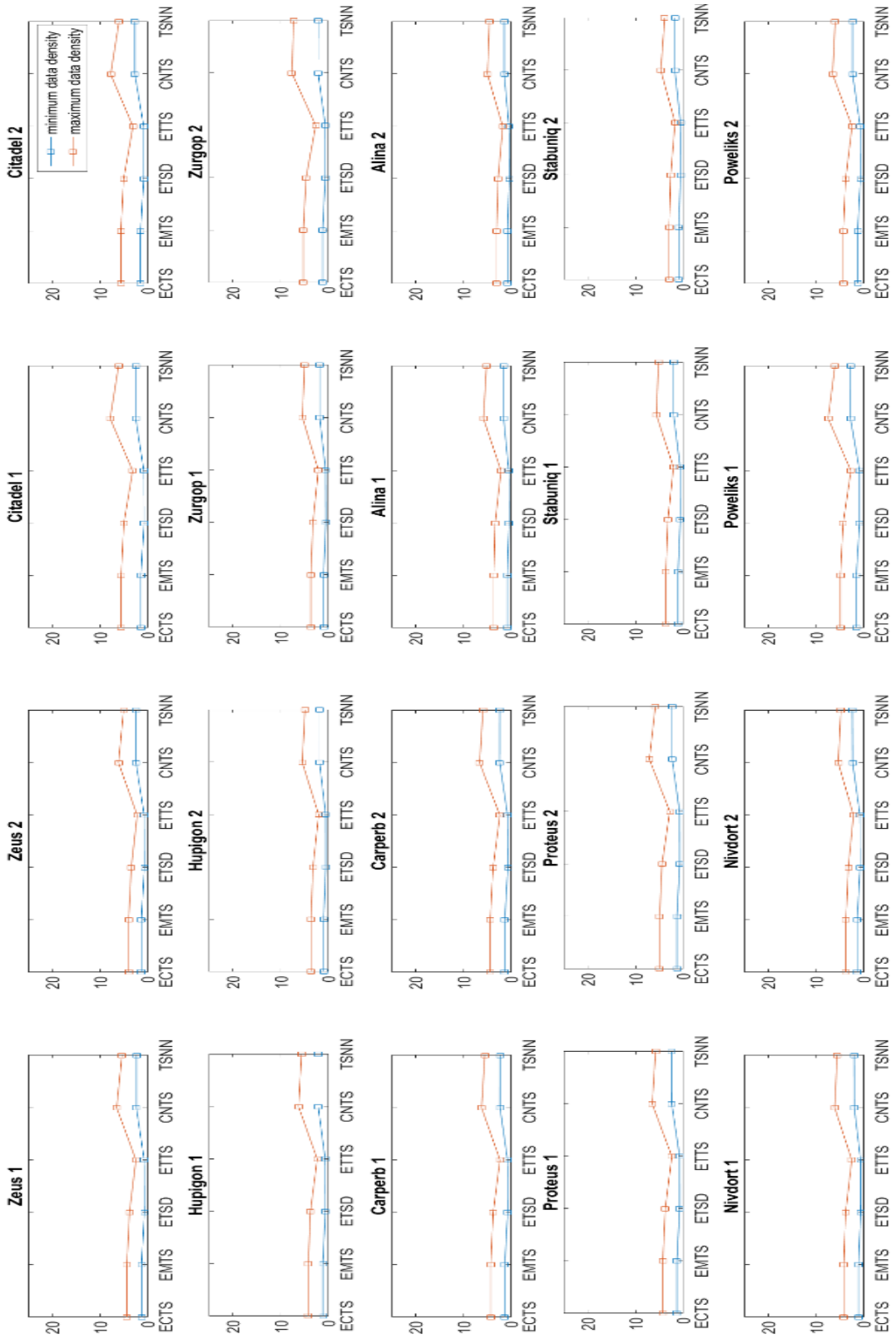


Figure 45: Data density of the features ECTS, EMTS, ETSD, ETTS, CNTS, TSNN.

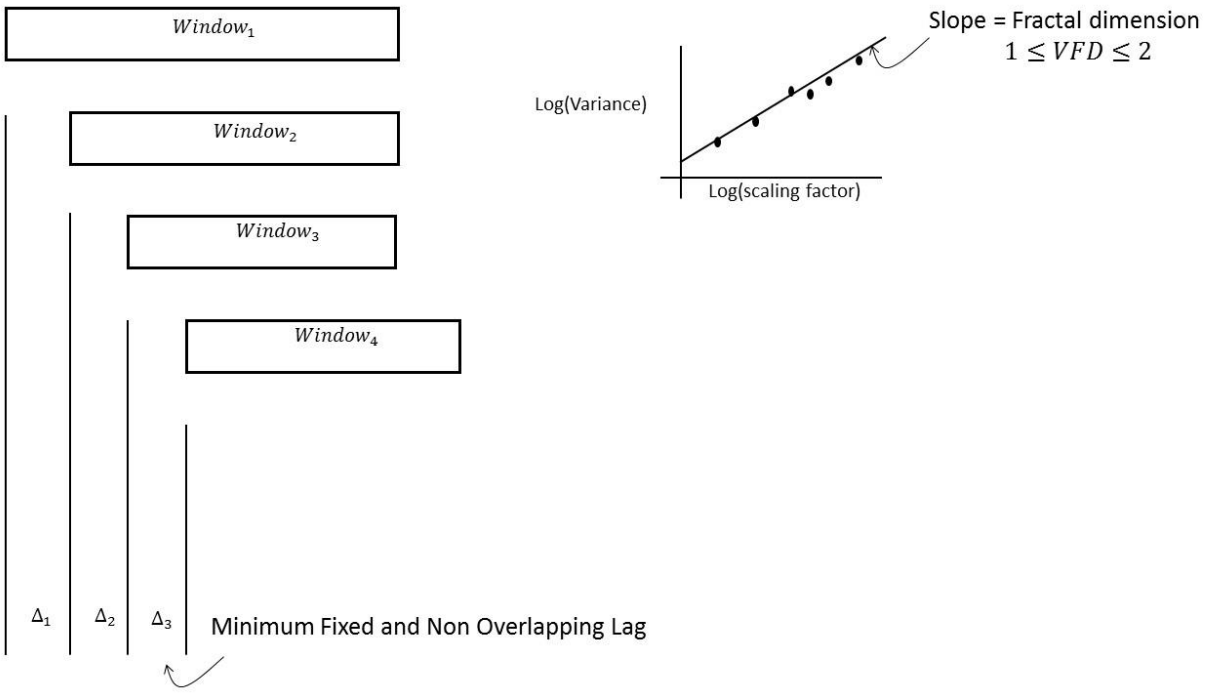


Figure 46: Adaptive Time sampling method showing fixed size lags and variable window sizes.

4.2.5.2 Effects of Varying Sampling Window Lag on Adaptive Time Window

In this subsection, an analysis of the effects of varying time window lag in time graph is illustrated and discussed by considering the already discussed example of Zeus Malware – Instance 1. The details of the data set is available in subsection appendices 7.1.1 and 7.2.1. A sample pictorial representation of the Zeus infected process tree graph data is available in Figure 47 to Figure 49 which depicts three different sampling instances with respect to the increasing time window lag (10 samples per 100 nano-second timestamps, 10,000,000 samples per 100 nano-second timestamps, and 10,000,000,000 per 100 nano-second timestamps repesetively). For brevity, only initial fourteen time window samples are shown in each figure. However, due to the increasing value of window lag, Figure 49 has only six windows available which is the largest window size in the experiment. These plots help visually realize the temporal evolution in the graph structure along with malware nodes and edges and can be conceptually considered as a foundational core for dynamic analysis of time series based graph edges and nodes. Also, it is noted that the method described in this subsection is unequivocally applied to all data sets. Further, the labelling is assigned in such a way that the existence of one or more malicious nodes or edges in a time-window causes it to be classified as malicious.

There are following important observations:

1) A time window consists of selected graphical structure i.e. nodes and edges with their corresponding timestamps. The selection of these time instances is obtained through adaptive sampling intervals with lags varying from 10 to 10^9 units (where 1 unit = 100 nano-second). For example, in Figure 47, time window 5 shows a relationship among nodes 10, 14, 16, 15 and 11, but there is no information regarding the nodes 1 to 9 which are shown in the previous time windows of 1 to 4. It is because each time window has relative information related to the samples appearing for the duration of that particular time window state. In short, only the samples that exist for the duration which directly corresponds to the start and end time interval are selected to appear in the respective time window [12].
2) It is observed consistently in all malware instances (not illustrated) that for first few time graphs, where the minimum, non-overlapping time window lag (refer to Figure 46 for time lag description) varies from 10 samples per 100 nano-second time window to 100,000 samples per 100 nano-second time window respectively, time graphical model shows similar behavior because of the very small time lags. The rationale for this observation is due to the selected small time lag which for each adaptive window size results at the same ending stationary point for each time window until the lag value exceeds the previously determined stationary point. This is further attributed to data sparsity which shows consistent behavior for small time intervals [416]. Therefore, due to data sparsity and overlapping non-uniform time windows, it is not expected that each evolving time window in a time series provides unique and different graph objects.
3) For each new time window in a time series, it is discovered that a particular process node evolves as the new child processes/modules are spawned creating new linkages (edges) in the graph. For example, in Figure 47, time window 4 and 5 shows that the graph of process node 10 evolves from path (10→14→15) to two distinct paths (10→14→15 and 10→16→11) depicting the addition of a child process and the retrieved module.
4) As time window evolves with respect to time, it is not necessary that the path from a root node shows a complete evolutionary portrait of the node from the beginning rather it captures and displays the most recent activity which occurred in the process tree for that time instance. For example, consider time windows 4, 5 and 6 in Figure 47, the path of node 10 in window 6 only shows connections between nodes 10, 16, 11, 17, 15, 19, and 20 which is depicted by edges 10→16→11 and 10→17→(15, 19 and 20) while ignoring its previous path which consisted of nodes 10, 14 and 15 i.e. edge 10→14→15. It is necessary to reveal only the recent related activity while avoiding information overload. However, in case of a need to review previous states, this information may be available (using data logs) that can be combined with the latest time window information to paint a bigger picture that can show relatively complex relationship for CSOC cyber experts.
5) The variable time window size itself poses a challenge as evident by the comparison between Figure 47 and Figure 49 where in the former figure, the large number of time windows capture the graphical system details in numerous separate smaller windows which themselves carry lesser information and therefore, clearly show the evolutionary behavior on micro scale. On the other hand, the later mentioned figure depicts the entire system information in one big chunk of the time instance thus, making it difficult for the cyber-security analyst to accurately

pinpoint the anomalous change in time. However, having relatively large time window provides a macro behavior of the process tree. Therefore, there is a trade-off between the size and the number of time window instances which should be carefully selected based on both the mathematical and cognitive rationale and are addressed in sub-section 4.2.5.4. In this dissertation, the lowest time window lag i.e. 10 samples per 100 nano-second time window, is selected for characterization.

It is important to note that the use of adaptive sampling intervals with small lags, helps in visual analysis which is aimed at empirically determining the most suitable time window which would be appropriate to detect malware conveniently and reliably. This convenience is related to the human cognitive analysis because having a large time window would make it difficult for the human experts (CSOC team members) to search the entire graph space for malicious object which may be hidden under normal/legitimate graph objects as the dataset depicts an over-lapping property (as can be observed for each figure having malware nodes). Also, this subsection provides support in terms of realizing the challenge of information/cognitive overload [417] in a particular time-window that may results in overlooking the malicious sample due to the big data challenges.

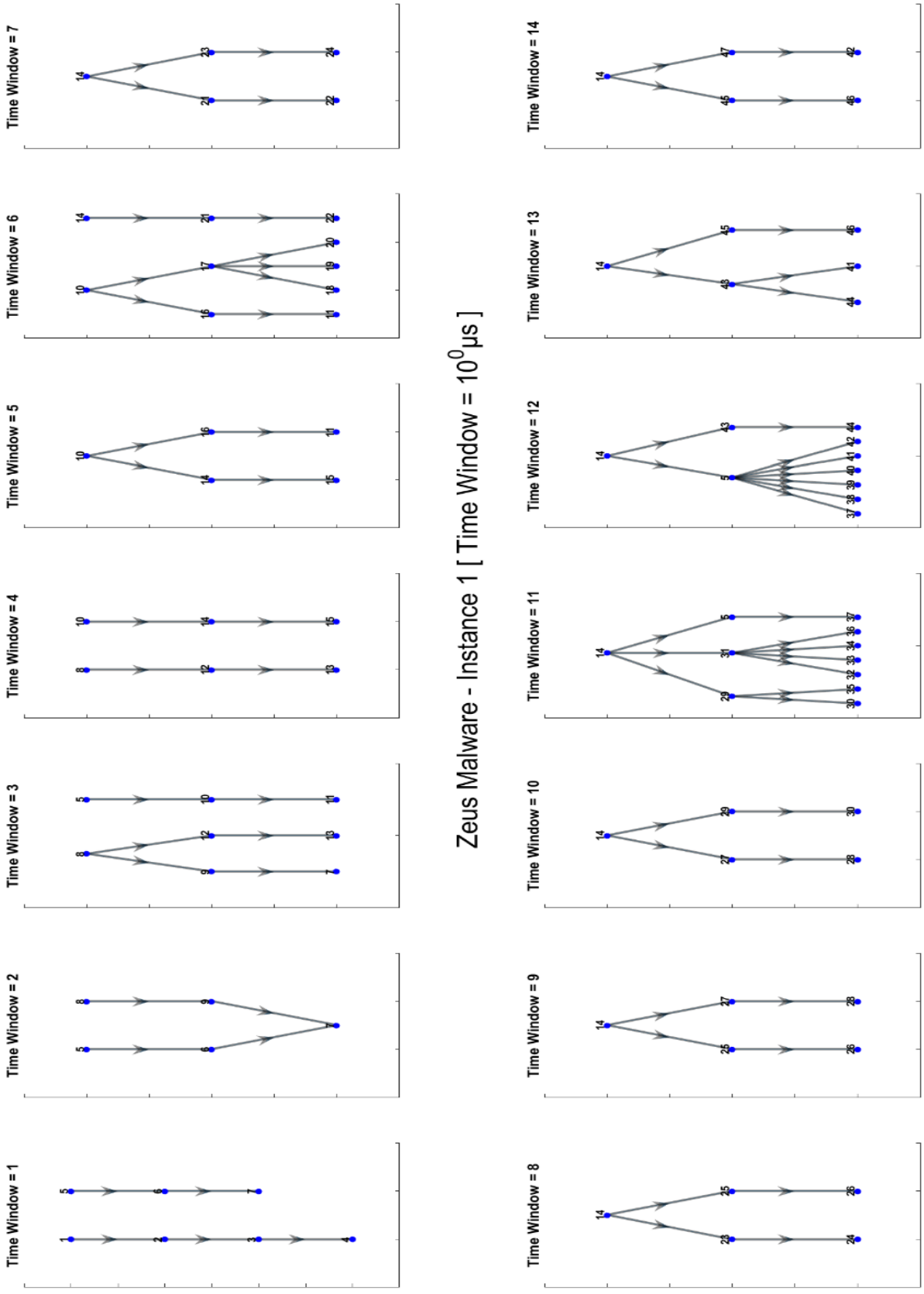


Figure 47: Zeus Malware – Instance 1 – 14 consecutive timestamps (10 samples of 100 ns each per time window).

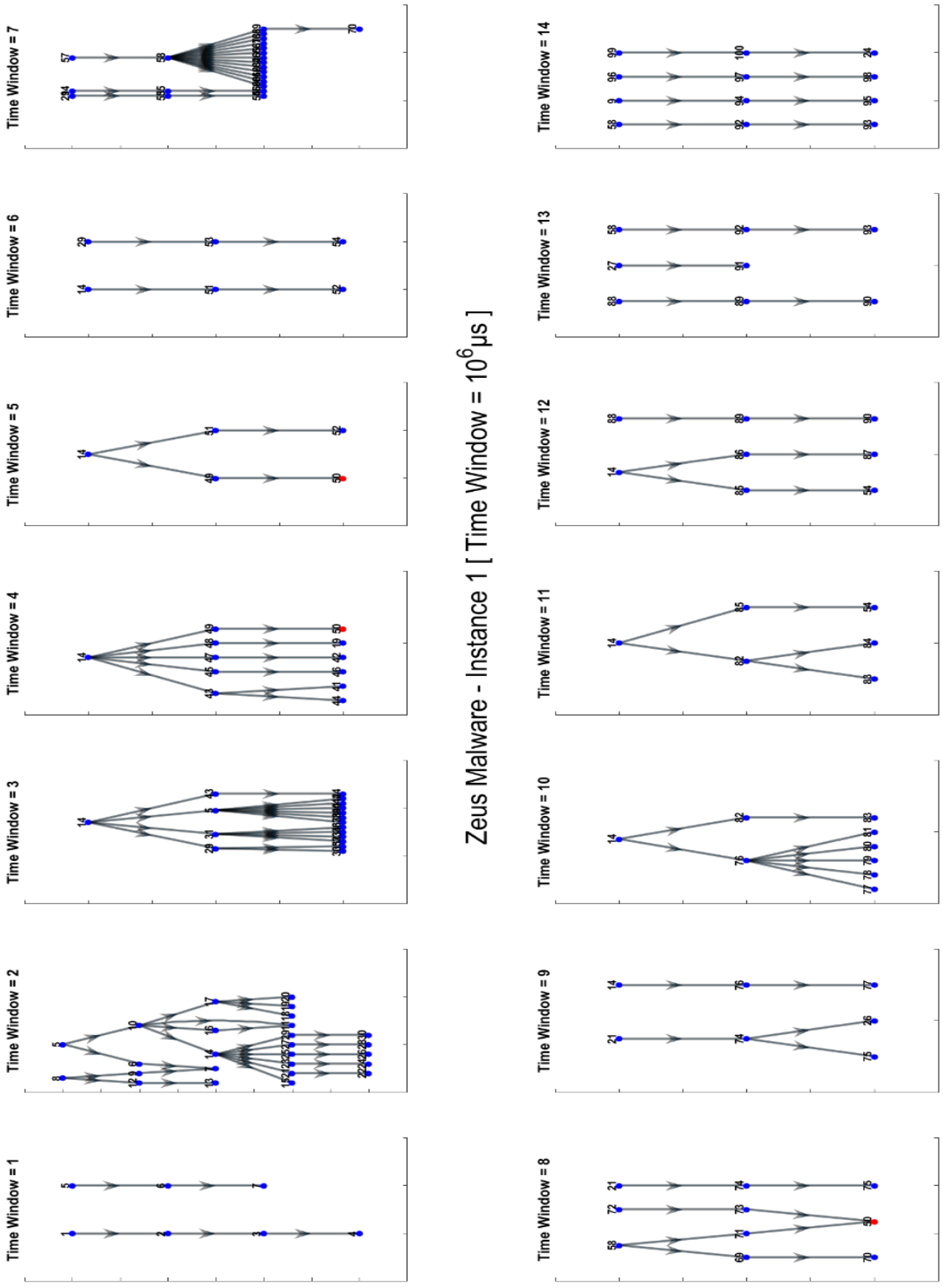


Figure 48: Zeus Malware – Instance 1 – 14 consecutive timestamps (10,000,000 samples of 100 ns each per time window).

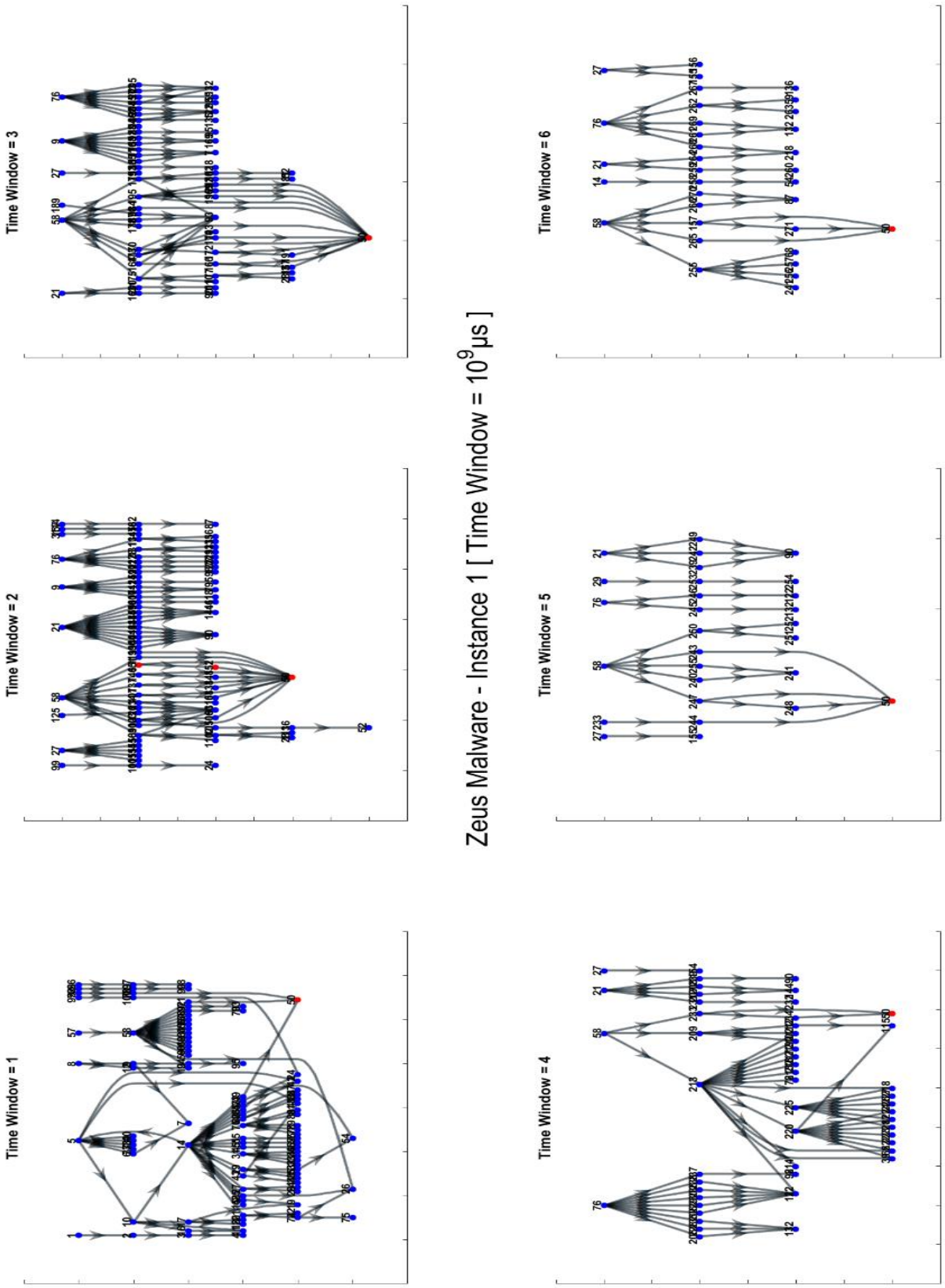


Figure 49: Zeus Malware – Instance 1 – 6 consecutive timestamps (10,000,000,000 samples of 100 ns each per time window).

4.2.5.3 Time Series Analysis for Graph Features

A number of statistical features for the characterization of malicious activity in a process tree graph are discussed at length in subsection 4.2.4. The continuous time based snapshots of these process tree statistics are then labelled in terms of normal and anomalous time windows to pinpoint the occurrence of change in time. The analysis of these statistical changes with respect to time is analogous to the evaluation of time series for the presence of malicious time instance. Considering the simplest and the most straight forward statistical feature of total nodes count and total edges count which are termed as *number of nodes per timestamp* (*TSNC*) and *number of unique edges per timestamp (TSNE)* respectively, a continuation (from subsection 4.2.2.1) of example using the dataset of Zeus Malware – Instance 1 has been illustrated in Figure 50 to Figure 52 and discussed below which can be further extended to other features in the same way.

Following important observations have been noted:

1) To achieve a class balance in a feature in terms of ratio between malicious and normal samples, inclusion of module level information (node number 50) in addition to the parent and child process (node number 151 and 152) information is necessary. This inclusion of module information basically gives rise to the *number of nodes per timestamp* measure corresponding to the anomalous/normal nodes and consequently improves the data class balance as encountered in cyber domain. For example, a comparison between Figure 50 where only parent and child process nodes are considered and Figure 51 where module related data is included, clearly depicts an increase in the malicious samples which can aid in accurate and reliable characterization of malware processes in an operating system. Also, it is enumerated in Table 6 and Table 7 where the last column depicts the ratio between the malware versus benign nodes that shows a drastic increase in the ratio with the inclusion of module information for the malware characterization.
2) It is worth considering that the Windows 7 modules themselves are legitimate (mostly) and do not show an independent malicious behavior and are therefore, tagged as normal when employing signature based threat detection techniques (having a-priori knowledge of the threat in contrast to detecting unknown threats). However, these modules which are often in the form of a DLL are exploited by the threat actors for their malign intents. Therefore, an analysis of the entire process tree reveals that these modules toggle between normal and malicious states depending on their connection with the parent node which in turn can cause them to be considered as malicious or normal. This characteristic is the root cause of the over-lapping behavior (class inseparability as described in subsection 2.5.1) as observed in the dataset that may result in higher false alarm rate.
3) It is also discovered that at the maximum graph depth which corresponds to the parent process, child process and module relationship, the graph complexity is maximum for both malignant and benign samples. However, at the minimum depth of the graph which means the existence of a single process without any child process/module relationship the graph becomes much simpler for the analysis. But, this simplicity comes with the cost of loss of information regarding the behavioral change in the process tree because of the presence of a malware.

4) The pictorial representation in Figure 51 reveals that with the increase in time window size, a macro level complexity of the time series becomes evident whereas reducing the window size decreases this complexity showing micro level information. From the perspective of cyber-expert this combination of information from different scales may benefit in accurately characterizing the malware instance while systematically managing the system's resources consumption as necessary for quick analysis.
5) Another edge based count feature which is termed as *number of edges per timestamp (TSNE)* that represents the total number of edges present in a time window is evaluated in this sub-section. As observed in Table 8, the ratio between malware and normal class is extremely small i.e. in the order of about 3% for most of the time windows except the last one. This indicates that using this feature for malware characterization may not be helpful due to the lack of data representation from each class (class imbalance problem as described in subsection 2.5.2). This limitation in addition to the inherent challenge of overlapping time series (i.e. class inseparability) which creates a complex scenario due to the absence of distinct graph based changes between malignant and benign data samples.
6) It is clearly evident in Figure 50, Figure 51, and Figure 52 that a distinct boundary does not exist between malicious and normal time series for the considered node/edge count related feature. It implies that there is a need to employ a characterization mechanism which can distinguish these samples based on the complexity analysis of their time series such as fractals rather than using a single scale thresholding technique which needs continuous update through human intervention.
7) It is observed that the initial 5 timestamp resolutions in each of the Figure 50, Figure 51, and Figure 52 shows similar behavior due to the adaptive and sliding window nature of time window selection as mentioned in the previous subsection.
8) Table 6: Zeus Malware – Instance 1 – TSNC feature - Ratio of Malware vs. Benign Nodes (Labelled for only true malware nodes 151 and 152).

Timestamp Resolution (μs)	**Total No. of Time Windows**	**No. of Windows having Malware Nodes**	**No. of Windows having Benign Nodes**	**Malware Ratio (%)**
10^0	146	3	143	2.10
10^1	146	3	143	2.10
10^2	146	3	143	2.10
10^3	143	3	140	2.14
10^4	142	3	139	2.16
10^5	113	2	111	1.80
10^6	89	2	87	2.30
10^7	57	1	56	1.79
10^8	26	1	25	4.00
10^9	6	1	5	20.00

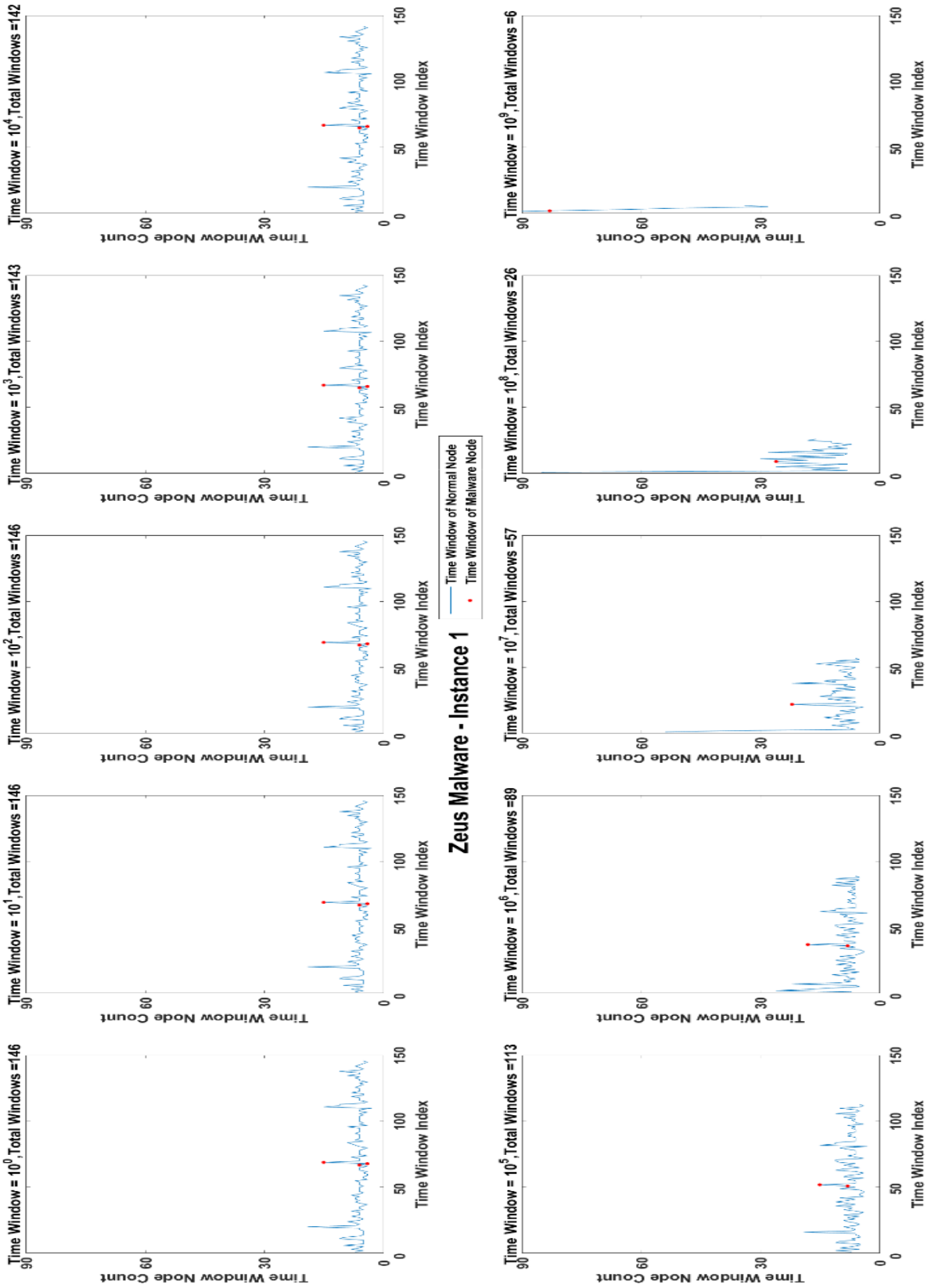


Figure 50: Zeus Malware – Instance 1 – TSNC feature (Labelled for only true malware nodes 151 and 152).

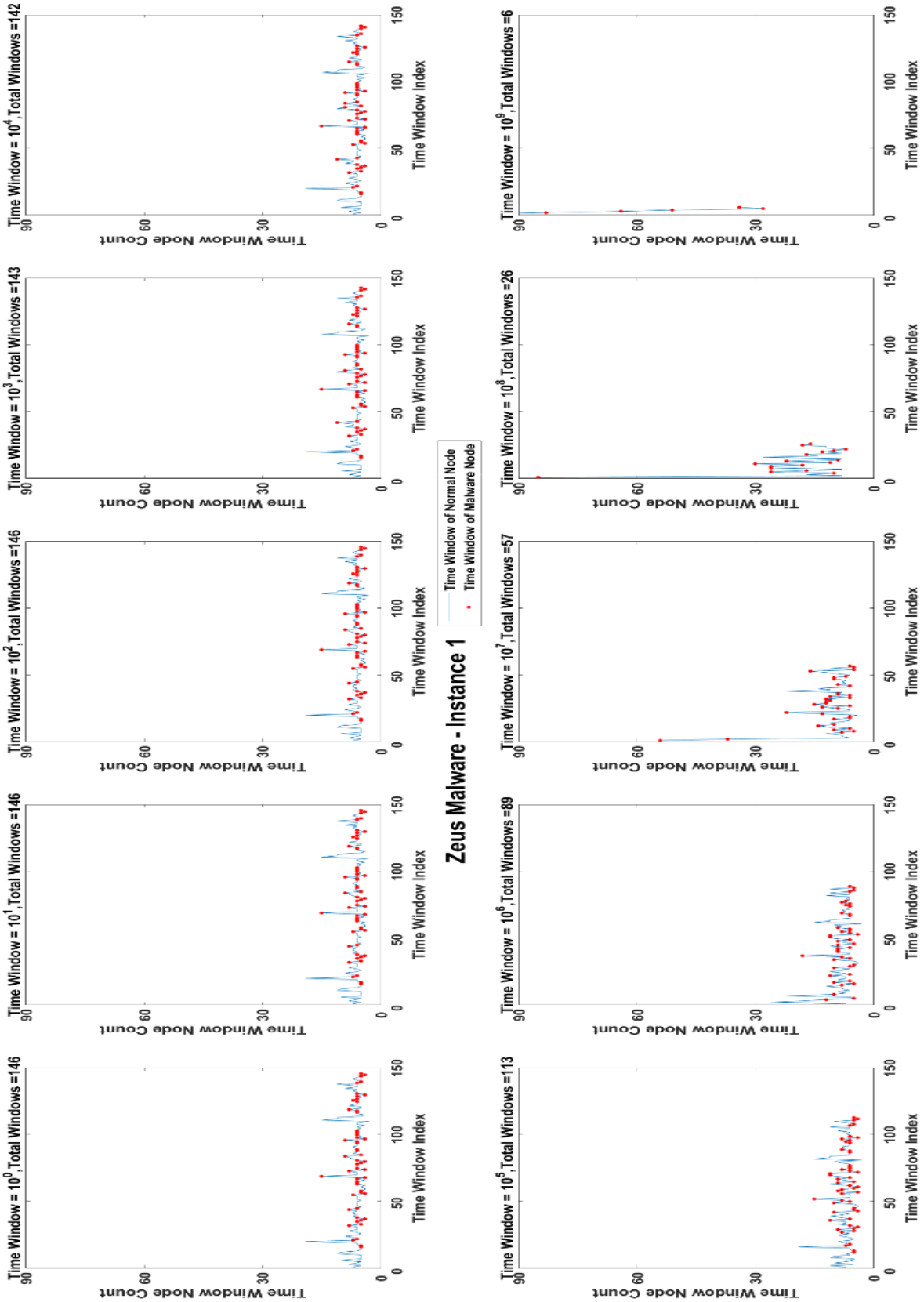


Figure 51: Zeus Malware – Instance 1 – TSNC feature (Labelled for all malware nodes 50, 151 and 152).

Table 7: Zeus Malware – Instance 1 – TSNC feature - Ratio of Malware vs. Benign Nodes (Labelled for all malware nodes 50, 151 and 152).

Timestamp Resolution (μs)	**Total No. of Time Windows**	**No. of Windows having Malware Nodes**	**No. of Windows having Benign Nodes**	**Malware Ratio (%)**
10^0	146	56	90	62.22
10^1	146	56	90	62.22
10^2	146	56	90	62.22
10^3	143	56	87	64.37
10^4	142	56	86	65.12
10^5	113	53	60	88.33
10^6	89	44	45	97.78
10^7	57	34	23	100.00
10^8	26	17	9	100.00
10^9	6	6	0	100.00

Table 8: Zeus Malware – Instance 1 – TSNC feature - Ratio of Malware vs. Benign edges (Labelled for all malware edges 134, 255, 256, and 257).

Timestamp Resolution (μs)	**Total No. of Time Windows**	**No. of Windows having Malware Edges**	**No. of Windows having Benign Edges**	**Malware Ratio (%)**
10^0	146	3	143	2.10
10^1	146	3	143	2.10
10^2	146	3	143	2.10
10^3	143	3	140	2.14
10^4	142	3	139	2.16
10^5	113	2	111	1.80
10^6	89	2	87	2.30
10^7	57	1	56	1.79
10^8	26	1	25	4.00
10^9	6	1	5	20.00

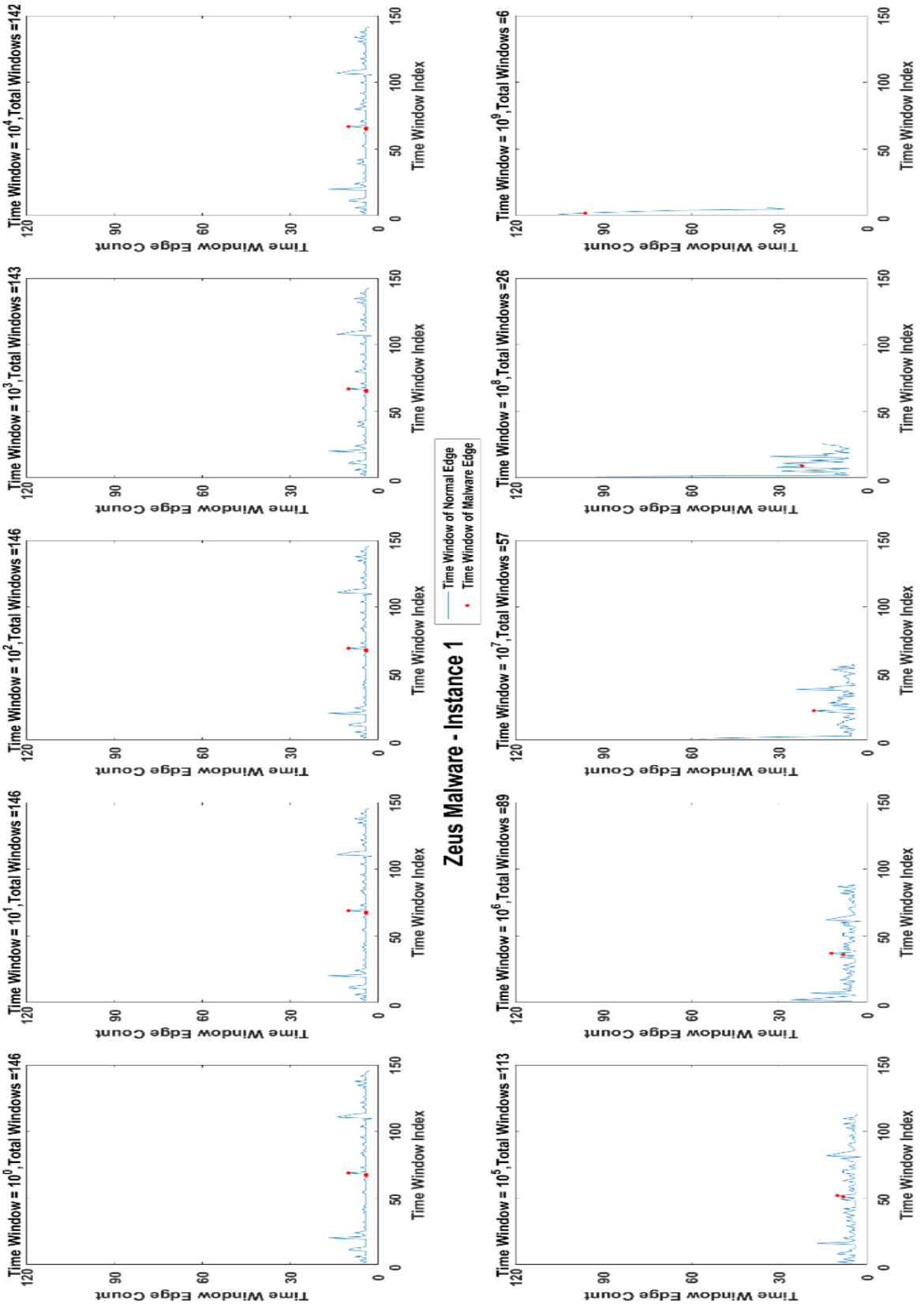


Figure 52: Zeus Malware – Instance 1 – TSNE feature (Labelled for all malware edges 134, 255, 256, and 257).

4.2.5.4 Statistical Analysis of Graph Features

Statistical analysis of the feature set is of utmost importance to verify the mathematical validity of the discussed approach. This is achieved by re-considering the example of Zeus Malware – Instance 1 as mentioned in the subsection 4.2.2.1. The following five aspects of the statistical analysis are evaluated for this research work and are discussed below.

1) Data sufficiency.
2) Fitting Probability Distribution Function (PDF).
3) Test of stationarity.
4) Validation of sampling time (Nyquist criteria).
5) Noise considerations.

1) Data sufficiency

As mentioned in Table 2, the data set of Zeus Malware – Instance 1 is collected for 85 minutes which produced 230,381 unique rows, that were processed further to develop time graph model. There are total 271 unique nodes and 394 unique edges connecting these nodes in the whole instance. Further, the total number of time windows for each timestamp resolution are given in Table 6 to Table 8. Maximum number of adaptive and sliding time windows are 146 for the minimum timestamp lag resolution which is 10^0, while minimum number of time windows are 6 for the maximum timestamp lag resolution of 10^9.

As the literature survey reveals, the sufficiency of the statistical analysis is dependent on the relationship of time with statistical accuracy, hypothesis inferences, precision and power of the data [418]. Further, noise and artefacts also play an important role in determining the data sufficiency. It is considered that with large sample sizes, more generalization is achieved. However, for large data sets, artefacts can be grater in number which may lead to inferential errors, e.g., large biases [419] . Further, with small number of sample size, it is hard to get adequate generalization and may as well lead to inferential errors [420]. Therefore, the question which must be addressed here deals with the determination of suitable sample size required for reliable analysis.

Based on the time, row count and number of windows statistics of Zeus Malware – Instance 1 data, it can be roughly stated that in order to get 1000 samples in the minimum timestamp resolution, an average factor of 8x is required, i.e., 2.5 million rows which is approximately 700 minutes of acquisition time to collect unique rows in the current usage pattern of the host. However, due to the availability of limited resources in terms of storage and processing speed for this research work, it was not possible to extend the acquisition time further which has an exponential order of growth with respect to computing resources. Also, the data set acquisition time window to capture malware dynamics followed the principles and limitations as stated in the threat model.

2) Fitting Probability Distribution Function

In order to analyze any statistical characteristic of the feature set, it is important to hypothesize that the empirical data has certain statistical distribution, which can later enable the application of statistical distribution parameters for analysis. As the data set is empirical, therefore, a non-parametric approach is appropriate, because there is no a-priori knowledge of any specific probability distribution model. The first step is to determine if the empirical data set shows large number of outliers or not. Large number of outliers indicates the presence of heavy or fat tailed distributions, i.e., Pareto and Beta, and thus sample variance cannot be estimated reliably because of not being finite for such distributions.

In this work, the kernel regression technique is utilized to estimate the type of probability distribution for the empirical data set [421]. The following equation (43) shows a mathematical model of the kernel estimation technique.

$$p(x) = \frac{1}{N} \sum_{i=1}^{N} K_B(x - x_i) \tag{43}$$

where K_B is the kernel function with bandwidth B. Kernel function can be chosen from any probability distribution, B is the smoothing/scaling window function and N is the total number of data samples in the empirical data set. Following the axioms of probability, kernel function should satisfy the following:

$$K_B \geq 0 \text{ and } \int K_B = 1 \tag{44}$$

Also, the scaling function should be chosen such that:

$$K_B = \frac{1}{B} K_B(\frac{x}{B}) \tag{45}$$

Analysis of equation (43) reveals the fact that it is an average of the sum of kernel functions Further, as proven in [422] [423], Kernel estimation methods asymptotically converge to the density as $N \rightarrow \infty$. In addition, histogram analysis, is also considered as a special case of Kernel density estimation as mentioned in [421]. Kernel density estimate is used primarily because it does not assume anything about the distribution of the underlying data and assign kernel functions to weight the data points. Contrary to distribution fitting mechanisms, kernel estimation technique is not a fit of a certain distribution as it does not assume anything about the data sample. In this work, Normal distribution is used as Kernel function due to its regularity, continuity, differentiability and local properties.

Another measure of finding the presence of a heavy tailed distribution is the calculation of the 4^{th} order moment of the PDF which is called Kurtosis and is defined in detail in subsection 2.8.5.

In the literature [424] [425] [426], it is proven that if Kurtosis value is greater than 3, then the distribution will have narrower peaks and heavy tails. This is due to the existence of many outliers outside the moderate range from the mean value. Kurtosis value less than 3 represents small number of outliers outside the moderate range from the mean. Higher value of Kurtosis represents more outliers and fatter tails. Following are the kurtosis values for some well-defined distributions:

1) Laplace Distribution = 6.
2) Logistic Distribution = 4.2.
3) Normal Distribution = 3.
4) Uniform Distribution = 1.8.
5) Double Exponential Distribution = 5.9.
6) Cauchy Distribution = 6693.

As shown in Figure 53, an estimated plot of PDF for each of the time window for the node count feature termed as *number of nodes per timestamp* (*TSNC*) is available. Moreover Table 9 provides results of four statistical hypothesis tests (discussed in detail in subsection 2.8) based on empirical data to reject or accept the hypothesis that the underlying distribution of empirical data is Normal or Gaussian. If the test rejects the hypothesis that the data has Normal or Gaussian distribution, then it is a TRUE or Logical 1. Also, included in this table is the kurtosis value of each plot that provides an evidence for the presence of a heavy tailed distribution.

Table 9: Zeus Malware - Instance 1 - Statistical tests for TSNC feature.

Timestamp Resolution (μs)	**Kolmogrov Smirnov Test**	**Chi Square Test**	**Lilliefors Test**	**t-Test**	**Kurtosis**	**VFD**	**SFD**	**Fs (Hz)**
10^0	1	1	1	1	15.25	1.622533	0.915455	1000000
10^1	1	1	1	1	15.25	1.622533	0.915455	100000
10^2	1	1	1	1	15.25	1.622533	0.915455	10000
10^3	1	1	1	1	13.08	1.720793	0.749779	1000
10^4	1	1	1	1	12.63	1.824804	0.749779	100
10^5	1	1	1	1	6.63	NaN	0.614606	NaN
10^6	1	1	1	1	10.35	NaN	0.614606	NaN
10^7	1	1	1	1	19.44	NaN	1.036031	NaN
10^8	1	0	1	1	15.19	NaN	1.763034	NaN
10^9	1	0	0	1	1.69	NaN	1.527243	NaN

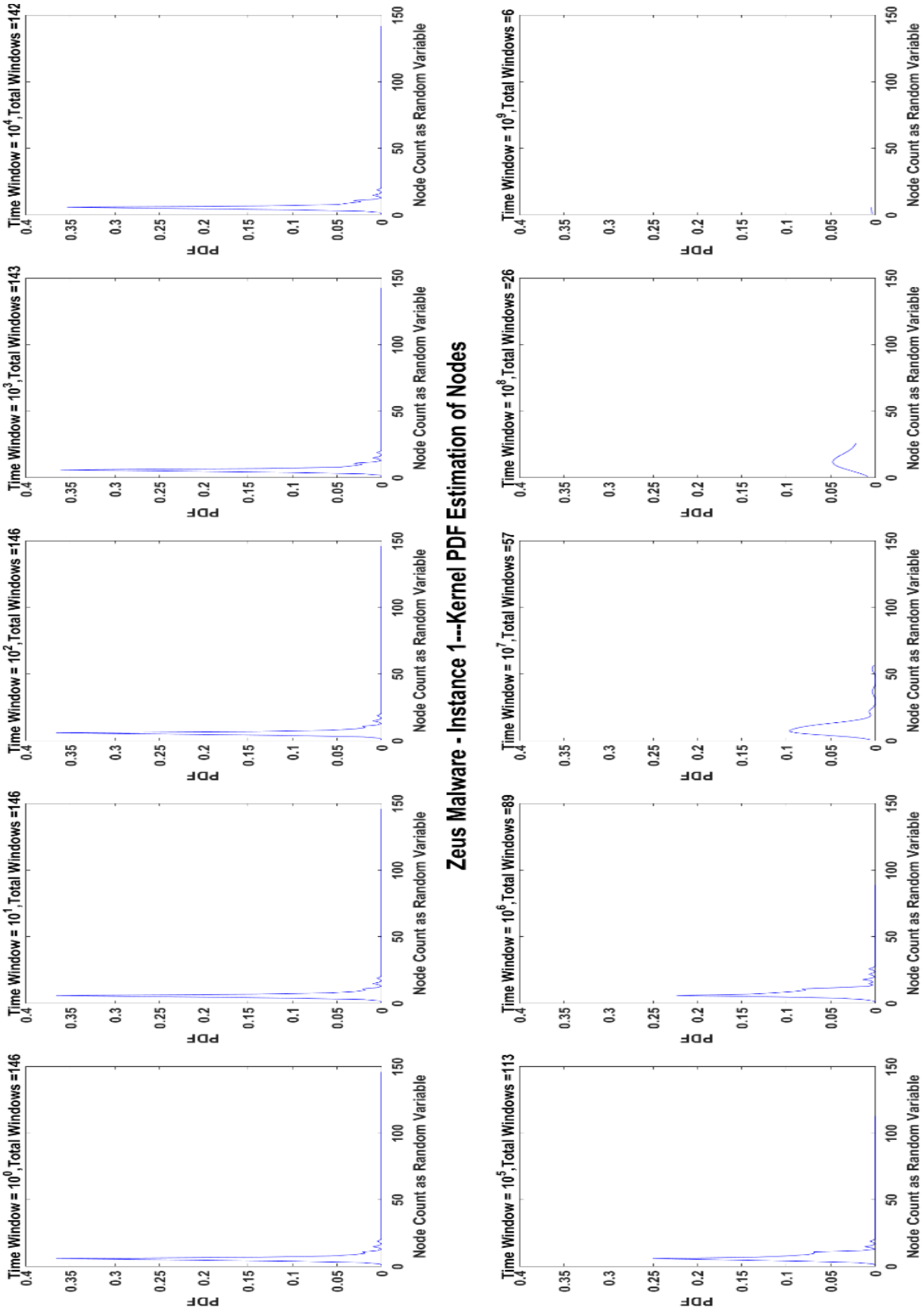


Figure 53: Zeus Malware – Instance 1 --- TSNC feature --- Kernel PDF estimate plots.

As evident from Table 9, data from all timestamp resolutions except the last 2 resolutions indicate the absence of Gaussian distribution as PDF. Further, kurtosis value corresponding to each time window is greater than 10 except the 6^{th} and 10^{th} resolution. This provides sufficient empirical evidence that lag timestamp resolutions from 10^0 till 10^4 depict the presence of heavy tailed distribution. However, despite knowing that it is a heavy tailed distribution, the exact probability distribution like Pareto and Beta is still unknown. It is important to note that after the 5^{th} timestamp resolution, data samples start to reduce in number and the data distribution shows irregularity in the shape which can be attributed towards the insufficiency of data samples. Further, with increasing timestamp resolution, time graphs also become cluttered and complex paving the way for malware to easily conceal itself. Therefore, timestamps 10^0 till 10^4 are selected as stationary valid with high degree of confidence for the time series analysis which represents underlying heavy tailed distribution having many outliers.

Similar results can be deduced for time series of edge feature termed as *number of edges per timestamp (TSNE)* as shown in Figure 54 and Table 10. Graph edges based time series shows signs of underlying heavy tailed distribution. Likewise, TSNC feature behavior, first five timestamp resolutions provide sufficient information about the data behavior statistically.

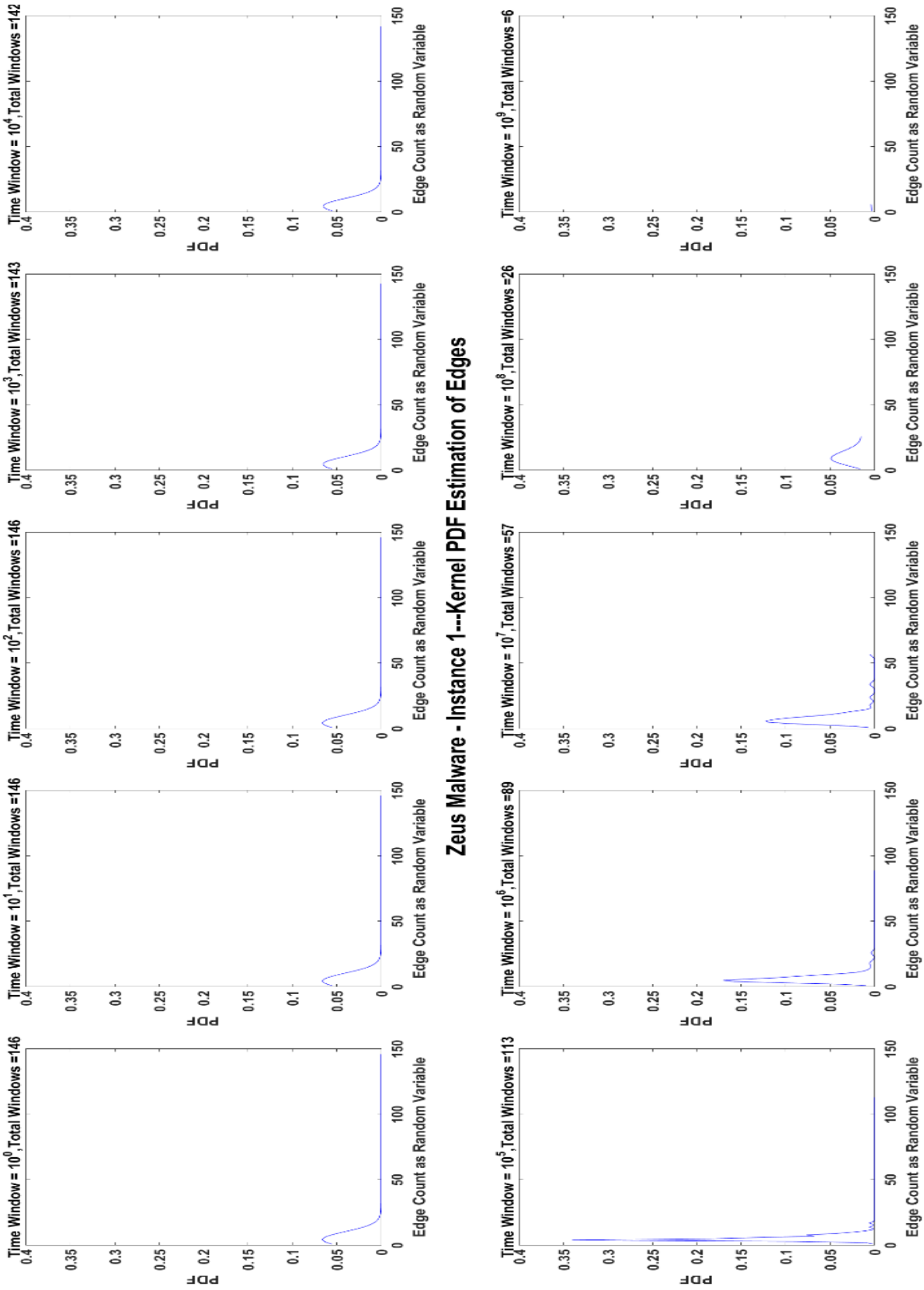


Figure 54: Zeus Malware – Instance 1 - TSNE feature - Kernel PDF estimate plots of node time series.

Table 10: Statistical Tests for TSNE Feature – Zeus Malware – Instance 1.

Timestamp Resolution (μs)	Kolmogrov Smirnov Test	Chi Square Test	Lilliefors Test	t-Test	Kurtosis	VFD	SFD	Fs (Hz)
10^0	1	1	1	1	21.55	1.56	1.13	1000000
10^1	1	1	1	1	21.55	1.56	1.13	100000
10^2	1	1	1	1	21.55	1.56	1.13	10000
10^3	1	1	1	1	19.15	1.64	1.13	1000
10^4	1	1	1	1	18.85	1.70	1.13	100
10^5	1	1	1	1	9.08	NaN	0.82	NaN
10^6	1	1	1	1	14.26	NaN	0.82	NaN
10^7	1	1	1	1	22.91	NaN	0.86	NaN
10^8	1	0	1	1	14.09	NaN	1.59	NaN
10^9	1	0	0	1	1.49	NaN	1.13	NaN

3) Test of stationarity

Heavy tailed distributions, in contrast to regular light tailed distributions, defy the concepts of weak sense stationarity, which is based on first and second order moments of the probability distribution. Theoretically, variance of heavy tailed distribution is infinite and thus it is not possible to find weak sense stationarity globally. However, due to the power law relationship of heavy tailed distributions, local stationarity can be found using fractals [427] [12] [13] [7]. As described in subsection 2.6.3.4, the key point in calculating Variance Fractal Dimension (VFD) is validating the embedding dimension which is between 1 and 2 for single dimensional (single variable) data set. Further, it should ensure that the power law relationship of the data set should have the fractal exponent within the embedded range. For the data set, the calculated VFD for each window size is shown in the seventh column of Table 9 which is embedded between 1 and 2 (for a single feature) and therefore, depicts a sense of stationarity in the local scope/scale. It is further evident from VFD that the empirically sufficient data set is from time stamp resolution 10^0 till 10^4 which is stationary in the second order statistical sense locally. Similar results of edge based time series can be deduced from Table 10.

4) Validating the sampling time (Nyquist criteria)

As the data set is digital and captured over a computer, therefore, it is necessary to validate the sampling interval which should follow Nyquist sampling criterion in statistical sense. This is required not only to provide mathematical validity to the analysis, but also infer the dynamics of the domain [4] [13]. Nyquist sampling criterion conforms to statistical information theoretic concept by capturing the necessary required information in the sampling interval and thus provide a way to reconstruct the signal from this captured information reliably. Therefore, the time graphs, which can be treated as signals on an adaptive and sliding time window based time series function, should capture the information within the time windows to construct them back theoretically.

As mentioned in [428] [7], sampling time is estimated using a valid spectral fractal dimension (SFD) of the power spectrum density (PSD) of each time series. Last two columns of Table 9 show Spectral Dimension (SD) and Estimated Sampling Frequency (Fs) for each timestamp resolution. The Spectral Dimension (as mentioned in subsection 2.6.3.4) of Zeus Malware – Instance 1 dataset indicates that it is close to fractional pink noise which has more attenuation of higher frequency components compare to white noise (for which spectral dimension is 0). Further, this SD value shows that the long term correlation is higher than white noise but lesser than standard Brownian motion process [7]. In addition, the estimated Fs for the first five timestamps shows valid Fs (which is the inverse of timestamp resolution) and conforms to the estimated stationarity from VFD column of Table 9. Also, in Table 9, the value of SD for TSNC feature is closer to 1 in the first three timestamps, therefore, these three timestamps are valid because having SD value greater than 2 for a single dimension feature is not correct. Therefore, these three timestamps are shortlisted for further processing. Similar results of TSNE feature can be deduced from Table 10.

A log-log estimated PSD plot of TSNC and TSNE features are shown in Figure 55 and Figure 56. It is observed that PSD of heavy tailed distributed temporal signal renders a shape of "Spanish Moss" which conforms to the findings in [429] and [7]. Also it is noted that lower frequencies are not dense and show little variability while higher frequencies are very dense and show high variability. Overall, this variation is due to the transformation of the plot in log-log scale format. The effects on higher frequencies are due to the presence of Levy Walk as observed in [429].

5) Noise considerations

Collected raw attributes for each malware instance contained an average of 5%-7% redundant data that does not contribute in the graphical analysis and instead hides the features and patterns within the complex data. Therefore, this is considered as first type of noise in this work and has been removed already. Extracting unique rows from the total rows of each malware instance serves the purpose. There is another noise which is attributed due to signal processing in the hardware of the system. This noise factor cannot be compensated due to the limitations of the computing architecture used in the experiments. For example, the virtual machine (VM) based computing architecture used in this work is based on 32 bit operating system with 2.3 GHz processor clock. Having more than 32 bits processor registers and faster clock can achieve more accuracy in terms of capturing the malware characteristic. Nevertheless, the noise entered due to digital quantization and sampling of data within the computer is considered out of the scope of this work. Lastly, there are observed numerical computation errors due to the accuracy of the programming platform and therefore, the decimal accuracy is found to be limited within two decimal numbers.

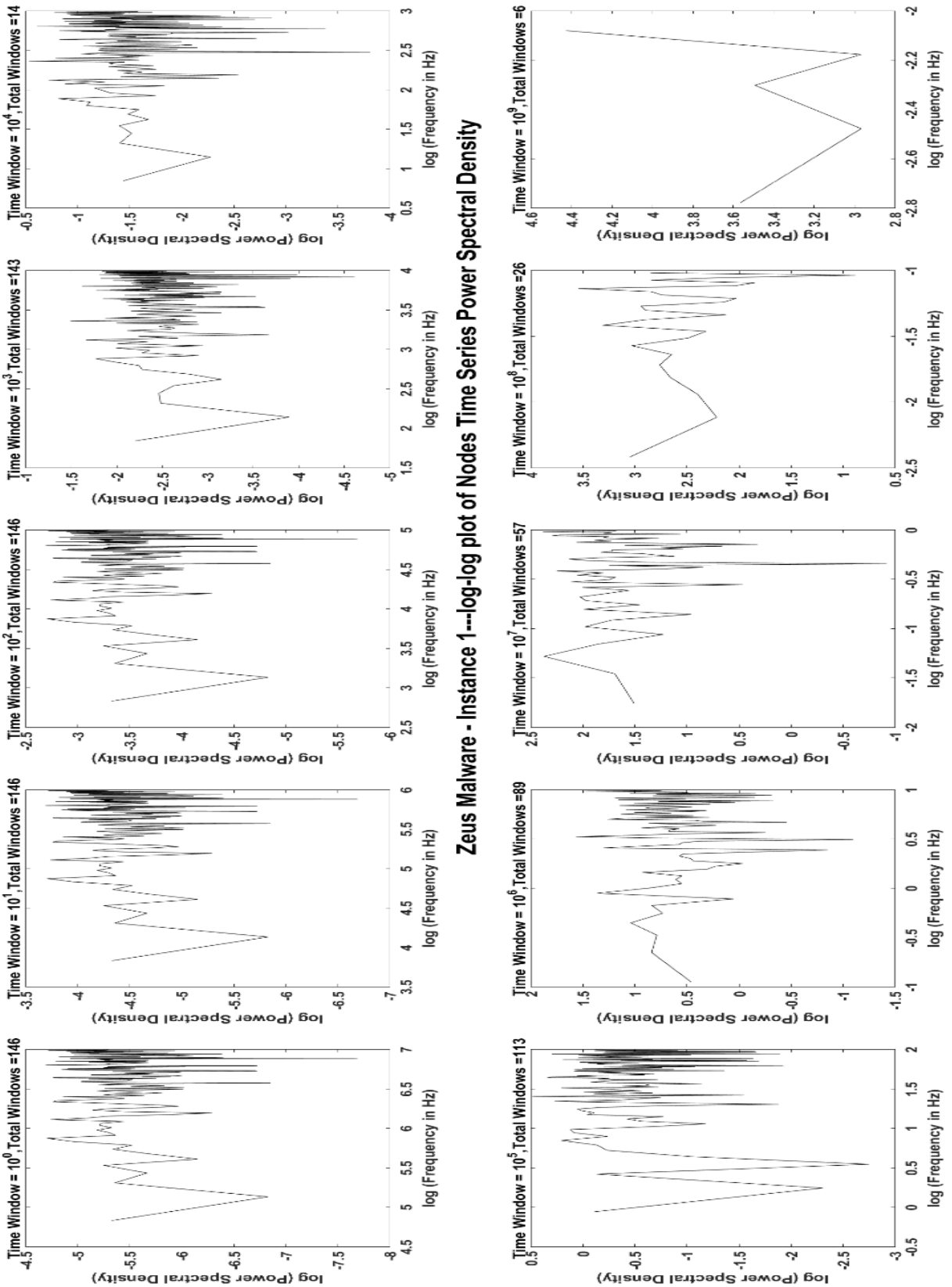


Figure 55: Zeus Malware - Instance 1 - Log-Log plot of PSD - TSNC feature.

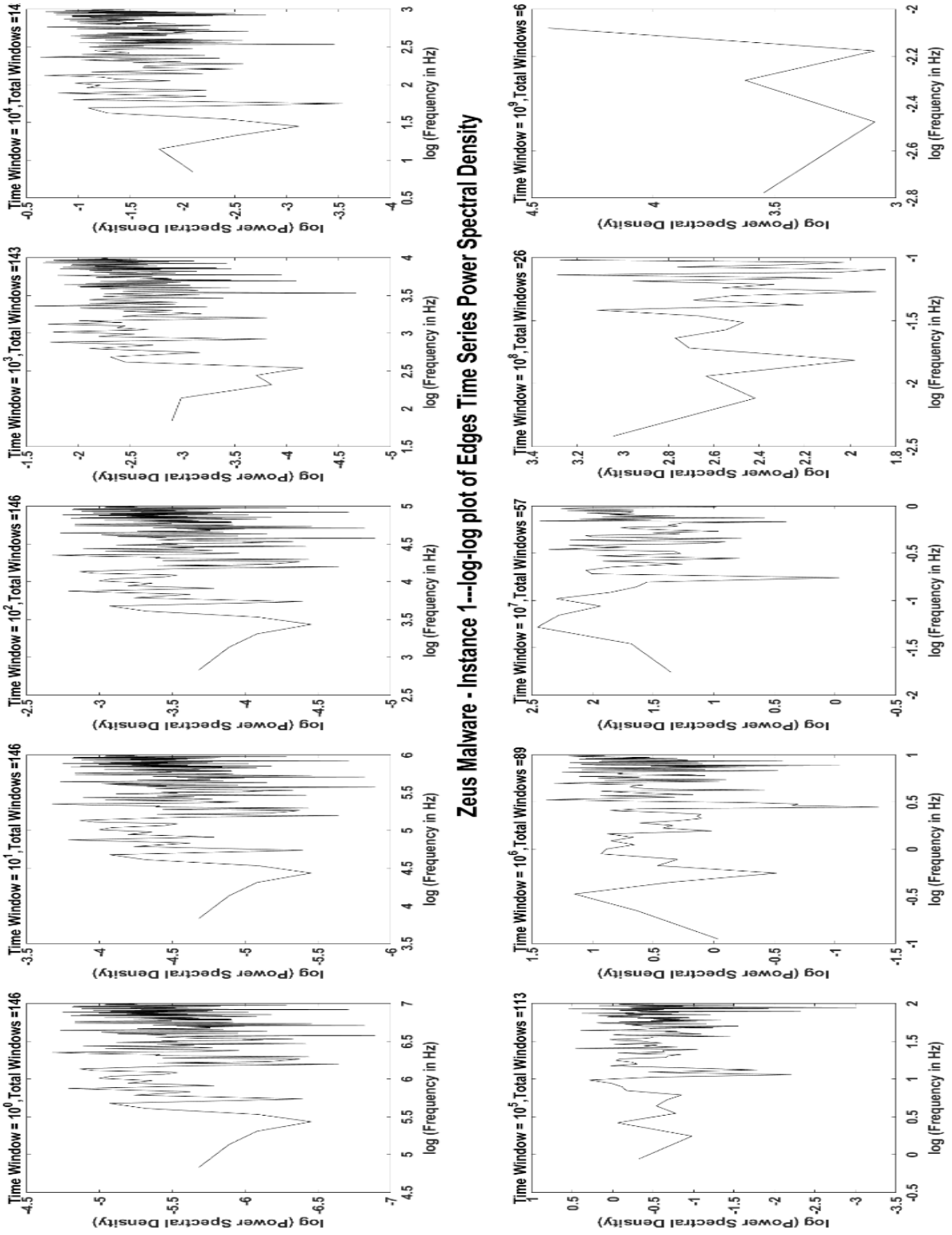


Figure 56: Zeus Malware - Instance 1 - Log-Log plot of PSD - TSNE Feature.

4.3 Fractal Characterization and Validation by K-means Clustering Algorithm

As already discussed, the overlapping nature of the malware and normal samples over space and time graph, sets forth the requirement of a technique that can characterize the malicious behavior by considering the subtle dynamic changes in the complexity measure of these graph based features. It is important because any machine learning system which aims to reduce the cognitive load of a cyber-security expert by autonomously determining the anomalous changes in the system as true or false requires distinct linear or non-linear class separation boundaries. However, as suggested in the literature [14] [9] and already mentioned in subsection 2.5.1, single scale (monoscale) similarity measure based characterization of malware dynamics is neither adequate nor reliable and therefore, necessitates the utilization of multiscale measures like fractals for this purpose. In this dissertation, three complexity measures i.e. Variance Fractal Dimension (VFD), Correlation Fractal Dimension (CFD) and Information Fractal Dimension (IFD) have been evaluated for malware characterization. As the names of each of these fractal dimensions suggest, these are aimed at extracting the multiscale nature of each relevant mutltiscale statistic, i.e. variance, correlation and Shannon entropy which is then compared with the single scale Euclidean based time series analysis where similarity is measured based on the squared Euclidean distance. The results show that the proposed approach can be used to determine the suitable set of features that can characterize the regular and irregular activities in the process time graph consistently.

4.3.1 fBm time series with Fractal Dimension Trajectories

In order to test the validity of K-means unsupervised clustering algorithm using fractal dimension based similarity measures on a time series having normal and malicious samples, a fractional Brownian motion (fBm) statistical process trajectory (time series) is generated with two distinct Hurst parameters and each fractal dimension based trajectory (time series) is used to benchmark the evaluation performance of the clustering algorithm. fBm with different Hurst parameters simulates different cognitive complexities and is already described in subsection 2.6.3.4. Therefore, using fBm as a validation mechanism is akin to measuring the malware complexity showing different multiscale behaviors. This time series is generated using a matrix where the rows represent timestamps (e.g. 250) and columns represents fBm values for that timestamp (e.g. 1024). This provides a simulation of the selected features (e.g. CNTS and ECTS) where each time stamp has various nodes represented by the columns of the matrix. This fBm time series is divided into two groups of 100 and 150 samples each such that both of them have different Hurst parameter values. Then for each sample group, the proposed three different types of fractal dimensions are estimated and plotted. Further details can be found in the algorithm section 3.4.7.

Figure 57: Fractal dimension estimation for fBm having Hurst values of 0.1 and 0.9.

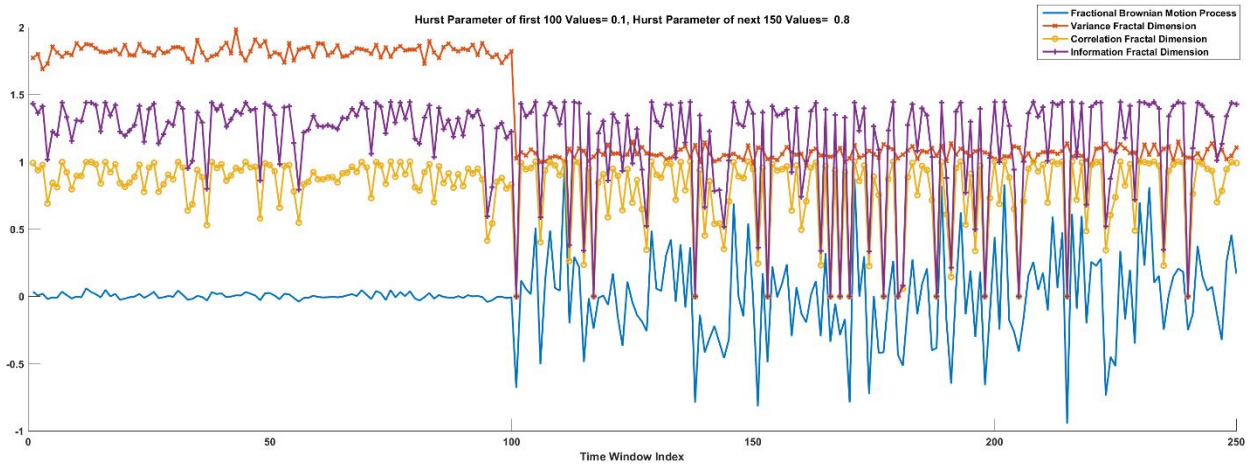


Figure 58: Fractal dimension estimation for fBm having Hurst values of 0.1 and 0.8.

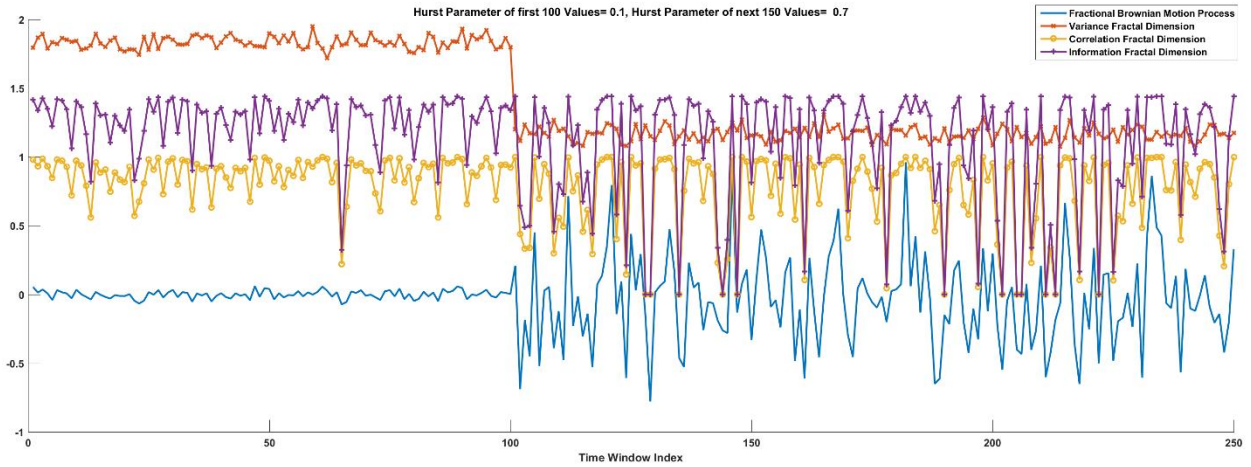


Figure 59: Fractal dimension estimation for fBm having Hurst values of 0.1 and 0.7.

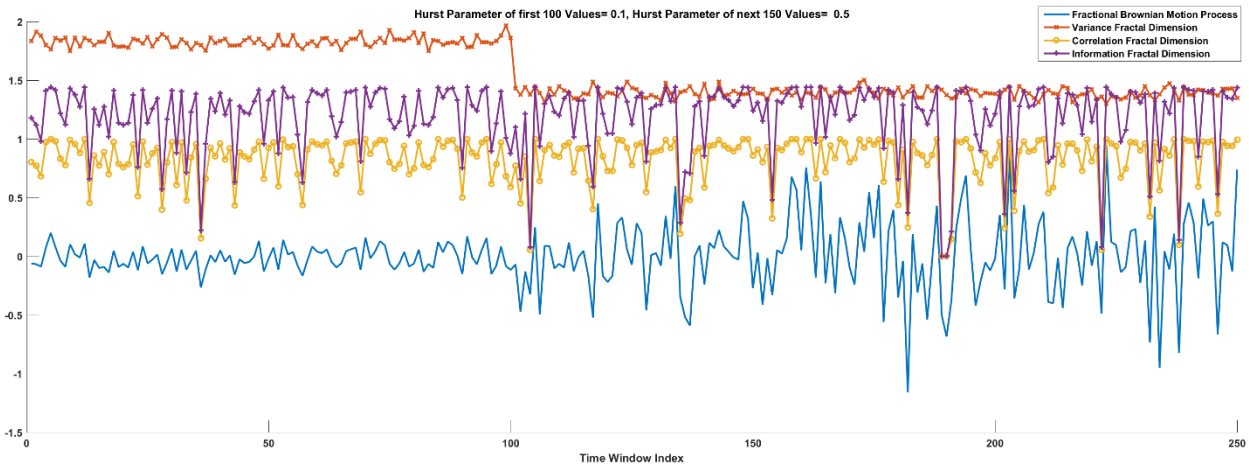


Figure 60: Fractal dimension estimation for fBm having Hurst values of 0.1 and 0.5.

Figure 61: Fractal dimension estimation for fBm having Hurst values of 0.1 and 0.3.

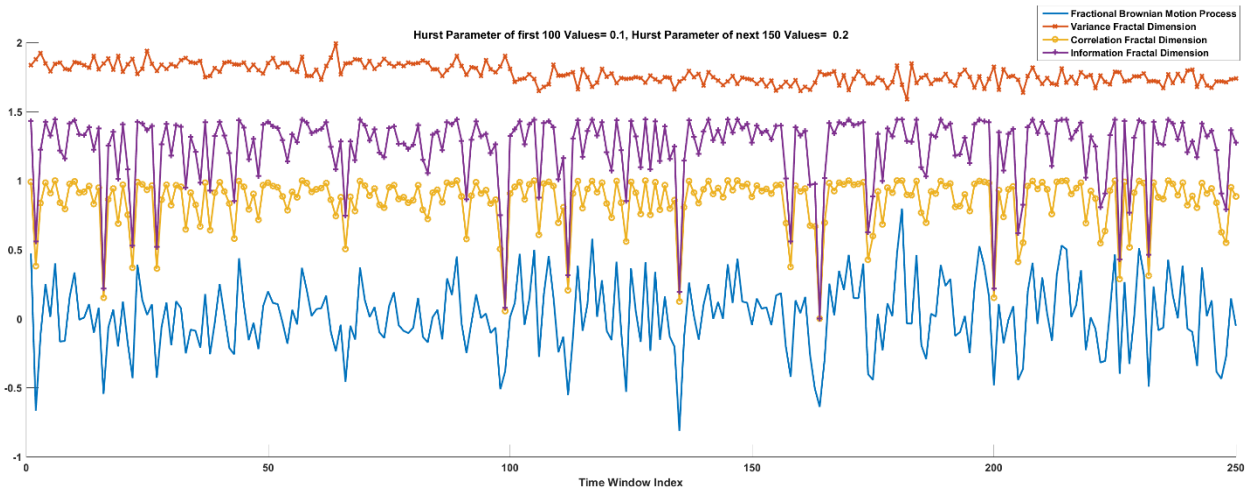


Figure 62: Fractal dimension estimation for fBm having Hurst values of 0.1 and 0.2.

4.3.1.1 Analysis of fBm with Fractal Dimension Trajectories

As shown in Figure 57 to Figure 62, an fBm trajectory is plotted, shown in blue color, with its variance fractal dimension trajectory (VFDT) shown in red color, correlation fractal dimension trajectory (CFDT) shown in yellow color and information fractal dimension trajectory (IFDT) shown in purple color. Following are the important observations from these plots:

1) fBm can take negative values (exists only for all $t \geq 0$).
2) fBm values are normalized in the range [-1, 1].
3) VFDT will be bounded between the values of 1 and 2 due to being a single Euclidean dimension (embedded between 1 and 2) [4].
4) CFDT is bounded in the interval [0, ∞) [4].
5) IFDT is bounded in the interval [0, ∞) [4].
6) VFDT distinctively switches magnitude between two Hurst parametric trajectories of fBm, if Hurst difference is higher as shown in Figure 57, Figure 58, and Figure 59.
7) As Hurst difference gets lower, VFD trajectory for both Hurst parameters gets less unique and visibly similar as observed in Figure 60, Figure 61, and Figure 62.
8) VFDT plot for a single Hurst parameter data shows bounded variations of relative magnitude. Regardless of the Hurst parameter value, the trajectory remains tightly bounded in magnitude; however, the overall trajectory magnitude changes with Hurst parameter value e.g. higher Hurst value shows lower mean VFDT and vice versa. It is analogous to electrical Alternating Current (AC) signals with DC values (mean). Higher Hurst value shows lower Direct Current (DC) value while the AC signal oscillations remain lower regardless of the DC value. Thus, Hurst parameters behaves as an offset value only.
9) Both CFDT and IFDT show relative variations with respect to Hurst parameter. Increasing value of Hurst parameter increases the variations in the CFDT and IFDT trajectories. However, CFDT variations are of low variance compare to IFDT. Also, CFDT variations remain within the bounds of 0 to 1 while IFDT variations remain within 0 to 1.5 range.
10) It is observed that with very low difference in Hurst parameter, discriminatory power of fractal dimension based trajectories diminishes, which could be a challenge in determining attacks having similar complexity with normal data, if fractal dimension based complexity measures are used to distinguish the malware and normal data behavior.

4.3.2 K-means Clustering Performance of Single scale and Multiscale Similarity Measures for fBm Dataset

In this subsection, a fractal based unsupervised characterization of a mathematical time series using fractional Brownian motion process is depicted. The objective of this complexity characterization is to evaluate the performance of fractal algorithms in distinctly characterizing the multiscale behavior of unknown malware samples and compare the performance with traditional single scale based unsupervised clustering algorithm. In other words, this subsection stipulates the idea of measuring the complexity without having any a-priori information and evaluate the characterization performance of fractal based clustering algorithms.

As fBm time series consists of two different Hurst parameters, the number of clusters selected for this validation step are two simulating the case of having a malicious object or not. The samples in each of these clusters signifies their closeness with that Hurst value. It implies that the objective to execute these four different similarity measure based k-mean is to validate their capability to correctly assign the time series data samples to their correct Hurst value cluster.

Table 11: Performance comparison of fBm clustering.

Metric	K-means	fBm (0.1 vs. 0.9)	fBm (0.1 vs. 0.8)	fBm (0.1 vs. 0.7)	fBm (0.1 vs. 0.5)	fBm (0.1 vs. 0.3)	fBm (0.1 vs. 0.2)	Mean values	% improvement from Euclidean
	Euclid.	96.67	74.00	81.33	75.33	76.67	86.00	81.66666667	N/A
	VFD	100.00	100.00	100.00	100.00	98.00	91.33	98.22	20.27210884
	CFD	25.33	20.67	24.67	12.00	8.67	6.00	16.22222222	-80.13605442
	IFD	25.33	20.00	24.00	12.00	8.00	6.00	15.89	-80.54421769
	Euclid.	100.00	100.00	100.00	99.00	100.00	86.00	97.5	N/A
	VFD	100.00	100.00	100.00	100.00	100.00	85.00	97.50	0
	CFD	98.00	99.00	99.00	94.00	95.00	95.00	96.66666667	-0.854700855
	IFD	98.00	99.00	99.00	94.00	95.00	95.00	96.67	-0.854700855
	Euclidean	100.00	100.00	100.00	100.00	87.00	91.00	96.33333333	N/A
	VFD	0.00	0.00	0.00	0.00	0.00	15.00	2.50	97.40484429
	CFD	2.00	1.00	1.00	6.00	5.00	5.00	3.333333333	96.53979239
	IFD	2.00	1.00	1.00	6.00	5.00	5.00	3.33	96.53979239
	Euclid.	71.33	87.33	62.00	76.67	98.67	70.67	77.77777778	N/A
	VFD	0.00	0.00	0.00	0.00	2.00	8.67	1.78	97.71428571
	CFD	74.67	79.33	75.33	88.00	91.33	94.00	83.77777778	-7.714285714
	IFD	74.67	80.00	76.00	88.00	92.00	94.00	84.11	-8.142857143
	Euclid.	58.00	66.00	69.20	57.20	51.60	75.86	62.97701149	N/A
	VFD	100.00	100.00	100.00	100.00	98.80	90.13	98.16	55.85887744
	CFD	54.40	52.00	54.40	44.80	43.20	64.29	52.18095238	-17.14285714
	IFD	54.40	51.60	54.00	44.80	42.80	64.29	51.98	-17.46043334

Acc. (%)	**Euclid.**	73.42	61.50	65.59	62.26	65.34	55.20	63.88413775	N/A
	VFD	100.00	100.00	100.00	100.00	98.99	88.80	97.96	53.3478992
	CFD	40.00	34.07	39.36	20.69	15.48	41.60	31.86558031	-50.11973014
	IFD	40.00	33.15	38.50	20.69	14.37	41.60	31.39	-50.87127928
	Euclid.	100.00	100.00	100.00	97.22	100.00	69.73	94.49199199	N/A
	VFD	100.00	100.00	100.00	100.00	100.00	90.73	98.45	4.193746011
	CFD	95.00	96.88	97.37	75.00	72.22	10.98	74.57354217	-21.07951097
	IFD	95.00	96.77	97.30	75.00	70.59	10.98	74.27	-21.39804187

Table 11 enumerates the performance comparison for fBm based time series (having varying Hurst parameters) using standard Euclidean and fractal dimension based similarity metrics which include VFD, CFD and IFD. Following are the significant observations:

1) VFD measure outperformed all other metrics when used as a similarity measures for unsupervised clustering of data having different inherent complexities which may be distinctly different (0.1 vs. 0.9 Hurst parameter) or closely similar (0.1 vs. 0.2).
2) In true positives, VFD measure shows performance improvement of average 20% compared to Euclidean measure. However, CFD and IFD underperformed badly (showing degradation).
3) In true negatives, VFD measure shows equal performance as that of Euclidean measure. However, CFD and IFD performed slightly lower than Euclidean and can be estimated to be equal in performance to that of Euclidean measure.
4) VFD outperforms Euclidean in terms of FPR measure by attaining diminishingly lower values. However, it is important to note that CFD and IFD as well performed significantly better in reducing FPR. It clearly indicates that fractal dimensions based similarity metrics are evidently better in decreasing false positive alarms which is a nuisance factor for CSOC team.
5) On the other hand, FNR is also greatly reduced by VFD as compared to Euclidean measure which indicates the true discriminating power of VFD for malware characterization. Whereas, CFD and IFD, although not better, are relatively closer in performance to Euclidean. In fact, FNR values are not in an encouraging range for CFD, IFD, and Euclidean based k-means for all fBm trajectories.
6) Precision and Accuracy values have been improved by more than 50% when VFD is employed as a similarity metric compared to standard Euclidean distance in clustering schemes. Nevertheless, clustering performance of CFD and IFD is either close to Euclidean or lower in terms of accuracy and precision metrics
7) The superior performance of VFD based k-means in accurately clustering different samples assigns it a better F1-score compared to the standard Euclidean based k-means. Further, CFD and IFD measures have a reduction of about 20% in their performance with respect to F1-scores signifying their inappropriateness for the clustering of fBm based dataset.
8) As a general observation, with the decreasing difference between Hurst parameters of two fBm time-series, performance of K-means algorithm decreases gradually irrespective of the similarity metric. However, VFD based measure shows maximum resistance in performance degradation and if not lesser, shows at least equal performance to that of Euclidean measure for the lowest margin fBm trajectory (i.e. fBm having Hurst values as 0.1 vs. 0.2). This can be

attributed to the increase in variance of fBm time series which loses discrimination as the difference between two Hurst parameters diminishes.

It can be deduced that CFD and IFD have relatively less discriminating power for k-means based clustering due to high variability, which is attributed to the relative change in variance magnitude with respect to the changing fractal dimension. VFD performed better since it is a low variability dimension with respect to change in fractal dimension. Also, it provides an elegant way of identifying the changes in dimension based on its change in mean fractal dimension magnitude rather change in variance of fractal dimension (does not imply change in variance dimension of the feature data set).

In the next section, a comparative K-means algorithm based clustering performance of Euclidean, VFD, CFD and IFD similarity is evaluated on individual malware infected data set and will be followed by a characterization discussion.

4.4 Feature Characterization and Clustering Performance Results of Malware Data Set

After elaborating and validating the performance of multiscale fractal dimension based similarity metrics for K-means algorithm and its single scale (Euclidean distance) counterpart for a theoretical fractional Brownian motion process (fBm), this section will describe the characterization and clustering performance of data set of individual malware instances. This data set of each malware sample in an operating system process tree is provided in appendix section 1.

Each malware instance data set is characterized by four tables, as follows:

1) A table for malware vs. normal sample ratio showing statistics of each timestamp resolution for nodes and edges is presented.
2) A table of four statistical significance tests i.e. Kolmogorav-Smirnovtest, t-test, Chi test, and Lilliefors test for each timestamp resolution for both nodes and edges data is enumerated (95% confidence). Further, an estimated Kurtosis value, average VFD value, SFD value, and normalized sampling frequency estimate are also included in the respective tables.
3) A table of average VFD, CFD and IFD values for each feature is shown for both nodes and edges of individual malware dataset.
4) A table of the clustering performance of individual selected features i.e. CNTS, TSNN, ECTS, EMTS, ETTS and ETSD is shown.

1) Zeus Malware – Instance 1

Table 12: Zeus Malware – Instance 1 - Malware vs. Normal sample ratio.

	Total	Zeus 01 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	271.00	3.00	10^0	146.00	56.00	90.00	38.36
			10^1	146.00	56.00	90.00	38.36
			10^2	146.00	56.00	90.00	38.36
			10^3	143.00	56.00	87.00	39.16
			10^4	142.00	56.00	86.00	39.44
			10^5	113.00	53.00	60.00	46.90
			10^6	89.00	44.00	45.00	49.44
			10^7	57.00	34.00	23.00	59.65
			10^8	26.00	17.00	9.00	65.38
			10^9	6.00	6.00	0.00	100.00
Edge	394.00	4.00	10^0	146.00	3.00	143.00	2.05
			10^1	146.00	3.00	143.00	2.05
			10^2	146.00	3.00	143.00	2.05
			10^3	143.00	3.00	140.00	2.10
			10^4	142.00	3.00	139.00	2.11
			10^5	113.00	2.00	111.00	1.77
			10^6	89.00	2.00	87.00	2.25
			10^7	57.00	1.00	56.00	1.75
			10^8	26.00	1.00	25.00	3.85
			10^9	6.00	1.00	5.00	16.67

Table 13: Zeus Malware – Instance 1 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Zeus 01 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1.00	1.00	1.00	1.00	15.25	1.17	0.92	1.00
	10^1	1.00	1.00	1.00	1.00	15.25	1.17	0.92	1.00
	10^2	1.00	1.00	1.00	1.00	15.25	1.17	0.92	1.00
	10^3	1.00	1.00	1.00	1.00	13.08	1.17	0.75	1.00
	10^4	1.00	1.00	1.00	1.00	12.63	1.17	0.75	1.00
	10^5	1.00	1.00	1.00	1.00	6.63	1.13	0.61	1.00
	10^6	1.00	1.00	1.00	1.00	10.35	1.22	0.61	1.00
	10^7	1.00	1.00	1.00	1.00	19.44	NaN	1.04	1.00
	10^8	1.00	0.00	1.00	1.00	15.19	NaN	1.76	1.00
	10^9	1.00	0.00	0.00	1.00	1.69	NaN	1.53	1.00
Edge	10^0	1.00	1.00	1.00	1.00	21.55	1.17	1.13	1.00
	10^1	1.00	1.00	1.00	1.00	21.55	1.17	1.13	1.00
	10^2	1.00	1.00	1.00	1.00	21.55	1.17	1.13	1.00
	10^3	1.00	1.00	1.00	1.00	19.15	1.17	1.13	1.00
	10^4	1.00	1.00	1.00	1.00	18.85	1.17	1.13	1.00
	10^5	1.00	1.00	1.00	1.00	9.08	1.13	0.82	1.00
	10^6	1.00	1.00	1.00	1.00	14.26	1.22	0.82	1.00
	10^7	1.00	1.00	1.00	1.00	22.91	NaN	0.86	1.00
	10^8	1.00	0.00	1.00	1.00	14.09	NaN	1.59	1.00
	10^9	1.00	0.00	0.00	1.00	1.49	NaN	1.13	1.00

Table 14: Zeus Malware – Instance 1 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.06	1.05	1.00	1.00	1.00	1.00	1.17	1.00	1.00	1.00	1.00	1.00	1.00
	Normal	1.11	1.11	1.12	1.12	1.11	1.07	1.22	1.14	1.08	1.08	1.08	1.10	1.17
	Delta Normal (%)	**4.65**	**5.16**	**10.91**	**10.91**	**9.86**	**6.73**	**3.91**	**12.23**	**7.66**	**7.66**	**7.70**	**8.98**	**14.89**
CFD	Malware	0.11	0.10	0.01	0.01	0.00	0.00	1.18	0.00	1.00	1.00	1.00	1.00	0.00
	Normal	0.17	0.18	0.20	0.20	0.10	0.11	1.11	1.01	1.05	1.05	1.02	0.96	1.03
	Delta Normal (%)	**36.39**	**43.87**	**97.44**	**97.44**	**97.79**	**98.16**	**-6.30**	**100.00**	**4.84**	**4.84**	**1.91**	**-4.01**	**100.00**
IFD	Malware	0.16	0.15	0.01	0.01	0.00	0.00	1.71	0.00	1.44	1.44	1.44	1.44	0.00
	Normal	0.26	0.27	0.29	0.29	0.14	0.17	1.61	1.46	1.52	1.52	1.48	1.39	1.48
	Delta Normal (%)	**36.95**	**43.99**	**97.51**	**97.51**	**97.83**	**98.17**	**-6.30**	**100.00**	**4.86**	**4.86**	**2.52**	**-4.12**	**100.00**

Table 15: Zeus Malware – Instance 1 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	32.83		27.17		20.00		100.00		0.00		60.00	
	VFD	96.23	**193.10**	94.34	**247.22**	100.00	**400.00**	50.00	**-50.00**	100.00	**100.00**	100.00	**66.67**
	CFD	54.72	**66.67**	47.17	**73.61**	50.00	**150.00**	50.00	**-50.00**	100.00	**100.00**	50.00	**-16.67**
	IFD	26.42	**-19.54**	16.98	**-37.50**	50.00	**150.00**	59.64	**-40.36**	100.00	**100.00**	100.00	**66.67**
TNR (%)	**Euclid.**	69.00		69.67		79.46		16.22		98.02		40.36	
	VFD	30.00	**-56.52**	26.67	**-61.72**	16.22	**-79.59**	19.82	**22.22**	9.91	**-89.89**	17.12	**-57.59**
	CFD	41.67	**-39.61**	66.67	**-4.31**	19.82	**-75.06**	27.93	**72.22**	11.71	**-88.05**	21.62	**-46.43**
	IFD	80.00	**15.94**	93.33	**33.97**	27.93	**-64.85**	40.36	**148.89**	11.71	**-88.05**	10.81	**-73.21**
FPR (%)	**Euclid.**	31.00		30.33		20.54		83.78		1.98		59.64	
	VFD	70.00	**-125.81**	73.33	**-141.76**	83.78	**-307.89**	80.18	**4.30**	90.09	**-4445.45**	82.88	**-38.97**
	CFD	58.33	**-88.17**	33.33	**-9.89**	80.18	**-290.35**	72.07	**13.98**	88.29	**-4354.55**	78.38	**-31.42**
	IFD	20.00	**35.48**	6.67	**78.02**	72.07	**-250.88**	60.00	**28.39**	88.29	**-4354.55**	89.19	**-49.55**
FNR (%)	**Euclid.**	67.17		72.83		80.00		0.00		100.00		40.00	
	VFD	3.77	**94.38**	5.66	**92.23**	0.00	**100.00**	50.00	**-5000.00**	0.00	**100.00**	0.00	**100.00**
	CFD	45.28	**32.58**	52.83	**27.46**	50.00	**37.50**	50.00	**-5000.00**	0.00	**100.00**	50.00	**-25.00**
	IFD	73.58	**-9.55**	83.02	**-13.99**	50.00	**37.50**	0.72	**-72.00**	0.00	**100.00**	0.00	**100.00**
Prec. (%)	**Euclid.**	44.13		36.46		0.36		2.11		0.00		1.07	
	VFD	54.84	**24.26**	53.19	**45.88**	2.11	**489.47**	1.11	**-47.22**	1.96	**1960.00**	2.13	**97.99**
	CFD	45.31	**2.68**	55.56	**52.37**	1.11	**211.11**	1.23	**-41.36**	2.00	**2000.00**	1.14	**5.74**
	IFD	53.85	**22.01**	69.23	**89.87**	1.23	**245.68**	59.29	**2716.37**	2.00	**2000.00**	1.98	**84.27**
Acc. (%)	**Euclid.**	52.04		49.73		78.41		17.70		96.28		40.71	
	VFD	61.06	**17.35**	58.41	**17.44**	17.70	**-77.43**	20.35	**15.00**	11.50	**-88.05**	18.58	**-54.35**
	CFD	47.79	**-8.16**	57.52	**15.66**	20.35	**-74.04**	28.32	**60.00**	13.27	**-86.21**	22.12	**-45.65**
	IFD	54.87	**5.44**	57.52	**15.66**	28.32	**-63.88**	1.41	**-92.04**	13.27	**-86.21**	12.39	**-69.57**
F1 (%)	**Euclid.**	33.63		23.39		0.70		4.12		0.00		2.11	
	VFD	69.86	**107.77**	68.03	**190.90**	4.12	**487.63**	2.17	**-47.28**	3.85	**385.00**	4.17	**97.33**
	CFD	49.57	**47.43**	51.02	**118.17**	2.17	**209.78**	2.41	**-41.57**	3.92	**392.00**	2.22	**5.25**
	IFD	35.44	**5.41**	27.27	**16.62**	2.41	**243.37**	1.41	**-65.81**	3.92	**392.00**	3.88	**83.92**

2) Zeus Malware – Instance 2

Table 16: Zeus Malware – Instance 2 – Malware vs. Normal sample ratio.

	Total	Zeus 02 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	247	3	10^0	144.0	57.0	87.0	39.6
			10^1	144.0	57.0	87.0	39.6
			10^2	144.0	57.0	87.0	39.6
			10^3	144.0	57.0	87.0	39.6
			10^4	138.0	57.0	81.0	41.3
			10^5	108.0	52.0	56.0	48.1
			10^6	85.0	44.0	41.0	51.8
			10^7	56.0	36.0	20.0	64.3
			10^8	29.0	25.0	4.0	86.2
			10^9	7.0	7.0	0.0	100.0
Edge	358	4	10^0	144.0	3.0	141.0	2.1
			10^1	144.0	3.0	141.0	2.1
			10^2	144.0	3.0	141.0	2.1
			10^3	144.0	3.0	141.0	2.1
			10^4	138.0	3.0	135.0	2.2
			10^5	108.0	2.0	106.0	1.9
			10^6	85.0	2.0	83.0	2.4
			10^7	56.0	1.0	55.0	1.8
			10^8	29.0	1.0	28.0	3.4
			10^9	7.0	1.0	6.0	14.3

Table 17: Zeus Malware – Instance 2 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Zeus 02 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1.0	1.0	1.0	1.0	8.9	1.2	0.5	1.0
	10^1	1.0	1.0	1.0	1.0	8.9	1.2	0.5	1.0
	10^2	1.0	1.0	1.0	1.0	8.9	1.2	0.5	1.0
	10^3	1.0	1.0	1.0	1.0	8.9	1.2	0.5	1.0
	10^4	1.0	1.0	1.0	1.0	7.0	1.2	0.5	1.0
	10^5	1.0	1.0	1.0	1.0	6.9	1.1	0.8	1.0
	10^6	1.0	1.0	1.0	1.0	14.5	1.2	0.6	1.0
	10^7	1.0	1.0	1.0	1.0	8.6	NaN	0.9	1.0
	10^8	1.0	0.0	1.0	1.0	14.8	NaN	1.6	1.0
	10^9	1.0	0.0	0.0	1.0	1.8	NaN	2.1	1.0
Edge	10^0	1.0	1.0	1.0	1.0	16.9	1.2	1.2	1.0
	10^1	1.0	1.0	1.0	1.0	16.9	1.2	1.2	1.0
	10^2	1.0	1.0	1.0	1.0	16.9	1.2	1.2	1.0
	10^3	1.0	1.0	1.0	1.0	16.9	1.2	1.2	1.0
	10^4	1.0	1.0	1.0	1.0	13.5	1.2	1.2	1.0
	10^5	1.0	1.0	1.0	1.0	8.5	1.1	0.9	1.0
	10^6	1.0	1.0	1.0	1.0	17.9	1.2	0.7	1.0
	10^7	1.0	1.0	1.0	1.0	8.5	NaN	0.8	1.0
	10^8	1.0	0.0	1.0	1.0	13.8	NaN	1.7	1.0
	10^9	1.0	0.0	0.0	1.0	2.1	NaN	2.1	1.0

Table 18: Zeus Malware – Instance 2 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.06	1.06	1.00	1.00	1.00	1.00	1.17	1.00	1.00	1.00	1.00	1.00	1.00
	Normal	1.12	1.11	1.16	1.16	1.10	1.10	1.22	1.10	1.13	1.13	1.13	1.15	1.17
	Delta Normal (%)	**4.8**	**4.2**	**13.6**	**13.6**	**9.1**	**9.1**	**3.9**	**9.1**	**11.6**	**11.6**	**11.7**	**13.1**	**14.9**
CFD	Malware	0.13	0.12	0.00	0.00	0.00	0.00	1.18	0.00	1.00	1.00	1.00	1.00	0.00
	Normal	0.19	0.19	0.21	0.21	0.09	0.12	1.09	1.13	1.07	1.07	1.04	0.97	1.03
	Delta Normal (%)	**32.4**	**36.8**	**97.8**	**97.8**	**97.8**	**98.0**	**-8.1**	**100.0**	**6.5**	**6.5**	**4.0**	**-3.0**	**100.0**
IFD	Malware	0.19	0.18	0.01	0.01	0.00	0.00	1.71	0.00	1.44	1.44	1.44	1.44	0.00
	Normal	0.28	0.29	0.32	0.32	0.13	0.18	1.58	1.63	1.54	1.54	1.51	1.41	1.48
	Delta Normal (%)	**32.6**	**37.0**	**97.8**	**97.8**	**97.9**	**98.0**	**-8.1**	**100.0**	**6.6**	**6.6**	**4.6**	**-2.7**	**100.0**

Table 19: Zeus Malware – Instance 2 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	67.31		32.69		20.00		20.00		20.00		40.00	
	VFD	90.38	**34.29**	90.38	**176.47**	100.00	**400.00**	100.00	**400.00**	100.00	**400.00**	50.00	**25.00**
	CFD	38.46	**-42.86**	46.15	**41.18**	50.00	**150.00**	50.00	**150.00**	100.00	**400.00**	50.00	**25.00**
	IFD	34.62	**-48.57**	38.46	**17.65**	50.00	**150.00**	50.00	**150.00**	50.00	**150.00**	50.00	**25.00**
TNR (%)	**Euclid.**	31.07		65.36		79.43		79.06		78.87		59.81	
	VFD	28.57	**-8.05**	26.79	**-59.02**	28.30	**-64.37**	28.30	**-64.20**	9.43	**-88.04**	44.34	**-25.87**
	CFD	60.71	**95.40**	67.86	**3.83**	33.02	**-58.43**	33.02	**-58.23**	7.55	**-90.43**	23.58	**-60.57**
	IFD	66.07	**112.64**	69.64	**6.56**	28.30	**-64.37**	28.30	**-64.20**	7.55	**-90.43**	13.21	**-77.92**
FPR (%)	**Euclid.**	68.93		34.64		20.57		20.94		21.13		40.19	
	VFD	71.43	**-3.63**	73.21	**-111.34**	71.70	**-248.62**	71.70	**-242.34**	90.57	**-328.57**	55.66	**-38.50**
	CFD	39.29	**43.01**	32.14	**7.22**	66.98	**-225.69**	66.98	**-219.82**	92.45	**-337.50**	76.42	**-90.14**
	IFD	33.93	**50.78**	30.36	**12.37**	71.70	**-248.62**	71.70	**-242.34**	92.45	**-337.50**	86.79	**-115.96**
FNR (%)	**Euclid.**	32.69		67.31		80.00		80.00		80.00		60.00	
	VFD	9.62	**70.59**	9.62	**85.71**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**	50.00	**16.67**
	CFD	61.54	**-88.24**	53.85	**20.00**	50.00	**37.50**	50.00	**37.50**	0.00	**100.00**	50.00	**16.67**
	IFD	65.38	**-100.00**	61.54	**8.57**	50.00	**37.50**	50.00	**37.50**	50.00	**37.50**	50.00	**16.67**
Prec. (%)	**Euclid.**	48.55		34.66		0.37		0.38		0.38		0.75	
	VFD	54.02	**11.27**	53.41	**54.08**	2.56	**585.90**	2.56	**579.49**	2.04	**440.82**	1.67	**122.92**
	CFD	47.62	**-1.92**	57.14	**64.85**	1.39	**271.53**	1.39	**268.06**	2.00	**430.00**	1.22	**63.11**
	IFD	48.65	**0.20**	54.05	**55.94**	1.30	**247.40**	1.30	**244.16**	1.01	**167.68**	1.08	**43.82**
Acc. (%)	**Euclid.**	48.52		49.63		78.33		77.96		77.78		59.44	
	VFD	58.33	**20.23**	57.41	**15.67**	29.63	**-62.17**	29.63	**-62.00**	11.11	**-85.71**	44.44	**-25.23**
	CFD	50.00	**3.05**	57.41	**15.67**	33.33	**-57.45**	33.33	**-57.24**	9.26	**-88.10**	24.07	**-59.50**
	IFD	50.93	**4.96**	54.63	**10.07**	28.70	**-63.36**	28.70	**-63.18**	8.33	**-89.29**	13.89	**-76.64**
F1 (%)	**Euclid.**	53.95		28.62		0.73		0.74		0.74		1.47	
	VFD	67.63	**25.35**	67.14	**134.59**	5.00	**581.25**	5.00	**575.00**	4.00	**440.00**	3.23	**119.76**
	CFD	42.55	**-21.12**	51.06	**78.41**	2.70	**268.24**	2.70	**264.86**	3.92	**429.41**	2.38	**62.20**
	IFD	40.45	**-25.02**	44.94	**57.03**	2.53	**244.94**	2.53	**241.77**	1.98	**167.33**	2.11	**43.42**

3) Citadel Malware – Instance 1

Table 20: Citadel Malware – Instance 1 - Malware vs. Normal sample ratio.

	Total	Citadel 01 Malware	Timestamp Resolution (micro-sec)	Total Timestamps (count)	Malware Timestamps (count)	Normal Timestamps (count)	Malware Ratio (%)
Node	249	7	10^0	134.0	54.0	80.0	40.3
			10^1	134.0	54.0	80.0	40.3
			10^2	134.0	54.0	80.0	40.3
			10^3	133.0	54.0	79.0	40.6
			10^4	130.0	54.0	76.0	41.5
			10^5	97.0	49.0	48.0	50.5
			10^6	73.0	39.0	34.0	53.4
			10^7	46.0	30.0	16.0	65.2
			10^8	20.0	15.0	5.0	75.0
			10^9	6.0	6.0	0.0	100.0
Edge	343	11	10^0	134.0	8.0	126.0	6.0
			10^1	134.0	8.0	126.0	6.0
			10^2	134.0	8.0	126.0	6.0
			10^3	133.0	8.0	125.0	6.0
			10^4	130.0	8.0	122.0	6.2
			10^5	97.0	7.0	90.0	7.2
			10^6	73.0	3.0	70.0	4.1
			10^7	46.0	2.0	44.0	4.3
			10^8	20.0	2.0	18.0	10.0
			10^9	6.0	1.0	5.0	16.7

Table 21: Citadel Malware – Instance 1 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Citadel 01 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	11.5454237	1.174371156	0.770446367	1
	10^1	1	1	1	1	11.5454237	1.174371156	0.770446367	1
	10^2	1	1	1	1	11.5454237	1.174371156	0.770446367	1
	10^3	1	1	1	1	10.94075026	1.174323837	0.770446367	1
	10^4	1	1	1	1	9.632777644	1.17415423	0.770446367	1
	10^5	1	1	1	1	12.12505395	1.131081156	0.770446367	1
	10^6	1	1	1	1	14.62367765	NaN	0.770446367	1
	10^7	1	1	1	1	16.13410549	NaN	0.770446367	1
	10^8	1	0	1	1	15.26490664	NaN	1.271608441	1
	10^9	1	0	0	1	3.065102638	NaN	3.179588312	1
Edge	10^0	1	1	1	1	23.53047372	1.174371156	1.022719896	1
	10^1	1	1	1	1	23.53047372	1.174371156	1.022719896	1
	10^2	1	1	1	1	23.53047372	1.174371156	1.022719896	1
	10^3	1	1	1	1	22.93533498	1.174323837	1.022719896	1
	10^4	1	1	1	1	20.79642927	1.17415423	0.934910059	1
	10^5	1	1	1	1	15.00726787	1.131081156	0.200099729	1
	10^6	1	1	1	1	17.60983275	NaN	1.145541141	1
	10^7	1	1	1	1	17.94255083	NaN	1.145541141	1
	10^8	1	0	1	1	14.71309687	NaN	1.607474149	1
	10^9	1	0	0	1	2.881266066	NaN	3.010837912	1

Table 22: Citadel Malware – Instance 1 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.05	1.05	1.01	1.01	1.01	1.00	1.17	1.00	1.68	1.68	1.69	1.75	1.58
	Normal	1.11	1.11	1.16	1.16	1.10	1.11	1.22	1.10	1.13	1.13	1.13	1.14	1.13
	Delta Normal (%)	**5.6**	**4.9**	**12.7**	**12.7**	**8.9**	**9.5**	**3.6**	**9.1**	**-48.2**	**-48.2**	**-49.2**	**-54.0**	**-40.3**
CFD	Malware	0.12	0.12	0.01	0.01	0.00	0.00	1.16	1.58	1.16	1.16	1.13	1.00	1.00
	Normal	0.18	0.19	0.20	0.20	0.09	0.13	1.07	1.12	1.05	1.05	1.02	0.95	1.17
	Delta Normal (%)	**33.7**	**37.2**	**94.8**	**94.8**	**94.6**	**97.4**	**-8.3**	**-40.9**	**-10.1**	**-10.1**	**-9.9**	**-4.9**	**14.8**
IFD	Malware	0.18	0.18	0.02	0.02	0.01	0.00	1.68	2.29	1.67	1.67	1.65	1.44	1.44
	Normal	0.27	0.28	0.30	0.30	0.13	0.18	1.55	1.62	1.52	1.52	1.49	1.38	1.69
	Delta Normal (%)	**33.8**	**37.6**	**94.7**	**94.7**	**94.6**	**97.5**	**-8.3**	**-40.9**	**-10.1**	**-10.1**	**-10.6**	**-4.3**	**14.8**

Table 23: Citadel Malware – Instance 1 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	64.49		72.65		60.00		60.00		17.14		17.14	
	VFD	95.92	**48.73**	95.92	**32.02**	100.00	**66.67**	100.00	**66.67**	85.71	**42.86**	100.00	**483.33**
	CFD	59.18	**-8.23**	61.22	**-15.73**	100.00	**66.67**	100.00	**66.67**	100.00	**66.67**	85.71	**400.00**
	IFD	53.06	**-17.72**	59.18	**-18.54**	42.86	**-28.57**	42.86	**-28.57**	100.00	**66.67**	100.00	**483.33**
TNR (%)	**Euclid.**	32.08		30.42		40.44		40.44		79.33		79.11	
	VFD	22.92	**-28.57**	22.92	**-24.66**	27.78	**-31.32**	27.78	**-31.32**	40.00	**-49.58**	36.67	**-53.65**
	CFD	41.67	**29.87**	45.83	**50.68**	27.78	**-31.32**	27.78	**-31.32**	17.78	**-77.59**	24.44	**-69.10**
	IFD	50.00	**55.84**	58.33	**91.78**	74.44	**84.07**	74.44	**84.07**	17.78	**-77.59**	15.56	**-80.34**
FPR (%)	**Euclid.**	67.92		69.58		59.56		59.56		20.67		20.89	
	VFD	77.08	**-13.50**	77.08	**-10.78**	72.22	**-21.27**	72.22	**-21.27**	60.00	**-190.32**	63.33	**-203.19**
	CFD	58.33	**14.11**	54.17	**22.16**	72.22	**-21.27**	72.22	**-21.27**	82.22	**-297.85**	75.56	**-261.70**
	IFD	50.00	**26.38**	41.67	**40.12**	25.56	**57.09**	25.56	**57.09**	82.22	**-297.85**	84.44	**-304.26**
FNR (%)	**Euclid.**	35.51		27.35		40.00		40.00		82.86		82.86	
	VFD	4.08	**88.51**	4.08	**85.07**	0.00	**100.00**	0.00	**100.00**	14.29	**82.76**	0.00	**100.00**
	CFD	40.82	**-14.94**	38.78	**-41.79**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**	14.29	**82.76**
	IFD	46.94	**-32.18**	40.82	**-49.25**	57.14	**-42.86**	57.14	**-42.86**	0.00	**100.00**	0.00	**100.00**
Prec. (%)	**Euclid.**	48.97		51.27		4.39		4.42		0.00		1.25	
	VFD	55.95	**14.25**	55.95	**9.12**	9.72	**121.45**	9.72	**119.91**	10.00	**1000.00**	10.94	**775.00**
	CFD	50.88	**3.89**	53.57	**4.48**	9.72	**121.45**	9.72	**119.91**	8.64	**864.00**	8.11	**548.65**
	IFD	52.00	**6.18**	59.18	**15.43**	11.54	**162.81**	11.54	**160.99**	8.64	**864.00**	8.43	**574.70**
Acc. (%)	**Euclid.**	48.45		51.75		41.86		41.86		74.85		74.64	
	VFD	59.79	**23.40**	59.79	**15.54**	32.99	**-21.18**	32.99	**-21.18**	43.30	**-42.15**	41.24	**-44.75**
	CFD	50.52	**4.26**	53.61	**3.59**	32.99	**-21.18**	32.99	**-21.18**	23.71	**-68.32**	28.87	**-61.33**
	IFD	51.55	**6.38**	58.76	**13.55**	72.16	**72.41**	72.16	**72.41**	23.71	**-68.32**	21.65	**-70.99**
F1 (%)	**Euclid.**	52.97		56.91		8.18		8.24		2.35		2.33	
	VFD	70.68	**33.42**	70.68	**24.19**	17.72	**116.59**	17.72	**115.19**	17.91	**661.19**	19.72	**746.24**
	CFD	54.72	**3.29**	57.14	**0.41**	17.72	**116.59**	17.72	**115.19**	15.91	**576.14**	14.81	**535.80**
	IFD	52.53	**-0.85**	59.18	**4.00**	18.18	**122.22**	18.18	**120.78**	15.91	**576.14**	15.56	**567.59**

4) Citadel Malware – Instance 2

Table 24: Citadel Malware – Instance 2 - Malware vs. Normal sample ratio.

	Total	Citadel 02 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	249	6	10^0	133.0	71.0	62.0	53.4
			10^1	133.0	71.0	62.0	53.4
			10^2	133.0	71.0	62.0	53.4
			10^3	132.0	71.0	61.0	53.8
			10^4	129.0	70.0	59.0	54.3
			10^5	96.0	56.0	40.0	58.3
			10^6	77.0	47.0	30.0	61.0
			10^7	42.0	33.0	9.0	78.6
			10^8	20.0	16.0	4.0	80.0
			10^9	6.0	6.0	0.0	100.0
Edge	343	10	10^0	133.0	8.0	125.0	6.0
			10^1	133.0	8.0	125.0	6.0
			10^2	133.0	8.0	125.0	6.0
			10^3	132.0	8.0	124.0	6.1
			10^4	129.0	8.0	121.0	6.2
			10^5	96.0	6.0	90.0	6.3
			10^6	77.0	5.0	72.0	6.5
			10^7	42.0	3.0	39.0	7.1
			10^8	20.0	3.0	17.0	15.0
			10^9	6.0	2.0	4.0	33.3

Table 25: Citadel Malware – Instance 2 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Citadel 02 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	16.45397268	1.174323837	0.821241631	1
	10^1	1	1	1	1	16.45397268	1.174323837	0.821241631	1
	10^2	1	1	1	1	16.45397268	1.174323837	0.821241631	1
	10^3	1	1	1	1	15.14075418	1.174323837	0.821241631	1
	10^4	1	1	1	1	14.00909619	1.174103906	0.619807359	1
	10^5	1	1	1	1	5.909113122	1.131081156	0.619807359	1
	10^6	1	1	1	1	3.30336673	NaN	1.064458715	1
	10^7	1	0	1	1	6.925674798	NaN	1.23957975	1
	10^8	1	0	1	1	14.18543921	NaN	0.734161598	1
	10^9	1	0	0	1	2.368467712	NaN	1.412647051	1
Edge	10^0	1	1	1	1	53.28359947	1.174323837	0.763962307	1
	10^1	1	1	1	1	53.28359947	1.174323837	0.763962307	1
	10^2	1	1	1	1	53.28359947	1.174323837	0.763962307	1
	10^3	1	1	1	1	50.65493197	1.174323837	0.763962307	1
	10^4	1	1	1	1	43.88714243	1.174103906	0.608381046	1
	10^5	1	1	1	1	8.927001715	1.131081156	0.608381046	1
	10^6	1	1	1	1	4.321115283	NaN	0.726364181	1
	10^7	1	0	1	1	7.32628763	NaN	0.600220914	1
	10^8	1	0	1	1	13.44586885	NaN	1.129658037	1
	10^9	1	0	0	1	1.786234965	NaN	2.610115485	1

Table 26: Citadel Malware – Instance 2 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.08	1.08	1.01	1.01	1.01	1.00	1.22	1.00	1.68	1.68	1.68	1.94	1.58
	Normal	1.09	1.09	1.15	1.15	1.10	1.10	1.17	1.10	1.14	1.14	1.14	1.16	1.13
	Delta Normal (%)	**0.9**	**0.4**	**12.5**	**12.5**	**8.5**	**8.3**	**-4.3**	**9.4**	**-47.3**	**-47.3**	**-47.3**	**-67.4**	**-40.3**
CFD	Malware	0.16	0.15	0.01	0.01	0.00	0.01	1.03	1.58	1.16	1.16	1.16	0.92	1.00
	Normal	0.14	0.14	0.19	0.19	0.08	0.12	1.22	1.09	1.04	1.04	1.02	0.94	1.17
	Delta Normal (%)	**-15.6**	**-8.2**	**95.2**	**95.2**	**94.7**	**95.5**	**16.1**	**-45.8**	**-11.9**	**-11.9**	**-14.3**	**2.5**	**14.6**
IFD	Malware	0.24	0.23	0.01	0.01	0.01	0.01	1.48	2.29	1.67	1.67	1.67	1.39	1.44
	Normal	0.21	0.21	0.29	0.29	0.12	0.17	1.76	1.57	1.50	1.50	1.47	1.36	1.69
	Delta Normal (%)	**-15.2**	**-8.2**	**95.1**	**95.1**	**94.8**	**95.5**	**16.1**	**-45.8**	**-11.9**	**-11.9**	**-13.7**	**-1.7**	**14.6**

Table 27: Citadel Malware – Instance 2 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	25.71		66.79		40.00		40.00		36.67		40.00	
	VFD	83.93	**226.39**	82.14	**22.99**	83.33	**108.33**	83.33	**108.33**	66.67	**66.67**	83.33	**108.33**
	CFD	32.14	**25.00**	33.93	**-49.20**	66.67	**66.67**	66.67	**66.67**	100.00	**150.00**	66.67	**66.67**
	IFD	37.50	**45.83**	39.29	**-41.18**	50.00	**25.00**	50.00	**25.00**	100.00	**150.00**	66.67	**66.67**
TNR (%)	**Euclid.**	73.00		36.50		59.33		60.00		58.89		59.78	
	VFD	40.00	**-45.21**	37.50	**2.74**	35.56	**-40.07**	35.56	**-40.74**	21.11	**-64.15**	30.00	**-49.81**
	CFD	55.00	**-24.66**	60.00	**64.38**	42.22	**-28.84**	42.22	**-29.63**	13.33	**-77.36**	44.44	**-25.65**
	IFD	55.00	**-24.66**	60.00	**64.38**	77.78	**31.09**	77.78	**29.63**	28.89	**-50.94**	28.89	**-51.67**
FPR (%)	**Euclid.**	27.00		63.50		40.67		40.00		41.11		40.22	
	VFD	60.00	**-122.22**	62.50	**1.57**	64.44	**-58.47**	64.44	**-61.11**	78.89	**-91.89**	70.00	**-74.03**
	CFD	45.00	**-66.67**	40.00	**37.01**	57.78	**-42.08**	57.78	**-44.44**	86.67	**-110.81**	55.56	**-38.12**
	IFD	45.00	**-66.67**	40.00	**37.01**	22.22	**45.36**	22.22	**44.44**	71.11	**-72.97**	71.11	**-76.80**
FNR (%)	**Euclid.**	74.29		33.21		60.00		60.00		63.33		60.00	
	VFD	16.07	**78.37**	17.86	**46.24**	16.67	**72.22**	16.67	**72.22**	33.33	**47.37**	16.67	**72.22**
	CFD	67.86	**8.65**	66.07	**-98.92**	33.33	**44.44**	33.33	**44.44**	0.00	**100.00**	33.33	**44.44**
	IFD	62.50	**15.87**	60.71	**-82.80**	50.00	**16.67**	50.00	**16.67**	0.00	**100.00**	33.33	**44.44**
Prec. (%)	**Euclid.**	45.83		55.13		2.54		2.55		2.33		2.53	
	VFD	66.20	**44.46**	64.79	**17.53**	7.94	**212.49**	7.94	**210.85**	5.33	**129.19**	7.35	**191.05**
	CFD	50.00	**9.11**	54.29	**-1.53**	7.14	**181.24**	7.14	**179.76**	7.14	**206.96**	7.41	**193.21**
	IFD	53.85	**17.50**	57.89	**5.02**	13.04	**413.57**	13.04	**410.87**	8.57	**268.35**	5.88	**132.84**
Acc. (%)	**Euclid.**	45.42		54.17		58.13		58.75		57.50		58.54	
	VFD	65.63	**44.50**	63.54	**17.31**	38.54	**-33.69**	38.54	**-34.40**	23.96	**-58.33**	33.33	**-43.06**
	CFD	41.67	**-8.26**	44.79	**-17.31**	43.75	**-24.73**	43.75	**-25.53**	18.75	**-67.39**	45.83	**-21.71**
	IFD	44.79	**-1.38**	47.92	**-11.54**	76.04	**30.82**	76.04	**29.43**	33.33	**-42.03**	31.25	**-46.62**
F1 (%)	**Euclid.**	24.35		57.30		4.78		4.80		4.38		4.75	
	VFD	74.02	**203.93**	72.44	**26.42**	14.49	**203.43**	14.49	**201.93**	9.88	**125.69**	13.51	**184.35**
	CFD	39.13	**60.68**	41.76	**-27.12**	12.90	**170.15**	12.90	**168.82**	13.33	**204.68**	13.33	**180.56**
	IFD	44.21	**81.54**	46.81	**-18.31**	20.69	**333.18**	20.69	**331.03**	15.79	**260.80**	10.81	**127.48**

5) Hupigon Malware – Instance 1

Table 28: Hupigon Malware – Instance 1 - Malware vs. Normal sample ratio.

	Total	Citadel 02 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	249	7	10^0	165.0	79.0	86.0	47.9
			10^1	165.0	79.0	86.0	47.9
			10^2	165.0	79.0	86.0	47.9
			10^3	165.0	79.0	86.0	47.9
			10^4	164.0	79.0	85.0	48.2
			10^5	126.0	67.0	59.0	53.2
			10^6	101.0	52.0	49.0	51.5
			10^7	71.0	41.0	30.0	57.7
			10^8	27.0	21.0	6.0	77.8
			10^9	6.0	6.0	0.0	100.0
Edge	343	10	10^0	165.0	5.0	160.0	3.0
			10^1	165.0	5.0	160.0	3.0
			10^2	165.0	5.0	160.0	3.0
			10^3	165.0	5.0	160.0	3.0
			10^4	164.0	5.0	159.0	3.0
			10^5	126.0	3.0	123.0	2.4
			10^6	101.0	2.0	99.0	2.0
			10^7	71.0	1.0	70.0	1.4
			10^8	27.0	1.0	26.0	3.7
			10^9	6.0	1.0	5.0	16.7

Table 29: Hupigon Malware – Instance 1 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Hpuigon 01 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	14.15286672	1.167097287	0.51217452	1
	10^1	1	1	1	1	14.15286672	1.167097287	0.51217452	1
	10^2	1	1	1	1	14.15286672	1.167097287	0.51217452	1
	10^3	1	1	1	1	14.15286672	1.167097287	0.51217452	1
	10^4	1	1	1	1	13.61831271	1.167097287	0.51217452	1
	10^5	1	1	1	1	10.57442344	1.129884448	0.419624662	1
	10^6	1	1	1	1	16.98613773	1.131577303	0.51217452	1
	10^7	1	1	1	1	14.66355563	NaN	0.51217452	1
	10^8	1	0	1	1	7.181302025	NaN	1.161486109	1
	10^9	1	0	0	1	1.985076345	NaN	1.390455134	1
Edge	10^0	1	1	1	1	25.65890035	1.167097287	1.227132368	1
	10^1	1	1	1	1	25.65890035	1.167097287	1.227132368	1
	10^2	1	1	1	1	25.65890035	1.167097287	1.227132368	1
	10^3	1	1	1	1	25.65890035	1.167097287	1.227132368	1
	10^4	1	1	1	1	25.17563722	1.167097287	1.227132368	1
	10^5	1	1	1	1	15.84069918	1.129884448	0.325089649	1
	10^6	1	1	1	1	22.37946133	1.131577303	0.999890682	1
	10^7	1	1	1	1	16.4036598	NaN	0.234389163	1
	10^8	1	0	0	1	5.720341007	NaN	1.66867243	1
	10^9	1	0	0	1	2.048612128	NaN	1.438543493	1

Table 30: Hupigon Malware – Instance 1 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.08	1.08	1.00	1.00	1.00	1.00	1.23	1.00	1.68	1.68	1.67	2.36	1.00
	Normal	1.08	1.09	1.13	1.13	1.10	1.08	1.22	1.14	1.08	1.08	1.08	1.10	1.17
	Delta Normal (%)	**0.2**	**0.8**	**11.0**	**11.0**	**9.2**	**7.2**	**-0.6**	**12.2**	**-55.0**	**-55.0**	**-54.5**	**-113.4**	**14.3**
CFD	Malware	0.13	0.13	0.01	0.01	0.00	0.00	1.07	1.58	1.16	1.16	1.10	0.74	1.00
	Normal	0.14	0.14	0.19	0.19	0.09	0.11	1.09	1.02	1.07	1.07	1.04	0.99	1.06
	Delta Normal (%)	**2.6**	**11.5**	**97.1**	**97.1**	**96.9**	**98.2**	**2.5**	**-54.7**	**-8.4**	**-8.4**	**-5.4**	**25.4**	**5.4**
IFD	Malware	0.20	0.19	0.01	0.01	0.00	0.00	1.54	2.29	1.67	1.67	1.62	1.10	1.44
	Normal	0.21	0.22	0.28	0.28	0.13	0.16	1.58	1.48	1.55	1.55	1.51	1.42	1.53
	Delta Normal (%)	**2.6**	**11.1**	**97.1**	**97.1**	**96.9**	**98.2**	**2.5**	**-54.7**	**-8.3**	**-8.3**	**-7.3**	**22.8**	**5.4**

Table 31: Hupigon Malware – Instance 1 - Evaluation Metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	74.03		16.12		40.00		73.33		20.00		80.00	
	VFD	85.07	**14.92**	86.57	**437.04**	100.00	**150.00**	100.00	**36.36**	33.33	**-16.67**	100.00	**25.00**
	CFD	40.30	**-45.56**	41.79	**159.26**	33.33	**-16.67**	33.33	**-54.55**	33.33	**-16.67**	66.67	**-16.67**
	IFD	13.43	**-81.85**	16.42	**1.85**	33.33	**-16.67**	33.33	**-54.55**	33.33	**-16.67**	66.67	**-16.67**
TNR (%)	**Euclid.**	25.42		83.39		59.67		20.81		79.19		20.49	
	VFD	20.34	**-20.00**	20.34	**-75.61**	28.46	**-52.32**	28.46	**36.72**	36.59	**-53.80**	21.14	**3.17**
	CFD	52.54	**106.67**	54.24	**-34.96**	52.03	**-12.81**	52.03	**150.00**	26.83	**-66.12**	20.33	**-0.79**
	IFD	74.58	**193.33**	79.66	**-4.47**	49.59	**-16.89**	49.59	**138.28**	35.77	**-54.83**	17.07	**-16.67**
FPR (%)	**Euclid.**	74.58		16.61		40.33		79.19		20.81		79.51	
	VFD	79.66	**-6.82**	79.66	**-379.59**	71.54	**-77.42**	71.54	**9.65**	63.41	**-204.69**	78.86	**0.82**
	CFD	47.46	**36.36**	45.76	**-175.51**	47.97	**-18.95**	47.97	**39.43**	73.17	**-251.56**	79.67	**-0.20**
	IFD	25.42	**65.91**	20.34	**-22.45**	50.41	**-25.00**	50.41	**36.34**	64.23	**-208.59**	82.93	**-4.29**
FNR (%)	**Euclid.**	25.97		83.88		60.00		26.67		80.00		20.00	
	VFD	14.93	**42.53**	13.43	**83.99**	0.00	**100.00**	0.00	**100.00**	66.67	**16.67**	0.00	**100.00**
	CFD	59.70	**-129.89**	58.21	**30.60**	66.67	**-11.11**	66.67	**-150.00**	66.67	**16.67**	33.33	**-66.67**
	IFD	86.57	**-233.33**	83.58	**0.36**	66.67	**-11.11**	66.67	**-150.00**	66.67	**16.67**	33.33	**-66.67**
Prec. (%)	**Euclid.**	52.92		38.09		0.97		1.77		0.48		1.92	
	VFD	54.81	**3.57**	55.24	**45.03**	3.30	**240.64**	3.30	**85.81**	1.27	**161.60**	3.00	**56.25**
	CFD	49.09	**-7.23**	50.91	**33.66**	1.67	**72.21**	1.67	**-6.06**	1.10	**127.11**	2.00	**4.17**
	IFD	37.50	**-29.14**	47.83	**25.57**	1.59	**64.01**	1.59	**-10.53**	1.25	**158.33**	1.92	**0.16**
Acc. (%)	**Euclid.**	51.27		47.62		59.21		22.06		77.78		21.90	
	VFD	54.76	**6.81**	55.56	**16.67**	30.16	**-49.06**	30.16	**36.69**	36.51	**-53.06**	23.02	**5.07**
	CFD	46.03	**-10.22**	47.62	**0.00**	51.59	**-12.87**	51.59	**133.81**	26.98	**-65.31**	21.43	**-2.17**
	IFD	42.06	**-17.96**	46.03	**-3.33**	49.21	**-16.89**	49.21	**123.02**	35.71	**-54.08**	18.25	**-16.67**
F1 (%)	**Euclid.**	60.33		18.34		1.89		3.46		0.94		3.75	
	VFD	66.67	**10.51**	67.44	**267.81**	6.38	**237.75**	6.38	**84.24**	2.44	**158.13**	5.83	**55.34**
	CFD	44.26	**-26.63**	45.90	**150.34**	3.17	**67.98**	3.17	**-8.37**	2.13	**125.18**	3.88	**3.56**
	IFD	19.78	**-67.21**	24.44	**33.31**	3.03	**60.34**	3.03	**-12.53**	2.41	**155.02**	3.74	**-0.31**

6) Hupigon Malware – Instance 2

Table 32: Hupigon Malware – Instance 2 - Malware vs. Normal sample ratio.

	Total	Hupigon 02 Malware	Timestamp Resolution (micro-sec)	Total Timestamps (count)	Malware Timestamps (count)	Normal Timestamps (count)	Malware Ratio (%)
Node	340	14	10^0	204.0	98.0	106.0	48.0
			10^1	204.0	98.0	106.0	48.0
			10^2	204.0	98.0	106.0	48.0
			10^3	202.0	97.0	105.0	48.0
			10^4	199.0	96.0	103.0	48.2
			10^5	150.0	80.0	70.0	53.3
			10^6	115.0	59.0	56.0	51.3
			10^7	73.0	46.0	27.0	63.0
			10^8	32.0	24.0	8.0	75.0
			10^9	7.0	6.0	1.0	85.7
Edge	516	23	10^0	204.0	14.0	190.0	6.9
			10^1	204.0	14.0	190.0	6.9
			10^2	204.0	14.0	190.0	6.9
			10^3	202.0	14.0	188.0	6.9
			10^4	199.0	14.0	185.0	7.0
			10^5	150.0	9.0	141.0	6.0
			10^6	115.0	6.0	109.0	5.2
			10^7	73.0	5.0	68.0	6.8
			10^8	32.0	3.0	29.0	9.4
			10^9	7.0	2.0	5.0	28.6

Table 33: Hupigon Malware – Instance 2 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Hpuigon 02 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	9.092949455	1.103536462	0.878803603	1
	10^1	1	1	1	1	9.092949455	1.103536462	0.878803603	1
	10^2	1	1	1	1	9.092949455	1.103536462	0.878803603	1
	10^3	1	1	1	1	8.529095779	1.103466783	0.800725925	1
	10^4	1	1	1	1	7.857715109	1.103302004	0.800725925	1
	10^5	1	1	1	1	9.239420557	1.174776103	0.682120802	1
	10^6	1	1	1	1	6.187119964	1.128877982	0.079882595	1
	10^7	1	1	1	1	20.17323736	NaN	0.371606087	1
	10^8	1	1	1	1	11.14163085	NaN	1.483963555	1
	10^9	1	0	0	1	1.904881061	NaN	1.384920482	1
Edge	10^0	1	1	1	1	23.91561637	1.103536462	0.878803603	1
	10^1	1	1	1	1	23.91561637	1.103536462	0.878803603	1
	10^2	1	1	1	1	23.91561637	1.103536462	0.878803603	1
	10^3	1	1	1	1	22.52253713	1.103466783	0.878803603	1
	10^4	1	1	1	1	20.84726705	1.103302004	0.878803603	1
	10^5	1	1	1	1	14.3844856	1.174776103	0.767953972	1
	10^6	1	1	1	1	8.361412269	1.128877982	0.313963067	1
	10^7	1	1	1	1	25.8474268	NaN	0.531669823	1
	10^8	1	0	1	1	11.37590539	NaN	1.485297651	1
	10^9	1	0	0	1	1.678549122	NaN	2.044376422	1

Table 34: Hupigon Malware – Instance 2 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.08	1.08	1.01	1.01	1.01	1.00	1.13	1.36	1.43	1.43	1.42	1.87	1.36
	Normal	1.08	1.08	1.10	1.10	1.08	1.05	1.13	1.13	1.08	1.08	1.08	1.11	1.17
	Delta Normal (%)	**0.2**	**0.3**	**8.5**	**8.5**	**7.1**	**4.4**	**0.1**	**-20.4**	**-32.5**	**-32.5**	**-31.8**	**-69.1**	**-16.7**
CFD	Malware	0.14	0.13	0.01	0.01	0.01	0.00	1.09	1.40	1.17	1.17	1.13	0.95	1.40
	Normal	0.14	0.14	0.15	0.15	0.07	0.08	1.12	1.05	1.10	1.10	1.08	1.01	1.11
	Delta Normal (%)	**-2.2**	**8.6**	**93.0**	**93.0**	**93.1**	**96.3**	**2.6**	**-33.8**	**-6.0**	**-6.0**	**-4.6**	**6.1**	**-26.7**
IFD	Malware	0.21	0.20	0.02	0.02	0.01	0.00	1.57	2.03	1.69	1.69	1.65	1.41	2.03
	Normal	0.21	0.22	0.23	0.23	0.11	0.12	1.61	1.51	1.59	1.59	1.56	1.45	1.60
	Delta Normal (%)	**-1.7**	**8.6**	**92.9**	**92.9**	**93.1**	**96.3**	**2.6**	**-33.8**	**-6.0**	**-6.0**	**-5.7**	**3.2**	**-26.7**

Table 35: Hupigon Malware – Instance 2 - Evaluation Metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	49.25		64.75		57.78		37.78		100.00		20.00	
	VFD	83.75	**70.05**	86.25	**33.20**	100.00	**73.08**	100.00	**164.71**	66.67	**15.38**	100.00	**400.00**
	CFD	58.75	**19.29**	67.50	**4.25**	66.67	**15.38**	66.67	**76.47**	88.89	**53.85**	77.78	**288.89**
	IFD	57.50	**16.75**	66.25	**2.32**	66.67	**15.38**	66.67	**76.47**	88.89	**53.85**	77.78	**288.89**
TNR (%)	**Euclid.**	52.29		36.57		40.43		59.43		1.70		79.29	
	VFD	25.71	**-50.82**	27.14	**-25.78**	19.86	**-50.88**	19.86	**-66.59**	22.70	**1233.33**	18.44	**-76.74**
	CFD	24.29	**-53.55**	35.71	**-2.34**	14.89	**-63.16**	14.89	**-74.94**	5.67	**233.33**	12.77	**-83.90**
	IFD	27.14	**-48.09**	38.57	**5.47**	16.31	**-59.65**	16.31	**-72.55**	6.38	**275.00**	12.06	**-84.79**
FPR (%)	**Euclid.**	47.71		63.43		59.57		40.57		98.30		20.71	
	VFD	74.29	**-55.69**	72.86	**-14.86**	80.14	**-34.52**	80.14	**-97.55**	77.30	**21.36**	81.56	**-293.84**
	CFD	75.71	**-58.68**	64.29	**-1.35**	85.11	**-42.86**	85.11	**-109.79**	94.33	**4.04**	87.23	**-321.23**
	IFD	72.86	**-52.69**	61.43	**3.15**	83.69	**-40.48**	83.69	**-106.29**	93.62	**4.76**	87.94	**-324.66**
FNR (%)	**Euclid.**	50.75		35.25		42.22		62.22		0.00		80.00	
	VFD	16.25	**67.98**	13.75	**60.99**	0.00	**100.00**	0.00	**100.00**	33.33	**-3333.00**	0.00	**100.00**
	CFD	41.25	**18.72**	32.50	**7.80**	33.33	**21.05**	33.33	**46.43**	11.11	**-1111.00**	22.22	**72.22**
	IFD	42.50	**16.26**	33.75	**4.26**	33.33	**21.05**	33.33	**46.43**	11.11	**-1111.00**	22.22	**72.22**
Prec. (%)	**Euclid.**	52.10		43.07		3.51		2.30		6.10		1.21	
	VFD	56.30	**8.07**	57.50	**33.49**	7.38	**110.01**	7.38	**221.12**	5.22	**-14.44**	7.26	**500.81**
	CFD	47.00	**-9.78**	54.55	**26.63**	4.76	**35.56**	4.76	**107.28**	5.67	**-6.95**	5.38	**345.73**
	IFD	47.42	**-8.97**	55.21	**28.17**	4.84	**37.75**	4.84	**110.63**	5.71	**-6.29**	5.34	**342.32**
Acc. (%)	**Euclid.**	50.67		51.60		41.47		58.13		7.60		75.73	
	VFD	56.67	**11.84**	58.67	**13.70**	24.67	**-40.51**	24.67	**-57.57**	25.33	**233.33**	23.33	**-69.19**
	CFD	42.67	**-15.79**	52.67	**2.07**	18.00	**-56.59**	18.00	**-69.04**	10.67	**40.35**	16.67	**-77.99**
	IFD	43.33	**-14.47**	53.33	**3.36**	19.33	**-53.38**	19.33	**-66.74**	11.33	**49.12**	16.00	**-78.87**
F1 (%)	**Euclid.**	44.74		51.05		6.62		4.33		11.49		2.28	
	VFD	67.34	**50.50**	69.00	**35.17**	13.74	**107.47**	13.74	**217.24**	9.68	**-15.81**	13.53	**493.98**
	CFD	52.22	**16.72**	60.34	**18.19**	8.89	**34.22**	8.89	**105.23**	10.67	**-7.20**	10.07	**342.05**
	IFD	51.98	**16.17**	60.23	**17.98**	9.02	**36.24**	9.02	**108.31**	10.74	**-6.58**	10.00	**338.89**

7) Zurgop Malware – Instance 1

Table 36: Zurgop Malware – Instance 1 - Malware vs. Normal sample ratio.

	Total	Zurgop 01 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	336	6	10^0	197.0	93.0	104.0	47.2
			10^1	197.0	93.0	104.0	47.2
			10^2	197.0	93.0	104.0	47.2
			10^3	196.0	93.0	103.0	47.4
			10^4	195.0	93.0	102.0	47.7
			10^5	150.0	74.0	76.0	49.3
			10^6	111.0	59.0	52.0	53.2
			10^7	70.0	46.0	24.0	65.7
			10^8	31.0	21.0	10.0	67.7
			10^9	6.0	6.0	0.0	100.0
Edge	517	8	10^0	197.0	8.0	189.0	4.1
			10^1	197.0	8.0	189.0	4.1
			10^2	197.0	8.0	189.0	4.1
			10^3	196.0	8.0	188.0	4.1
			10^4	195.0	8.0	187.0	4.1
			10^5	150.0	8.0	142.0	5.3
			10^6	111.0	6.0	105.0	5.4
			10^7	70.0	6.0	64.0	8.6
			10^8	31.0	4.0	27.0	12.9
			10^9	6.0	4.0	2.0	66.7

Table 37: Zurgop Malware – Instance 1 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Zurgop 01 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	16.65290671	1.103280543	0.808255513	1
	10^1	1	1	1	1	16.65290671	1.103280543	0.808255513	1
	10^2	1	1	1	1	16.65290671	1.103280543	0.808255513	1
	10^3	1	1	1	1	16.14672976	1.103280543	0.808255513	1
	10^4	1	1	1	1	15.66104266	1.103204954	0.808255513	1
	10^5	1	1	1	1	11.60061941	1.174776103	0.482338104	1
	10^6	1	1	1	1	13.42799163	1.13255672	0.193510766	1
	10^7	1	1	1	1	15.67752707	NaN	1.019906073	1
	10^8	1	1	1	1	14.3926202	NaN	1.230528091	1
	10^9	1	0	0	1	2.271901289	NaN	2.488223064	1
Edge	10^0	1	1	1	1	37.11812093	1.103280543	0.926400176	1
	10^1	1	1	1	1	37.11812093	1.103280543	0.926400176	1
	10^2	1	1	1	1	37.11812093	1.103280543	0.926400176	1
	10^3	1	1	1	1	35.93397582	1.103280543	0.926400176	1
	10^4	1	1	1	1	34.80505492	1.103204954	0.926400176	1
	10^5	1	1	1	1	16.83203108	1.174776103	0.828679453	1
	10^6	1	1	1	1	14.4685489	1.13255672	0.372363337	1
	10^7	1	1	1	1	21.21775778	NaN	1.111302853	1
	10^8	1	1	1	1	15.70044358	NaN	1.117418365	1
	10^9	1	0	0	1	2.344485182	NaN	2.917520306	1

Table 38: Zurgop Malware – Instance 1 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.07	1.07	1.01	1.01	1.00	1.00	1.22	1.00	1.58	1.58	1.58	1.74	1.58
	Normal	1.10	1.11	1.14	1.14	1.09	1.08	1.13	1.13	1.08	1.08	1.08	1.09	1.17
	Delta Normal (%)	**2.8**	**3.2**	**11.7**	**11.7**	**8.2**	**7.4**	**-7.7**	**11.7**	**-46.8**	**-46.8**	**-46.7**	**-58.7**	**-35.7**
CFD	Malware	0.13	0.13	0.01	0.01	0.00	0.00	1.12	1.58	1.00	1.00	1.00	0.71	1.00
	Normal	0.14	0.15	0.18	0.18	0.08	0.10	1.11	1.05	1.11	1.11	1.08	1.02	1.11
	Delta Normal (%)	**4.1**	**13.4**	**95.3**	**95.3**	**95.0**	**97.2**	**-0.9**	**-50.5**	**10.1**	**10.1**	**7.4**	**30.8**	**9.6**
IFD	Malware	0.20	0.19	0.01	0.01	0.01	0.00	1.62	2.29	1.44	1.44	1.44	1.08	1.44
	Normal	0.21	0.22	0.27	0.27	0.12	0.15	1.61	1.52	1.61	1.61	1.57	1.48	1.60
	Delta Normal (%)	**4.5**	**13.5**	**95.3**	**95.3**	**94.9**	**97.2**	**-0.9**	**-50.5**	**10.1**	**10.1**	**8.0**	**26.7**	**9.6**

Table 39: Zurgop Malware – Instance 1 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	25.95		26.22		0.00		60.00		60.00		60.00	
	VFD	93.24	**259.38**	95.95	**265.98**	62.50	**6250.00**	62.50	**4.17**	75.00	**25.00**	75.00	**25.00**
	CFD	37.84	**45.83**	45.95	**75.26**	50.00	**5000.00**	50.00	**-16.67**	87.50	**45.83**	87.50	**45.83**
	IFD	18.92	**-27.08**	22.97	**-12.37**	50.00	**5000.00**	50.00	**-16.67**	87.50	**45.83**	87.50	**45.83**
TNR (%)	**Euclid.**	76.05		73.68		99.30		40.14		40.28		40.14	
	VFD	36.84	**-51.56**	38.16	**-48.21**	25.35	**-74.47**	25.35	**-36.84**	21.13	**-47.55**	30.99	**-22.81**
	CFD	44.74	**-41.18**	53.95	**-26.79**	43.66	**-56.03**	43.66	**8.77**	15.49	**-61.54**	16.20	**-59.65**
	IFD	68.42	**-10.03**	73.68	**0.00**	28.17	**-71.63**	28.17	**-29.82**	16.20	**-59.79**	15.49	**-61.40**
FPR (%)	**Euclid.**	23.95		26.32		0.70		59.86		59.72		59.86	
	VFD	63.16	**-163.74**	61.84	**-135.00**	74.65	**-10500.00**	74.65	**-24.71**	78.87	**-32.08**	69.01	**-15.29**
	CFD	55.26	**-130.77**	46.05	**-75.00**	56.34	**-7900.00**	56.34	**5.88**	84.51	**-41.51**	83.80	**-40.00**
	IFD	31.58	**-31.87**	26.32	**0.00**	71.83	**-10100.00**	71.83	**-20.00**	83.80	**-40.33**	84.51	**-41.18**
FNR (%)	**Euclid.**	74.05		73.78		100.00		40.00		40.00		40.00	
	VFD	6.76	**90.88**	4.05	**94.51**	37.50	**62.50**	37.50	**6.25**	25.00	**37.50**	25.00	**37.50**
	CFD	62.16	**16.06**	54.05	**26.74**	50.00	**50.00**	50.00	**-25.00**	12.50	**68.75**	12.50	**68.75**
	IFD	81.08	**-9.49**	77.03	**-4.40**	50.00	**50.00**	50.00	**-25.00**	12.50	**68.75**	12.50	**68.75**
Prec. (%)	**Euclid.**	43.62		37.93		0.00		3.24		3.24		3.22	
	VFD	58.97	**35.21**	60.17	**58.62**	4.50	**450.00**	4.50	**38.88**	5.08	**56.77**	5.77	**79.09**
	CFD	40.00	**-8.29**	49.28	**29.90**	4.76	**476.00**	4.76	**46.82**	5.51	**69.94**	5.56	**72.45**
	IFD	36.84	**-15.53**	45.95	**21.12**	3.77	**377.00**	3.77	**16.35**	5.56	**71.29**	5.51	**71.10**
Acc. (%)	**Euclid.**	51.33		50.27		94.00		41.20		41.33		41.20	
	VFD	64.67	**25.97**	66.67	**32.63**	27.33	**-70.92**	27.33	**-33.66**	24.00	**-41.94**	33.33	**-19.09**
	CFD	41.33	**-19.48**	50.00	**-0.53**	44.00	**-53.19**	44.00	**6.80**	19.33	**-53.23**	20.00	**-51.46**
	IFD	44.00	**-14.29**	48.67	**-3.18**	29.33	**-68.79**	29.33	**-28.80**	20.00	**-51.61**	19.33	**-53.07**
F1 (%)	**Euclid.**	26.70		23.10		0.00		6.15		6.15		6.11	
	VFD	72.25	**170.63**	73.96	**220.20**	8.40	**840.00**	8.40	**36.55**	9.52	**54.76**	10.71	**75.22**
	CFD	38.89	**45.66**	47.55	**105.88**	8.70	**840.00**	8.70	**41.30**	10.37	**68.51**	10.45	**70.86**
	IFD	25.00	**-6.36**	30.63	**32.62**	7.02	**702.00**	7.02	**14.03**	10.45	**69.77**	10.37	**69.60**

8) Zurgop Malware – Instance 2

Table 40: Zurgop Malware – Instance 2 - Malware vs. Normal sample ratio.

	Total	Zurgop 02 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	303	5	10^0	161.0	64.0	97.0	39.8
			10^1	161.0	64.0	97.0	39.8
			10^2	161.0	64.0	97.0	39.8
			10^3	161.0	64.0	97.0	39.8
			10^4	158.0	64.0	94.0	40.5
			10^5	121.0	51.0	70.0	42.1
			10^6	91.0	38.0	53.0	41.8
			10^7	59.0	32.0	27.0	54.2
			10^8	21.0	15.0	6.0	71.4
			10^9	6.0	5.0	1.0	83.3
Edge	434	8	10^0	161.0	8.0	153.0	5.0
			10^1	161.0	8.0	153.0	5.0
			10^2	161.0	8.0	153.0	5.0
			10^3	161.0	8.0	153.0	5.0
			10^4	158.0	8.0	150.0	5.1
			10^5	121.0	6.0	115.0	5.0
			10^6	91.0	5.0	86.0	5.5
			10^7	59.0	4.0	55.0	6.8
			10^8	21.0	3.0	18.0	14.3
			10^9	6.0	2.0	4.0	33.3

Table 41: Zurgop Malware – Instance 2 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Zurgop 02 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	28.71332451	1.166956355	0.382840731	1
	10^1	1	1	1	1	28.71332451	1.166956355	0.382840731	1
	10^2	1	1	1	1	28.71332451	1.166956355	0.382840731	1
	10^3	1	1	1	1	28.71332451	1.166956355	0.382840731	1
	10^4	1	1	1	1	26.29090821	1.175220521	0.382840731	1
	10^5	1	1	1	1	14.62820293	1.129491273	0.619807359	1
	10^6	1	1	1	1	9.103303465	1.218997094	0.219846532	1
	10^7	1	1	1	1	11.55130643	NaN	0.435345982	1
	10^8	1	0	1	1	7.15837261	NaN	0.648033781	1
	10^9	1	0	0	1	3.380456026	NaN	1.618524552	1
Edge	10^0	1	1	1	1	47.31198932	1.166956355	0.843976621	1
	10^1	1	1	1	1	47.31198932	1.166956355	0.843976621	1
	10^2	1	1	1	1	47.31198932	1.166956355	0.843976621	1
	10^3	1	1	1	1	47.31198932	1.166956355	0.843976621	1
	10^4	1	1	1	1	43.61715624	1.175220521	0.843976621	1
	10^5	1	1	1	1	22.80998664	1.129491273	1.004332262	1
	10^6	1	1	1	1	10.52342881	1.218997094	-0.13675345	1
	10^7	1	1	1	1	17.04419599	NaN	1.061586398	1
	10^8	1	0	1	1	8.324043282	NaN	1.16632445	1
	10^9	1	0	1	1	3.334951345	NaN	1.929545773	1

Table 42: Zurgop Malware – Instance 2 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.06	1.06	1.01	1.01	1.01	1.01	1.22	1.00	1.58	1.58	1.58	1.74	1.58
	Normal	1.11	1.11	1.12	1.12	1.10	1.07	1.13	1.14	1.08	1.08	1.08	1.12	1.18
	Delta Normal (%)	**4.4**	**4.7**	**10.1**	**10.1**	**8.4**	**5.8**	**-8.1**	**12.2**	**-46.4**	**-46.4**	**-46.3**	**-54.9**	**-34.9**
CFD	Malware	0.11	0.10	0.01	0.01	0.00	0.01	1.00	1.00	1.00	1.00	1.00	0.71	1.00
	Normal	0.17	0.17	0.20	0.20	0.09	0.11	1.08	1.04	1.07	1.07	1.04	0.99	1.05
	Delta Normal (%)	**36.0**	**41.6**	**94.2**	**94.2**	**95.3**	**94.9**	**7.7**	**3.7**	**6.9**	**6.9**	**3.8**	**28.3**	**5.0**
IFD	Malware	0.16	0.15	0.02	0.02	0.01	0.01	1.44	1.44	1.44	1.44	1.44	1.08	1.44
	Normal	0.26	0.26	0.29	0.29	0.13	0.17	1.56	1.50	1.55	1.55	1.51	1.42	1.52
	Delta Normal (%)	**36.0**	**41.8**	**94.1**	**94.1**	**95.3**	**94.9**	**7.7**	**3.7**	**6.9**	**6.9**	**4.4**	**23.9**	**5.0**

Table 43: Zurgop Malware – Instance 2 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	22.75		65.88		40.00		20.00		0.00		40.00	
	VFD	96.08	**322.41**	100.00	**51.79**	66.67	**66.67**	66.67	**233.33**	33.33	**-16.67**	66.67	**66.67**
	CFD	49.02	**115.52**	39.22	**-40.48**	50.00	**25.00**	50.00	**150.00**	83.33	**108.33**	50.00	**25.00**
	IFD	35.29	**55.17**	33.33	**-49.40**	33.33	**-16.67**	33.33	**66.67**	83.33	**108.33**	50.00	**25.00**
TNR (%)	**Euclid.**	74.57		28.00		59.13		79.48		98.26		60.35	
	VFD	30.00	**-59.77**	31.43	**12.24**	30.43	**-48.53**	30.43	**-61.71**	28.70	**-70.80**	16.52	**-72.62**
	CFD	58.57	**-21.46**	68.57	**144.90**	23.48	**-60.29**	23.48	**-70.46**	7.83	**-92.04**	16.52	**-72.62**
	IFD	64.29	**-13.79**	78.57	**180.61**	21.74	**-63.24**	21.74	**-72.65**	7.83	**-92.04**	8.70	**-85.59**
FPR (%)	**Euclid.**	25.43		72.00		40.87		20.52		1.74		39.65	
	VFD	70.00	**-175.28**	68.57	**4.76**	69.57	**-70.21**	69.57	**-238.98**	71.30	**-4000.00**	83.48	**-110.53**
	CFD	41.43	**-62.92**	31.43	**56.35**	76.52	**-87.23**	76.52	**-272.88**	92.17	**-5200.00**	83.48	**-110.53**
	IFD	35.71	**-40.45**	21.43	**70.24**	78.26	**-91.49**	78.26	**-281.36**	92.17	**-5200.00**	91.30	**-130.26**
FNR (%)	**Euclid.**	77.25		34.12		60.00		80.00		100.00		60.00	
	VFD	3.92	**94.92**	0.00	**100.00**	33.33	**44.44**	33.33	**58.33**	66.67	**33.33**	33.33	**44.44**
	CFD	50.98	**34.01**	60.78	**-78.16**	50.00	**16.67**	50.00	**37.50**	16.67	**83.33**	50.00	**16.67**
	IFD	64.71	**16.24**	66.67	**-95.40**	66.67	**-11.11**	66.67	**16.67**	16.67	**83.33**	50.00	**16.67**
Prec. (%)	**Euclid.**	28.17		36.62		2.00		0.00		0.00		2.03	
	VFD	50.00	**77.46**	51.52	**40.69**	4.76	**138.10**	4.76	**476.00**	2.38	**1000.00**	4.00	**96.67**
	CFD	46.30	**64.32**	47.62	**30.05**	3.30	**64.84**	3.30	**330.00**	4.50	**864.00**	3.03	**48.99**
	IFD	41.86	**48.58**	53.13	**45.09**	2.17	**8.70**	2.17	**217.00**	4.50	**864.00**	2.78	**36.57**
Acc. (%)	**Euclid.**	52.73		43.97		58.18		76.53		93.39		59.34	
	VFD	57.85	**9.72**	60.33	**37.22**	32.23	**-44.60**	32.23	**-57.88**	28.93	**-69.03**	19.01	**-67.97**
	CFD	54.55	**3.45**	56.20	**27.82**	24.79	**-57.39**	24.79	**-67.60**	11.57	**-87.61**	18.18	**-69.36**
	IFD	52.07	**-1.25**	59.50	**35.34**	22.31	**-61.65**	22.31	**-70.84**	11.57	**-87.61**	10.74	**-81.89**
F1 (%)	**Euclid.**	20.09		42.94		3.81		1.92		0.00		3.87	
	VFD	65.77	**227.35**	68.00	**58.36**	8.89	**133.33**	8.89	**362.96**	4.44	**444.00**	7.55	**94.97**
	CFD	47.62	**137.00**	43.01	**0.17**	6.19	**62.37**	6.19	**222.16**	8.55	**855.00**	5.71	**47.62**
	IFD	38.30	**90.61**	40.96	**-4.60**	4.08	**7.14**	4.08	**112.59**	8.55	**855.00**	5.26	**35.96**

9) Carperb Malware – Instance 1

Table 44: Carperb Malware – Instance 1 - Malware vs. Normal sample ratio.

	Total	Carperb 01 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	250	3	10^0	149.0	51.0	98.0	34.2
			10^1	149.0	51.0	98.0	34.2
			10^2	149.0	51.0	98.0	34.2
			10^3	149.0	51.0	98.0	34.2
			10^4	146.0	51.0	95.0	34.9
			10^5	124.0	44.0	80.0	35.5
			10^6	96.0	31.0	65.0	32.3
			10^7	70.0	30.0	40.0	42.9
			10^8	27.0	17.0	10.0	63.0
			10^9	5.0	5.0	0.0	100.0
Edge	362	4	10^0	149.0	3.0	146.0	2.0
			10^1	149.0	3.0	146.0	2.0
			10^2	149.0	3.0	146.0	2.0
			10^3	149.0	3.0	146.0	2.0
			10^4	146.0	3.0	143.0	2.1
			10^5	124.0	2.0	122.0	1.6
			10^6	96.0	1.0	95.0	1.0
			10^7	70.0	1.0	69.0	1.4
			10^8	27.0	1.0	26.0	3.7
			10^9	5.0	1.0	4.0	20.0

Table 45: Carperb Malware – Instance 2 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Carperb 01 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	31.10435688	1.174738463	0.666443034	1
	10^1	1	1	1	1	31.10435688	1.174738463	0.666443034	1
	10^2	1	1	1	1	31.10435688	1.174738463	0.666443034	1
	10^3	1	1	1	1	31.10435688	1.174738463	0.666443034	1
	10^4	1	1	1	1	26.81568406	1.174604331	0.661693085	1
	10^5	1	1	1	1	23.14473729	1.129809376	0.500270647	1
	10^6	1	0	1	1	23.71730495	1.131081156	0.941424373	1
	10^7	1	0	1	1	14.57586984	NaN	-0.533322677	1
	10^8	1	0	0	1	5.855745163	NaN	0.538431344	1
	10^9	1	0	0	1	2.204708194	NaN	1.003964034	1
Edge	10^0	1	0	1	1	67.66493754	1.174738463	0.988677416	1
	10^1	1	0	1	1	67.66493754	1.174738463	0.988677416	1
	10^2	1	0	1	1	67.66493754	1.174738463	0.988677416	1
	10^3	1	0	1	1	67.66493754	1.174738463	0.988677416	1
	10^4	1	0	1	1	59.63776379	1.174604331	1.097992816	1
	10^5	1	1	1	1	41.97188399	1.129809376	0.216063605	1
	10^6	1	1	1	1	33.25703552	1.131081156	0.216063605	1
	10^7	1	1	1	1	16.15740468	NaN	0.286705367	1
	10^8	1	0	0	1	6.621627074	NaN	0.49742535	1
	10^9	1	0	0	1	1.702199644	NaN	1.935855879	1

Table 46: Carperb Malware – Instance 1 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.06	1.05	1.00	1.00	1.00	1.00	1.17	1.00	1.00	1.00	1.00	1.00	1.00
	Normal	1.11	1.11	1.17	1.17	1.10	1.12	1.13	1.10	1.13	1.13	1.13	1.16	1.17
	Delta Normal (%)	**4.6**	**4.9**	**13.9**	**13.9**	**9.1**	**10.1**	**-3.6**	**9.1**	**11.6**	**11.6**	**11.7**	**13.5**	**14.9**
CFD	Malware	0.11	0.10	0.00	0.00	0.00	0.00	1.13	0.00	1.00	1.00	1.00	0.00	0.00
	Normal	0.20	0.20	0.21	0.21	0.09	0.14	1.09	1.13	1.07	1.07	1.05	0.97	1.04
	Delta Normal (%)	**46.1**	**50.0**	**98.1**	**98.1**	**97.6**	**98.5**	**-3.8**	**100.0**	**6.8**	**6.8**	**4.5**	**100.0**	**100.0**
IFD	Malware	0.16	0.15	0.01	0.01	0.00	0.00	1.63	0.00	1.44	1.44	1.44	0.00	0.00
	Normal	0.29	0.30	0.32	0.32	0.13	0.20	1.57	1.63	1.55	1.55	1.52	1.41	1.50
	Delta Normal (%)	**46.3**	**49.9**	**98.1**	**98.1**	**97.6**	**98.5**	**-3.8**	**100.0**	**6.8**	**6.8**	**4.9**	**100.0**	**100.0**

Table 47: Carperb Malware – Instance 1 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	26.36		49.09		100.00		60.00		30.00		60.00	
	VFD	81.82	**210.34**	84.09	**71.30**	50.00	**-50.00**	50.00	**-16.67**	50.00	**-50.00**	50.00	**-16.67**
	CFD	59.09	**124.14**	63.64	**29.63**	100.00	**0.00**	100.00	**66.67**	100.00	**0.00**	50.00	**-16.67**
	IFD	18.18	**-31.03**	29.55	**-39.81**	100.00	**0.00**	100.00	**66.67**	100.00	**0.00**	100.00	**66.67**
TNR (%)	**Euclid.**	72.00		54.50		1.64		40.00		76.07		40.16	
	VFD	32.50	**-54.86**	32.50	**-40.37**	33.61	**1950.00**	33.61	**-15.98**	34.43	**-54.74**	18.03	**-55.10**
	CFD	28.75	**-60.07**	38.75	**-28.90**	12.30	**650.00**	12.30	**-69.26**	4.10	**-94.61**	10.66	**-73.47**
	IFD	66.25	**-7.99**	71.25	**30.73**	6.56	**300.00**	6.56	**-83.61**	3.28	**-95.69**	7.38	**-81.63**
FPR (%)	**Euclid.**	28.00		45.50		98.36		60.00		23.93		59.84	
	VFD	67.50	**-141.07**	67.50	**-48.35**	66.39	**32.50**	66.39	**-10.66**	65.57	**-173.97**	81.97	**-36.99**
	CFD	71.25	**-154.46**	61.25	**-34.62**	87.70	**10.83**	87.70	**-46.17**	95.90	**-300.68**	89.34	**-49.32**
	IFD	33.75	**-20.54**	28.75	**36.81**	93.44	**5.00**	93.44	**-55.74**	96.72	**-304.11**	92.62	**-54.79**
FNR (%)	**Euclid.**	73.64		50.91		0.00		40.00		70.00		40.00	
	VFD	18.18	**75.31**	15.91	**68.75**	50.00	**5000.00**	50.00	**-25.00**	50.00	**28.57**	50.00	**-25.00**
	CFD	40.91	**44.44**	36.36	**28.57**	0.00	**0.00**	0.00	**100.00**	0.00	**100.00**	50.00	**-25.00**
	IFD	81.82	**-11.11**	70.45	**-38.39**	0.00	**0.00**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**
Prec. (%)	**Euclid.**	35.29		37.88		1.64		0.98		1.28		0.98	
	VFD	40.00	**13.34**	40.66	**7.34**	1.22	**-25.61**	1.22	**24.32**	1.23	**-3.57**	0.99	**1.49**
	CFD	31.33	**-11.24**	36.36	**-4.00**	1.83	**11.92**	1.83	**87.05**	1.68	**31.28**	0.91	**-6.82**
	IFD	22.86	**-35.23**	36.11	**-4.67**	1.72	**5.17**	1.72	**75.76**	1.67	**30.18**	1.74	**78.26**
Acc. (%)	**Euclid.**	55.81		52.58		3.23		40.32		75.32		40.48	
	VFD	50.00	**-10.40**	50.81	**-3.37**	33.87	**950.00**	33.87	**-16.00**	34.68	**-53.96**	18.55	**-54.18**
	CFD	39.52	**-29.19**	47.58	**-9.51**	13.71	**325.00**	13.71	**-66.00**	5.65	**-92.51**	11.29	**-72.11**
	IFD	49.19	**-11.85**	56.45	**7.36**	8.06	**150.00**	8.06	**-80.00**	4.84	**-93.58**	8.87	**-78.09**
F1 (%)	**Euclid.**	22.00		36.18		3.23		1.93		2.38		1.92	
	VFD	53.73	**144.22**	54.81	**51.49**	2.38	**-26.19**	2.38	**23.34**	2.41	**1.06**	1.94	**1.13**
	CFD	40.94	**86.10**	46.28	**27.90**	3.60	**11.71**	3.60	**86.68**	3.31	**38.65**	1.79	**-6.99**
	IFD	20.25	**-7.95**	32.50	**-10.18**	3.39	**5.08**	3.39	**75.61**	3.28	**37.51**	3.42	**78.06**

10) Carperb Malware – Instance 2

Table 48: Carperb Malware – Instance 2 - Malware vs. Normal sample ratio.

	Total	Carperb 02 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	260	3	10^0	146.0	55.0	91.0	37.7
			10^1	146.0	55.0	91.0	37.7
			10^2	146.0	55.0	91.0	37.7
			10^3	144.0	55.0	89.0	38.2
			10^4	141.0	55.0	86.0	39.0
			10^5	112.0	51.0	61.0	45.5
			10^6	90.0	41.0	49.0	45.6
			10^7	59.0	34.0	25.0	57.6
			10^8	26.0	19.0	7.0	73.1
			10^9	6.0	6.0	0.0	100.0
Edge	371	4	10^0	146.0	3.0	143.0	2.1
			10^1	146.0	3.0	143.0	2.1
			10^2	146.0	3.0	143.0	2.1
			10^3	144.0	3.0	141.0	2.1
			10^4	141.0	3.0	138.0	2.1
			10^5	112.0	2.0	110.0	1.8
			10^6	90.0	1.0	89.0	1.1
			10^7	59.0	1.0	58.0	1.7
			10^8	26.0	1.0	25.0	3.8
			10^9	6.0	1.0	5.0	16.7

Table 49: Carperb Malware – Instance 2 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Carperb 02 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	36.46453741	1.174604331	0.666443034	1
	10^1	1	1	1	1	36.46453741	1.174604331	0.666443034	1
	10^2	1	1	1	1	36.46453741	1.174604331	0.666443034	1
	10^3	1	1	1	1	34.27618331	1.174564571	0.619807359	1
	10^4	1	1	1	1	29.69922397	1.174886897	0.619807359	1
	10^5	1	0	1	1	18.30861584	1.128785959	0.619807359	1
	10^6	1	1	1	1	21.75952934	1.218997094	1.001242479	1
	10^7	1	1	1	1	12.03160758	NaN	1.101178897	1
	10^8	1	0	1	1	4.423435946	NaN	1.031788915	1
	10^9	1	0	0	1	1.322864773	NaN	2.371003334	1
Edge	10^0	1	1	1	1	58.78656026	1.174604331	0.611658638	1
	10^1	1	1	1	1	58.78656026	1.174604331	0.611658638	1
	10^2	1	1	1	1	58.78656026	1.174604331	0.611658638	1
	10^3	1	1	1	1	56.4943552	1.174564571	0.611658638	1
	10^4	1	1	1	1	50.85101969	1.174886897	1.025460549	1
	10^5	1	1	1	1	28.77877438	1.128785959	0.666443034	1
	10^6	1	1	1	1	25.21672066	1.218997094	0.92850745	1
	10^7	1	1	1	1	13.96268282	NaN	1.138970676	1
	10^8	1	0	1	1	4.526872874	NaN	1.11933329	1
	10^9	1	0	0	1	1.118915146	NaN	2.403931024	1

Table 50: Carperb Malware – Instance 2 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.05	1.05	1.00	1.00	1.00	1.00	1.17	1.00	1.00	1.00	1.00	1.00	1.00
	Normal	1.11	1.11	1.16	1.16	1.11	1.12	1.22	1.14	1.13	1.13	1.13	1.15	1.17
	Delta Normal (%)	**5.2**	**5.2**	**13.5**	**13.5**	**9.3**	**10.2**	**3.7**	**12.2**	**11.7**	**11.7**	**11.7**	**12.9**	**14.9**
CFD	Malware	0.10	0.09	0.00	0.00	0.00	0.00	1.16	0.00	1.00	1.00	1.00	0.00	0.00
	Normal	0.17	0.17	0.21	0.21	0.09	0.13	1.11	1.00	1.08	1.08	1.05	0.98	1.03
	Delta Normal (%)	**44.5**	**45.6**	**98.1**	**98.1**	**97.6**	**98.2**	**-4.4**	**100.0**	**7.3**	**7.3**	**4.5**	**100.0**	**100.0**
IFD	Malware	0.14	0.14	0.01	0.01	0.00	0.00	1.68	0.00	1.44	1.44	1.44	0.00	0.00
	Normal	0.26	0.26	0.32	0.32	0.13	0.19	1.61	1.44	1.56	1.56	1.52	1.42	1.48
	Delta Normal (%)	**44.5**	**46.1**	**98.0**	**98.0**	**97.6**	**98.2**	**-4.4**	**100.0**	**7.3**	**7.3**	**5.0**	**100.0**	**100.0**

Table 51: Carperb Malware – Instance 2 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	40.00		36.08		20.00		40.00		40.00		80.00	
	VFD	88.24	**120.59**	82.35	**128.26**	100.00	**400.00**	100.00	**150.00**	50.00	**150.00**	100.00	**25.00**
	CFD	72.55	**81.37**	72.55	**101.09**	0.00	**-100.00**	0.00	**-100.00**	100.00	**400.00**	0.00	**-100.00**
	IFD	68.63	**71.57**	68.63	**90.22**	0.00	**-100.00**	0.00	**-100.00**	50.00	**150.00**	0.00	**-100.00**
TNR (%)	**Euclid.**	54.75		64.26		78.73		59.09		59.64		20.55	
	VFD	47.54	**-13.17**	40.98	**-36.22**	27.27	**-65.36**	27.27	**-53.85**	36.36	**-39.02**	23.64	**15.04**
	CFD	45.90	**-16.17**	45.90	**-28.57**	27.27	**-65.36**	27.27	**-53.85**	7.27	**-87.80**	50.91	**147.79**
	IFD	47.54	**-13.17**	47.54	**-26.02**	69.09	**-12.24**	69.09	**16.92**	11.82	**-80.18**	49.09	**138.94**
FPR (%)	**Euclid.**	45.25		35.74		21.27		40.91		40.36		79.45	
	VFD	52.46	**-15.94**	59.02	**-65.14**	72.73	**-241.88**	72.73	**-77.78**	63.64	**-57.66**	76.36	**3.89**
	CFD	54.10	**-19.57**	54.10	**-51.38**	72.73	**-241.88**	72.73	**-77.78**	92.73	**-129.73**	49.09	**38.22**
	IFD	52.46	**-15.94**	52.46	**-46.79**	30.91	**-45.30**	30.91	**24.44**	88.18	**-118.47**	50.91	**35.93**
FNR (%)	**Euclid.**	60.00		63.92		80.00		60.00		60.00		20.00	
	VFD	11.76	**80.39**	17.65	**72.39**	0.00	**100.00**	0.00	**100.00**	50.00	**16.67**	0.00	**100.00**
	CFD	27.45	**54.25**	27.45	**57.06**	100.00	**-25.00**	100.00	**-66.67**	0.00	**100.00**	100.00	**-400.00**
	IFD	31.37	**47.71**	31.37	**50.92**	100.00	**-25.00**	100.00	**-66.67**	50.00	**16.67**	100.00	**-400.00**
Prec. (%)	**Euclid.**	25.28		30.57		0.36		0.73		0.73		1.44	
	VFD	58.44	**131.22**	53.85	**76.14**	2.44	**576.83**	2.44	**235.37**	1.41	**92.78**	2.33	**61.34**
	CFD	52.86	**109.12**	52.86	**72.90**	0.00	**-100.00**	0.00	**-100.00**	1.92	**163.22**	0.00	**-100.00**
	IFD	52.24	**106.68**	52.24	**70.88**	0.00	**-100.00**	0.00	**-100.00**	1.02	**39.67**	0.00	**-100.00**
Acc. (%)	**Euclid.**	48.04		51.43		77.68		58.75		59.29		21.61	
	VFD	66.07	**37.55**	59.82	**16.32**	28.57	**-63.22**	28.57	**-51.37**	36.61	**-38.25**	25.00	**15.70**
	CFD	58.04	**20.82**	58.04	**12.85**	26.79	**-65.52**	26.79	**-54.41**	8.93	**-84.94**	50.00	**131.40**
	IFD	57.14	**18.96**	57.14	**11.11**	67.86	**-12.64**	67.86	**15.50**	12.50	**-78.92**	48.21	**123.14**
F1 (%)	**Euclid.**	28.88		26.31		0.71		1.43		1.44		2.83	
	VFD	70.31	**143.43**	65.12	**147.47**	4.76	**572.62**	4.76	**233.33**	2.74	**90.92**	4.55	**60.51**
	CFD	61.16	**111.74**	61.16	**132.42**	0.00	**-100.00**	0.00	**-100.00**	3.77	**162.97**	0.00	**-100.00**
	IFD	59.32	**105.38**	59.32	**125.45**	0.00	**-100.00**	0.00	**-100.00**	2.00	**39.37**	0.00	**-100.00**

11) Alina Malware – Instance 1

Table 52: Alina Malware – Instance 1 - Malware vs. Normal sample ratio.

	Total	Alina 01 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	401	8	10^0	259.0	88.0	171.0	34.0
			10^1	259.0	88.0	171.0	34.0
			10^2	259.0	88.0	171.0	34.0
			10^3	259.0	88.0	171.0	34.0
			10^4	254.0	85.0	169.0	33.5
			10^5	190.0	74.0	116.0	38.9
			10^6	132.0	59.0	73.0	44.7
			10^7	76.0	46.0	30.0	60.5
			10^8	31.0	25.0	6.0	80.6
			10^9	6.0	6.0	0.0	100.0
Edge	670	14	10^0	259.0	12.0	247.0	4.6
			10^1	259.0	12.0	247.0	4.6
			10^2	259.0	12.0	247.0	4.6
			10^3	259.0	12.0	247.0	4.6
			10^4	254.0	12.0	242.0	4.7
			10^5	190.0	8.0	182.0	4.2
			10^6	132.0	8.0	124.0	6.1
			10^7	76.0	6.0	70.0	7.9
			10^8	31.0	3.0	28.0	9.7
			10^9	6.0	3.0	3.0	50.0

Table 53: Alina Malware – Instance 1 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Alina 01 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	19.90468671	1.139206945	0.588321389	1
	10^1	1	1	1	1	19.90468671	1.139206945	0.588321389	1
	10^2	1	1	1	1	19.90468671	1.139206945	0.588321389	1
	10^3	1	1	1	1	19.90468671	1.139206945	0.588321389	1
	10^4	1	1	1	1	18.83752475	1.100512716	0.588321389	1
	10^5	1	1	1	1	15.24396674	1.167706943	0.744100239	1
	10^6	1	1	1	1	13.43440096	1.174323837	0.533160797	1
	10^7	1	1	1	1	10.10630353	NaN	0.284687026	1
	10^8	1	0	1	1	7.913427308	NaN	0.396986286	1
	10^9	1	0	0	1	1.05476471	NaN	0.74268847	1
Edge	10^0	1	1	1	1	30.77228214	1.139206945	1.022719896	1
	10^1	1	1	1	1	30.77228214	1.139206945	1.022719896	1
	10^2	1	1	1	1	30.77228214	1.139206945	1.022719896	1
	10^3	1	1	1	1	30.77228214	1.139206945	1.022719896	1
	10^4	1	1	1	1	28.78144891	1.100512716	1.022719896	1
	10^5	1	1	1	1	17.84771196	1.167706943	0.936666661	1
	10^6	1	1	1	1	15.21784098	1.174323837	0.074597142	1
	10^7	1	1	1	1	11.09905976	NaN	0.274098101	1
	10^8	1	0	1	1	8.161343512	NaN	1.199452697	1
	10^9	1	0	0	1	1.025274586	NaN	0.713398649	1

Table 54: Alina Malware – Instance 1 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.03	1.03	1.01	1.01	1.00	1.00	1.22	1.58	1.36	1.36	1.36	1.35	1.32
	Normal	1.09	1.09	1.15	1.15	1.09	1.10	1.17	1.08	1.11	1.11	1.11	1.11	1.10
	Delta Normal (%)	**5.5**	**5.4**	**12.7**	**12.7**	**7.4**	**8.8**	**-4.4**	**-46.3**	**-23.1**	**-23.1**	**-23.0**	**-21.6**	**-20.1**
CFD	Malware	0.08	0.08	0.01	0.01	0.00	0.00	1.11	1.00	1.40	1.40	1.40	1.22	1.29
	Normal	0.18	0.18	0.19	0.19	0.08	0.11	1.07	1.05	1.04	1.04	1.02	0.96	1.13
	Delta Normal (%)	**53.2**	**55.3**	**95.0**	**95.0**	**95.0**	**96.1**	**-3.2**	**5.1**	**-34.6**	**-34.6**	**-38.2**	**-27.4**	**-14.5**
IFD	Malware	0.12	0.12	0.01	0.01	0.01	0.01	1.60	1.44	2.03	2.03	2.03	1.82	1.86
	Normal	0.26	0.27	0.28	0.28	0.12	0.17	1.55	1.52	1.51	1.51	1.47	1.39	1.63
	Delta Normal (%)	**53.8**	**55.8**	**95.1**	**95.1**	**95.1**	**96.1**	**-3.2**	**5.1**	**-34.5**	**-34.5**	**-37.4**	**-30.5**	**-14.5**

Table 55: Alina Malware – Instance 1 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	23.24		15.14		20.00		80.00		40.00		80.00	
	VFD	90.54	**289.53**	89.19	**489.29**	75.00	**275.00**	75.00	**-6.25**	62.50	**212.50**	87.50	**9.38**
	CFD	64.86	**179.07**	66.22	**337.50**	50.00	**150.00**	50.00	**-37.50**	100.00	**400.00**	75.00	**-6.25**
	IFD	25.68	**10.47**	33.78	**123.21**	50.00	**150.00**	50.00	**-37.50**	87.50	**337.50**	75.00	**-6.25**
TNR (%)	**Euclid.**	75.52		85.00		79.34		20.33		60.11		20.33	
	VFD	25.86	**-65.75**	24.14	**-71.60**	36.81	**-53.60**	36.81	**81.08**	19.78	**-67.09**	22.53	**10.81**
	CFD	49.14	**-34.93**	50.86	**-40.16**	18.13	**-77.15**	18.13	**-10.81**	8.79	**-85.37**	18.13	**-10.81**
	IFD	81.03	**7.31**	87.07	**2.43**	20.88	**-73.68**	20.88	**2.70**	9.89	**-83.55**	19.78	**-2.70**
FPR (%)	**Euclid.**	24.48		15.00		20.66		79.67		39.89		79.67	
	VFD	74.14	**-202.82**	75.86	**-405.75**	63.19	**-205.85**	63.19	**20.69**	80.22	**-101.10**	77.47	**2.76**
	CFD	50.86	**-107.75**	49.14	**-227.59**	81.87	**-296.28**	81.87	**-2.76**	91.21	**-128.65**	81.87	**-2.76**
	IFD	18.97	**22.54**	12.93	**13.79**	79.12	**-282.98**	79.12	**0.69**	90.11	**-125.90**	80.22	**-0.69**
FNR (%)	**Euclid.**	76.76		84.86		80.00		20.00		60.00		20.00	
	VFD	9.46	**87.68**	10.81	**87.26**	25.00	**68.75**	25.00	**-25.00**	37.50	**37.50**	12.50	**37.50**
	CFD	35.14	**54.23**	33.78	**60.19**	50.00	**37.50**	50.00	**-150.00**	0.00	**100.00**	25.00	**-25.00**
	IFD	74.32	**3.17**	66.22	**21.97**	50.00	**37.50**	50.00	**-150.00**	12.50	**79.17**	25.00	**-25.00**
Prec. (%)	**Euclid.**	32.52		35.99		0.85		3.40		1.71		3.39	
	VFD	43.79	**34.65**	42.86	**19.08**	4.96	**485.74**	4.96	**46.05**	3.31	**94.02**	4.73	**39.67**
	CFD	44.86	**37.94**	46.23	**28.44**	2.61	**208.82**	2.61	**-23.00**	4.60	**169.39**	3.87	**14.31**
	IFD	46.34	**42.50**	62.50	**73.66**	2.70	**219.26**	2.70	**-20.40**	4.09	**139.86**	3.95	**16.57**
Acc. (%)	**Euclid.**	55.16		57.79		76.84		22.84		59.26		22.84	
	VFD	51.05	**-7.44**	49.47	**-14.39**	38.42	**-50.00**	38.42	**68.20**	21.58	**-63.59**	25.26	**10.60**
	CFD	55.26	**0.19**	56.84	**-1.64**	19.47	**-74.66**	19.47	**-14.75**	12.63	**-78.69**	20.53	**-10.14**
	IFD	59.47	**7.82**	66.32	**14.75**	22.11	**-71.23**	22.11	**-3.23**	13.16	**-77.80**	22.11	**-3.23**
F1 (%)	**Euclid.**	18.12		18.82		1.62		6.51		3.27		6.50	
	VFD	59.03	**225.81**	57.89	**207.65**	9.30	**472.67**	9.30	**42.80**	6.29	**92.12**	8.97	**38.12**
	CFD	53.04	**192.74**	54.44	**189.32**	4.97	**205.90**	4.97	**-23.72**	8.79	**168.54**	7.36	**13.31**
	IFD	33.04	**82.38**	43.86	**133.07**	5.13	**215.71**	5.13	**-21.27**	7.82	**138.91**	7.50	**15.43**

12) Alina Malware – Instance 2

Table 56: Alina Malware – Instance 2 - Malware vs. Normal sample ratio.

	Total	Alina 02 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	446	8	10^0	294.0	123.0	171.0	41.8
			10^1	294.0	123.0	171.0	41.8
			10^2	294.0	123.0	171.0	41.8
			10^3	294.0	123.0	171.0	41.8
			10^4	290.0	120.0	170.0	41.4
			10^5	211.0	104.0	107.0	49.3
			10^6	156.0	87.0	69.0	55.8
			10^7	98.0	72.0	26.0	73.5
			10^8	39.0	32.0	7.0	82.1
			10^9	8.0	7.0	1.0	87.5
Edge	741	14	10^0	294.0	12.0	282.0	4.1
			10^1	294.0	12.0	282.0	4.1
			10^2	294.0	12.0	282.0	4.1
			10^3	294.0	12.0	282.0	4.1
			10^4	290.0	12.0	278.0	4.1
			10^5	211.0	8.0	203.0	3.8
			10^6	156.0	8.0	148.0	5.1
			10^7	98.0	7.0	91.0	7.1
			10^8	39.0	4.0	35.0	10.3
			10^9	8.0	3.0	5.0	37.5

Table 57: Alina Malware – Instance 2 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Alina 02 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	12.47858844	1.138929127	0.61081538	1
	10^1	1	1	1	1	12.47858844	1.138929127	0.61081538	1
	10^2	1	1	1	1	12.47858844	1.138929127	0.61081538	1
	10^3	1	1	1	1	12.47858844	1.138929127	0.61081538	1
	10^4	1	1	1	1	11.68161289	1.138894642	0.61081538	1
	10^5	1	1	1	1	12.00753026	1.103421065	0.405862638	1
	10^6	1	1	1	1	17.09680064	1.175186642	0.565886947	1
	10^7	1	1	1	1	14.19289222	1.131206418	0.68128924	1
	10^8	1	1	1	1	10.55252629	NaN	1.063490226	1
	10^9	1	0	0	1	2.154365211	NaN	2.242924296	1
Edge	10^0	1	1	1	1	23.84101518	1.138929127	0.843976621	1
	10^1	1	1	1	1	23.84101518	1.138929127	0.843976621	1
	10^2	1	1	1	1	23.84101518	1.138929127	0.843976621	1
	10^3	1	1	1	1	23.84101518	1.138929127	0.843976621	1
	10^4	1	1	1	1	21.68756505	1.138894642	0.843976621	1
	10^5	1	1	1	1	14.6149391	1.103421065	0.625249798	1
	10^6	1	1	1	1	21.93864363	1.175186642	0.43354805	1
	10^7	1	1	1	1	15.85177417	1.131206418	0.642464072	1
	10^8	1	1	1	1	10.77726814	NaN	0.653959009	1
	10^9	1	0	0	1	2.085422926	NaN	2.214741456	1

Table 58: Alina Malware – Instance 2 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.05	1.05	1.01	1.01	1.00	1.00	1.13	1.58	1.36	1.36	1.36	1.35	1.32
	Normal	1.09	1.08	1.14	1.14	1.09	1.09	1.17	1.08	1.11	1.11	1.11	1.13	1.14
	Delta Normal (%)	**2.9**	**2.8**	**11.8**	**11.8**	**7.9**	**7.6**	**3.2**	**-46.4**	**-23.1**	**-23.1**	**-23.1**	**-19.8**	**-16.0**
CFD	Malware	0.11	0.11	0.01	0.01	0.00	0.00	1.16	1.00	1.40	1.40	1.40	1.22	1.29
	Normal	0.16	0.16	0.18	0.18	0.08	0.11	1.07	1.08	1.06	1.06	1.04	0.99	1.02
	Delta Normal (%)	**29.5**	**31.5**	**95.4**	**95.4**	**95.9**	**95.6**	**-8.3**	**7.6**	**-31.9**	**-31.9**	**-35.5**	**-23.0**	**-26.1**
IFD	Malware	0.17	0.16	0.01	0.01	0.00	0.01	1.68	1.44	2.03	2.03	2.03	1.82	1.86
	Normal	0.24	0.24	0.27	0.27	0.12	0.15	1.55	1.56	1.54	1.54	1.50	1.44	1.48
	Delta Normal (%)	**29.9**	**32.2**	**95.4**	**95.4**	**96.0**	**95.6**	**-8.3**	**7.6**	**-31.8**	**-31.8**	**-34.6**	**-26.7**	**-26.1**

Table 59: Alina Malware – Instance 2 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	35.38		66.54		40.00		22.50		60.00		40.00	
	VFD	81.73	**130.98**	80.77	**21.39**	50.00	**25.00**	50.00	**122.22**	50.00	**25.00**	75.00	**87.50**
	CFD	60.58	**71.20**	61.54	**-7.51**	37.50	**-6.25**	37.50	**66.67**	100.00	**150.00**	75.00	**87.50**
	IFD	49.04	**38.59**	54.81	**-17.63**	50.00	**25.00**	50.00	**122.22**	87.50	**118.75**	62.50	**56.25**
TNR (%)	**Euclid.**	62.43		36.07		60.00		79.51		40.10		59.90	
	VFD	30.84	**-50.60**	28.97	**-19.69**	36.45	**-39.24**	36.45	**-54.15**	21.67	**-45.95**	29.06	**-51.48**
	CFD	52.34	**-16.17**	54.21	**50.26**	25.12	**-58.13**	25.12	**-68.40**	9.36	**-76.66**	20.69	**-65.46**
	IFD	59.81	**-4.19**	66.36	**83.94**	22.66	**-62.23**	22.66	**-71.50**	10.34	**-74.20**	27.09	**-54.77**
FPR (%)	**Euclid.**	37.57		63.93		40.00		20.49		59.90		40.10	
	VFD	69.16	**-84.08**	71.03	**-11.11**	63.55	**-58.87**	63.55	**-210.10**	78.33	**-30.76**	70.94	**-76.90**
	CFD	47.66	**-26.87**	45.79	**28.36**	74.88	**-87.19**	74.88	**-265.38**	90.64	**-51.32**	79.31	**-97.79**
	IFD	40.19	**-6.97**	33.64	**47.37**	77.34	**-93.35**	77.34	**-277.40**	89.66	**-49.67**	72.91	**-81.82**
FNR (%)	**Euclid.**	64.62		33.46		60.00		77.50		40.00		60.00	
	VFD	18.27	**71.73**	19.23	**42.53**	50.00	**16.67**	50.00	**35.48**	50.00	**-25.00**	25.00	**58.33**
	CFD	39.42	**38.99**	38.46	**-14.94**	62.50	**-4.17**	62.50	**19.35**	0.00	**100.00**	25.00	**58.33**
	IFD	50.96	**21.13**	45.19	**-35.06**	50.00	**16.67**	50.00	**35.48**	12.50	**68.75**	37.50	**37.50**
Prec. (%)	**Euclid.**	35.95		50.22		1.53		7.44		2.29		1.52	
	VFD	53.46	**48.71**	52.50	**4.54**	3.01	**96.90**	3.01	**-59.55**	2.45	**7.02**	4.00	**162.50**
	CFD	55.26	**53.73**	56.64	**12.78**	1.94	**26.71**	1.94	**-73.97**	4.17	**81.71**	3.59	**135.78**
	IFD	54.26	**50.93**	61.29	**22.04**	2.48	**62.65**	2.48	**-66.59**	3.70	**61.52**	3.27	**114.46**
Acc. (%)	**Euclid.**	49.10		51.09		59.24		77.35		40.85		59.15	
	VFD	55.92	**13.90**	54.50	**6.68**	36.97	**-37.60**	36.97	**-52.21**	22.75	**-44.32**	30.81	**-47.92**
	CFD	56.40	**14.86**	57.82	**13.17**	25.59	**-56.80**	25.59	**-66.91**	12.80	**-68.68**	22.75	**-61.54**
	IFD	54.50	**11.00**	60.66	**18.74**	23.70	**-60.00**	23.70	**-69.36**	13.27	**-67.52**	28.44	**-51.92**
F1 (%)	**Euclid.**	31.33		49.93		2.94		5.12		4.42		2.94	
	VFD	64.64	**106.34**	63.64	**27.45**	5.67	**92.82**	5.67	**10.86**	4.68	**5.91**	7.59	**158.70**
	CFD	57.80	**84.50**	58.99	**18.14**	3.68	**25.10**	3.68	**-28.08**	8.00	**81.11**	6.86	**133.57**
	IFD	51.52	**64.45**	57.87	**15.90**	4.73	**60.87**	4.73	**-7.51**	7.11	**60.88**	6.21	**111.57**

13) Proteus Malware – Instance 1

Table 60: Proteus Malware – Instance 1 - Malware vs. Normal sample ratio.

	Total	Proteus 01 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	254	5	10^0	148.0	73.0	75.0	49.3
			10^1	148.0	73.0	75.0	49.3
			10^2	148.0	73.0	75.0	49.3
			10^3	148.0	73.0	75.0	49.3
			10^4	146.0	73.0	73.0	50.0
			10^5	115.0	66.0	49.0	57.4
			10^6	85.0	50.0	35.0	58.8
			10^7	65.0	43.0	22.0	66.2
			10^8	27.0	21.0	6.0	77.8
			10^9	6.0	6.0	0.0	100.0
Edge	372	8	10^0	148.0	6.0	142.0	4.1
			10^1	148.0	6.0	142.0	4.1
			10^2	148.0	6.0	142.0	4.1
			10^3	148.0	6.0	142.0	4.1
			10^4	146.0	6.0	140.0	4.1
			10^5	115.0	4.0	111.0	3.5
			10^6	85.0	4.0	81.0	4.7
			10^7	65.0	4.0	61.0	6.2
			10^8	27.0	1.0	26.0	3.7
			10^9	6.0	1.0	5.0	16.7

Table 61: Proteus Malware – Instance 1 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Proteus 01 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	7.933661773	1.174738463	0.666443034	1
	10^1	1	1	1	1	7.933661773	1.174738463	0.666443034	1
	10^2	1	1	1	1	7.933661773	1.174738463	0.666443034	1
	10^3	1	1	1	1	7.933661773	1.174738463	0.666443034	1
	10^4	1	1	1	1	7.386969356	1.174604331	0.666443034	1
	10^5	1	1	1	1	5.9290833	1.128877982	0.80410801	1
	10^6	1	1	1	1	7.936161457	1.218200793	0.473768762	1
	10^7	1	1	1	1	12.95787407	NaN	0.287907386	1
	10^8	1	0	1	1	5.021015717	NaN	1.311819822	1
	10^9	1	0	0	1	3.250340347	NaN	1.207483071	1
Edge	10^0	1	1	1	1	23.11719303	1.174738463	0.988677416	1
	10^1	1	1	1	1	23.11719303	1.174738463	0.988677416	1
	10^2	1	1	1	1	23.11719303	1.174738463	0.988677416	1
	10^3	1	1	1	1	23.11719303	1.174738463	0.988677416	1
	10^4	1	1	1	1	21.19139384	1.174604331	0.988677416	1
	10^5	1	1	1	1	10.61372989	1.128877982	1.073814062	1
	10^6	1	1	1	1	8.362975784	1.218200793	0.661693085	1
	10^7	1	1	1	1	16.07587746	NaN	1.03841844	1
	10^8	1	0	1	1	5.101530195	NaN	1.455518884	1
	10^9	1	0	0	1	2.930098581	NaN	1.236589008	1

Table 62: Proteus Malware – Instance 1 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.07	1.06	1.01	1.01	1.00	1.00	1.23	1.00	1.58	1.58	1.58	1.32	1.00
	Normal	1.09	1.09	1.17	1.17	1.11	1.11	1.23	1.10	1.13	1.13	1.13	1.15	1.17
	Delta Normal (%)	**2.1**	**2.7**	**14.3**	**14.3**	**9.6**	**9.9**	**0.0**	**9.1**	**-40.0**	**-40.0**	**-39.9**	**-14.7**	**14.9**
CFD	Malware	0.15	0.14	0.01	0.01	0.00	0.01	1.04	1.00	1.00	1.00	1.00	0.71	1.58
	Normal	0.16	0.16	0.22	0.22	0.09	0.13	1.05	1.13	1.08	1.08	1.05	0.99	1.03
	Delta Normal (%)	**4.2**	**12.4**	**96.3**	**96.3**	**97.2**	**95.9**	**0.5**	**11.7**	**7.2**	**7.2**	**4.9**	**28.3**	**-54.1**
IFD	Malware	0.22	0.21	0.01	0.01	0.00	0.01	1.51	1.44	1.44	1.44	1.44	1.08	2.29
	Normal	0.23	0.24	0.32	0.32	0.14	0.20	1.51	1.63	1.56	1.56	1.53	1.43	1.48
	Delta Normal (%)	**4.0**	**13.1**	**96.3**	**96.3**	**97.2**	**95.9**	**0.5**	**11.7**	**7.2**	**7.2**	**5.5**	**24.4**	**-54.1**

Table 63: Proteus Malware – Instance 1 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	52.73		31.82		20.00		40.00		60.00		40.00	
	VFD	89.39	**69.54**	89.39	**180.95**	100.00	**400.00**	100.00	**150.00**	100.00	**400.00**	100.00	**150.00**
	CFD	43.94	**-16.67**	50.00	**57.14**	100.00	**400.00**	100.00	**150.00**	100.00	**400.00**	50.00	**25.00**
	IFD	48.48	**-8.05**	53.03	**66.67**	100.00	**400.00**	100.00	**150.00**	100.00	**400.00**	75.00	**87.50**
TNR (%)	**Euclid.**	42.86		63.27		78.92		59.10		40.18		59.82	
	VFD	46.94	**9.52**	46.94	**-25.81**	38.74	**-50.91**	38.74	**-34.45**	19.82	**-50.67**	23.42	**-60.84**
	CFD	57.14	**33.33**	65.31	**3.23**	43.24	**-45.21**	43.24	**-26.83**	10.81	**-73.09**	22.52	**-62.35**
	IFD	59.18	**38.10**	65.31	**3.23**	52.25	**-33.79**	52.25	**-11.59**	11.71	**-70.85**	13.51	**-77.41**
FPR (%)	**Euclid.**	57.14		36.73		21.08		40.90		59.82		40.18	
	VFD	53.06	**7.14**	53.06	**-44.44**	61.26	**-190.60**	61.26	**-49.78**	80.18	**-34.04**	76.58	**-90.58**
	CFD	42.86	**25.00**	34.69	**5.56**	56.76	**-169.23**	56.76	**-38.77**	89.19	**-49.10**	77.48	**-92.83**
	IFD	40.82	**28.57**	34.69	**5.56**	47.75	**-126.50**	47.75	**-16.74**	88.29	**-47.59**	86.49	**-115.25**
FNR (%)	**Euclid.**	47.27		68.18		80.00		60.00		40.00		60.00	
	VFD	10.61	**77.56**	10.61	**84.44**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**
	CFD	56.06	**-18.59**	50.00	**26.67**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**	50.00	**16.67**
	IFD	51.52	**-8.97**	46.97	**31.11**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**	25.00	**58.33**
Prec. (%)	**Euclid.**	54.28		43.91		0.71		1.42		2.12		1.40	
	VFD	69.41	**27.87**	69.41	**58.07**	5.56	**684.72**	5.56	**292.36**	4.30	**102.51**	4.49	**220.22**
	CFD	58.00	**6.85**	66.00	**50.30**	5.97	**743.28**	5.97	**321.64**	3.88	**82.85**	2.27	**61.93**
	IFD	61.54	**13.37**	67.31	**53.28**	7.02	**891.23**	7.02	**395.61**	3.92	**84.64**	3.03	**115.91**
Acc. (%)	**Euclid.**	48.52		45.22		76.87		58.43		40.87		59.13	
	VFD	71.30	**46.95**	71.30	**57.69**	40.87	**-46.83**	40.87	**-30.06**	22.61	**-44.68**	26.09	**-55.88**
	CFD	49.57	**2.15**	56.52	**25.00**	45.22	**-41.18**	45.22	**-22.62**	13.91	**-65.96**	23.48	**-60.29**
	IFD	53.04	**9.32**	58.26	**28.85**	53.91	**-29.86**	53.91	**-7.74**	14.78	**-63.83**	15.65	**-73.53**
F1 (%)	**Euclid.**	48.56		28.65		1.37		2.74		4.10		2.71	
	VFD	78.15	**60.93**	78.15	**172.77**	10.53	**669.74**	10.53	**284.87**	8.25	**101.03**	8.60	**217.20**
	CFD	50.00	**2.97**	56.90	**98.60**	11.27	**723.94**	11.27	**311.97**	7.48	**82.24**	4.35	**60.33**
	IFD	54.24	**11.69**	59.32	**107.06**	13.11	**859.02**	13.11	**379.51**	7.55	**83.96**	5.83	**114.81**

14) Proteus Malware – Instance 2

Table 64: Proteus Malware – Instance 2 - Malware vs. Normal sample ratio.

	Total	Proteus 02 Malware	Timestamp Resolution (micro-sec)	Total Timestamps (count)	Malware Timestamps (count)	Normal Timestamps (count)	Malware Ratio (%)
Node	262	8	10^0	146.0	63.0	83.0	43.2
			10^1	146.0	63.0	83.0	43.2
			10^2	146.0	63.0	83.0	43.2
			10^3	146.0	63.0	83.0	43.2
			10^4	143.0	62.0	81.0	43.4
			10^5	106.0	52.0	54.0	49.1
			10^6	84.0	42.0	42.0	50.0
			10^7	58.0	33.0	25.0	56.9
			10^8	23.0	15.0	8.0	65.2
			10^9	5.0	5.0	0.0	100.0
Edge	386	14	10^0	146.0	10.0	136.0	6.8
			10^1	146.0	10.0	136.0	6.8
			10^2	146.0	10.0	136.0	6.8
			10^3	146.0	10.0	136.0	6.8
			10^4	143.0	10.0	133.0	7.0
			10^5	106.0	10.0	96.0	9.4
			10^6	84.0	9.0	75.0	10.7
			10^7	58.0	9.0	49.0	15.5
			10^8	23.0	4.0	19.0	17.4
			10^9	5.0	3.0	2.0	60.0

Table 65: Proteus Malware – Instance 2 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Proteus 02 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	6.123138026	1.174604331	0.548383564	1
	10^1	1	1	1	1	6.123138026	1.174604331	0.548383564	1
	10^2	1	1	1	1	6.123138026	1.174604331	0.548383564	1
	10^3	1	1	1	1	6.123138026	1.174604331	0.548383564	1
	10^4	1	1	1	1	5.748451512	1.174928963	0.548383564	1
	10^5	1	1	1	1	7.724345295	1.132141441	0.800725925	1
	10^6	1	1	1	1	9.590740713	1.218200793	0.717197644	1
	10^7	1	1	1	1	20.46259241	NaN	0.673961703	1
	10^8	1	0	1	1	12.37525667	NaN	1.097322593	1
	10^9	1	0	0	1	2.101017503	NaN	1.794649922	1
Edge	10^0	1	1	1	1	12.59100866	1.174604331	0.661693085	1
	10^1	1	1	1	1	12.59100866	1.174604331	0.661693085	1
	10^2	1	1	1	1	12.59100866	1.174604331	0.661693085	1
	10^3	1	1	1	1	12.59100866	1.174604331	0.661693085	1
	10^4	1	1	1	1	11.40767062	1.174928963	0.661693085	1
	10^5	1	1	1	1	9.118770904	1.132141441	0.608381046	1
	10^6	1	1	1	1	11.33819288	1.218200793	0.558335781	1
	10^7	1	0	1	1	23.13719754	NaN	0.544211986	1
	10^8	1	0	1	1	12.71780794	NaN	1.294167043	1
	10^9	1	0	0	1	1.927698641	NaN	1.804859375	1

Table 66: Proteus Malware – Instance 2 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.06	1.06	1.01	1.01	1.01	1.01	1.17	1.58	1.36	1.36	1.36	1.28	1.68
	Normal	1.11	1.11	1.14	1.14	1.11	1.08	1.22	1.10	1.13	1.13	1.13	1.15	1.17
	Delta Normal (%)	**4.8**	**4.6**	**11.0**	**11.0**	**8.8**	**6.4**	**3.6**	**-44.0**	**-20.4**	**-20.4**	**-20.4**	**-11.4**	**-42.9**
CFD	Malware	0.11	0.11	0.01	0.01	0.01	0.01	1.22	1.00	1.40	1.40	1.40	1.08	1.16
	Normal	0.15	0.15	0.19	0.19	0.09	0.11	1.08	1.14	1.08	1.08	1.05	0.99	1.02
	Delta Normal (%)	**30.0**	**29.7**	**92.0**	**92.0**	**91.8**	**91.2**	**-13.4**	**12.2**	**-29.5**	**-29.5**	**-33.1**	**-8.6**	**-14.0**
IFD	Malware	0.16	0.16	0.02	0.02	0.01	0.01	1.76	1.44	2.03	2.03	2.03	1.61	1.67
	Normal	0.23	0.23	0.28	0.28	0.14	0.16	1.56	1.64	1.56	1.56	1.53	1.44	1.47
	Delta Normal (%)	**29.4**	**29.6**	**92.2**	**92.2**	**91.9**	**91.3**	**-13.4**	**12.2**	**-29.4**	**-29.4**	**-32.2**	**-11.9**	**-14.0**

Table 67: Proteus Malware – Instance 2 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	50.00		35.38		40.00		40.00		0.00		78.00	
	VFD	98.08	**96.15**	96.15	**171.74**	80.00	**100.00**	80.00	**100.00**	100.00	**150.00**	70.00	**-10.26**
	CFD	63.46	**26.92**	63.46	**79.35**	90.00	**125.00**	90.00	**125.00**	100.00	**150.00**	90.00	**15.38**
	IFD	36.54	**-26.92**	36.54	**3.26**	90.00	**125.00**	90.00	**125.00**	100.00	**150.00**	90.00	**15.38**
TNR (%)	**Euclid.**	53.33		60.37		59.38		59.58		98.54		20.63	
	VFD	42.59	**-20.14**	38.89	**-35.58**	22.92	**-61.40**	22.92	**-61.54**	9.38	**-90.49**	23.96	**16.16**
	CFD	44.44	**-16.67**	46.30	**-23.31**	15.63	**-73.68**	15.63	**-73.78**	15.63	**-84.14**	21.88	**6.06**
	IFD	72.22	**35.42**	74.07	**22.70**	27.08	**-54.39**	27.08	**-54.55**	18.75	**-80.97**	13.54	**-34.34**
FPR (%)	**Euclid.**	46.67		39.63		40.63		40.42		1.46		79.38	
	VFD	57.41	**-23.02**	61.11	**-54.21**	77.08	**-89.74**	77.08	**-90.72**	90.63	**-6114.29**	76.04	**4.20**
	CFD	55.56	**-19.05**	53.70	**-35.51**	84.38	**-107.69**	84.38	**-108.76**	84.38	**-5685.71**	78.13	**1.57**
	IFD	27.78	**40.48**	25.93	**34.58**	72.92	**-79.49**	72.92	**-80.41**	81.25	**-5471.43**	86.46	**-8.92**
FNR (%)	**Euclid.**	50.00		64.62		60.00		60.00		100.00		22.00	
	VFD	1.92	**96.15**	3.85	**94.05**	20.00	**66.67**	20.00	**66.67**	0.00	**100.00**	30.00	**-36.36**
	CFD	36.54	**26.92**	36.54	**43.45**	10.00	**83.33**	10.00	**83.33**	0.00	**100.00**	10.00	**54.55**
	IFD	63.46	**-26.92**	63.46	**1.79**	10.00	**83.33**	10.00	**83.33**	0.00	**100.00**	10.00	**54.55**
Prec. (%)	**Euclid.**	40.49		26.01		3.83		3.86		0.00		7.45	
	VFD	62.20	**53.62**	60.24	**131.59**	9.76	**154.87**	9.76	**152.43**	10.31	**1031.00**	8.75	**17.53**
	CFD	52.38	**29.38**	53.23	**104.63**	10.00	**161.24**	10.00	**158.74**	10.99	**1099.00**	10.71	**43.91**
	IFD	55.88	**38.03**	57.58	**121.35**	11.39	**197.62**	11.39	**194.77**	11.36	**1136.00**	9.78	**31.40**
Acc. (%)	**Euclid.**	51.70		48.11		57.55		57.74		89.25		26.04	
	VFD	69.81	**35.04**	66.98	**39.22**	28.30	**-50.82**	28.30	**-50.98**	17.92	**-79.92**	28.30	**8.70**
	CFD	53.77	**4.01**	54.72	**13.73**	22.64	**-60.66**	22.64	**-60.78**	23.58	**-73.57**	28.30	**8.70**
	IFD	54.72	**5.84**	55.66	**15.69**	33.02	**-42.62**	33.02	**-42.81**	26.42	**-70.40**	20.75	**-20.29**
F1 (%)	**Euclid.**	41.72		27.72		6.99		7.05		0.00		13.59	
	VFD	76.12	**82.46**	74.07	**167.24**	17.39	**148.91**	17.39	**146.73**	18.69	**1869.00**	15.56	**14.44**
	CFD	57.39	**37.57**	57.89	**108.87**	18.00	**157.62**	18.00	**155.37**	19.80	**1980.00**	19.15	**40.88**
	IFD	44.19	**5.92**	44.71	**61.29**	20.22	**189.46**	20.22	**186.93**	20.41	**2041.00**	17.65	**29.83**

15) Stabuniq Malware – Instance 1

Table 68: Stabuniq Malware – Instance 1 - Malware vs. Normal sample ratio.

	Total	Stabuniq 01 Malware	Timestamp Resolution (micro-sec)	Total Timestamps (count)	Malware Timestamps (count)	Normal Timestamps (count)	Malware Ratio (%)
Node	305	5	10^0	186.0	69.0	117.0	37.1
			10^1	186.0	69.0	117.0	37.1
			10^2	186.0	69.0	117.0	37.1
			10^3	186.0	69.0	117.0	37.1
			10^4	182.0	68.0	114.0	37.4
			10^5	137.0	65.0	72.0	47.4
			10^6	100.0	54.0	46.0	54.0
			10^7	65.0	44.0	21.0	67.7
			10^8	32.0	23.0	9.0	71.9
			10^9	6.0	6.0	0.0	100.0
Edge	464	8	10^0	186.0	7.0	179.0	3.8
			10^1	186.0	7.0	179.0	3.8
			10^2	186.0	7.0	179.0	3.8
			10^3	186.0	7.0	179.0	3.8
			10^4	182.0	7.0	175.0	3.8
			10^5	137.0	6.0	131.0	4.4
			10^6	100.0	4.0	96.0	4.0
			10^7	65.0	3.0	62.0	4.6
			10^8	32.0	2.0	30.0	6.3
			10^9	6.0	2.0	4.0	33.3

Table 69: Stabuniq Malware – Instance 1 - Goodness of Fit Tests, Kurtosis, VFD, SFD, Sampling frequency.

Stabuniq 01 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	13.93588023	1.167601332	0.666443034	1
	10^1	1	1	1	1	13.93588023	1.167601332	0.666443034	1
	10^2	1	1	1	1	13.93588023	1.167601332	0.666443034	1
	10^3	1	1	1	1	13.93588023	1.167601332	0.666443034	1
	10^4	1	1	1	1	11.64870279	1.167405756	0.666443034	1
	10^5	1	1	1	1	10.75684492	1.174692009	0.553749713	1
	10^6	1	1	1	1	12.90316378	1.131577303	0.96517351	1
	10^7	1	1	1	1	15.40618188	NaN	0.952034768	1
	10^8	1	1	1	1	18.28164092	NaN	1.295695917	1
	10^9	1	0	0	1	2.864747299	NaN	1.821564866	1
Edge	10^0	1	1	1	1	24.60139629	1.167601332	0.843976621	1
	10^1	1	1	1	1	24.60139629	1.167601332	0.843976621	1
	10^2	1	1	1	1	24.60139629	1.167601332	0.843976621	1
	10^3	1	1	1	1	24.60139629	1.167601332	0.843976621	1
	10^4	1	1	1	1	20.7738869	1.167405756	0.934910059	1
	10^5	1	1	1	1	20.2995945	1.174692009	0.826285347	1
	10^6	1	1	1	1	15.35447028	1.131577303	0.767953972	1
	10^7	1	1	1	1	19.1588163	NaN	0.936666661	1
	10^8	1	0	1	1	19.84255015	NaN	0.730966258	1
	10^9	1	0	0	1	3.181240417	NaN	1.889172551	1

Table 70: Stabuniq Malware – Instance 1 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.06	1.06	1.01	1.01	1.01	1.00	1.22	1.00	1.32	1.32	1.32	1.32	1.00
	Normal	1.11	1.11	1.17	1.17	1.10	1.11	1.13	1.14	1.08	1.08	1.08	1.09	1.17
	Delta Normal (%)	**4.6**	**4.9**	**13.7**	**13.7**	**8.8**	**9.9**	**-8.4**	**12.2**	**-22.4**	**-22.4**	**-22.4**	**-21.5**	**14.3**
CFD	Malware	0.10	0.10	0.01	0.01	0.01	0.00	1.02	1.58	1.29	1.29	1.16	1.29	1.58
	Normal	0.17	0.17	0.22	0.22	0.09	0.13	1.15	1.04	1.08	1.08	1.06	0.98	1.09
	Delta Normal (%)	**39.4**	**43.4**	**97.3**	**97.3**	**94.2**	**99.7**	**11.0**	**-52.7**	**-19.5**	**-19.5**	**-9.5**	**-31.8**	**-45.6**
IFD	Malware	0.16	0.15	0.01	0.01	0.01	0.00	1.47	2.29	1.86	1.86	1.67	1.86	2.29
	Normal	0.26	0.26	0.32	0.32	0.13	0.20	1.65	1.50	1.56	1.56	1.54	1.42	1.57
	Delta Normal (%)	**39.2**	**43.5**	**97.3**	**97.3**	**94.3**	**99.7**	**11.0**	**-52.7**	**-19.4**	**-19.4**	**-9.0**	**-31.3**	**-45.6**

Table 71: Stabuniq Malware – Instance 1 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	52.62		6.77		40.00		40.00		36.67		56.67	
	VFD	98.46	**87.13**	93.85	**1286.36**	83.33	**108.33**	83.33	**108.33**	66.67	**66.67**	100.00	**76.47**
	CFD	50.77	**-3.51**	52.31	**672.73**	100.00	**150.00**	100.00	**150.00**	100.00	**150.00**	100.00	**76.47**
	IFD	30.77	**-41.52**	36.92	**445.45**	100.00	**150.00**	100.00	**150.00**	50.00	**25.00**	100.00	**76.47**
TNR (%)	**Euclid.**	45.00		92.50		59.69		59.54		59.69		40.15	
	VFD	34.72	**-22.84**	30.56	**-66.97**	24.43	**-59.08**	24.43	**-58.97**	17.56	**-70.59**	20.61	**-48.67**
	CFD	48.61	**8.02**	50.00	**-45.95**	12.98	**-78.26**	12.98	**-78.21**	6.11	**-89.77**	11.45	**-71.48**
	IFD	65.28	**45.06**	72.22	**-21.92**	64.89	**8.70**	64.89	**8.97**	30.53	**-48.85**	15.27	**-61.98**
FPR (%)	**Euclid.**	55.00		7.50		40.31		40.46		40.31		59.85	
	VFD	65.28	**-18.69**	69.44	**-825.93**	75.57	**-87.50**	75.57	**-86.79**	82.44	**-104.55**	79.39	**-32.65**
	CFD	51.39	**6.57**	50.00	**-566.67**	87.02	**-115.91**	87.02	**-115.09**	93.89	**-132.95**	88.55	**-47.96**
	IFD	34.72	**36.87**	27.78	**-270.37**	35.11	**12.88**	35.11	**13.21**	69.47	**-72.35**	84.73	**-41.58**
FNR (%)	**Euclid.**	47.38		93.23		60.00		60.00		63.33		43.33	
	VFD	1.54	**96.75**	6.15	**93.40**	16.67	**72.22**	16.67	**72.22**	33.33	**47.37**	0.00	**100.00**
	CFD	49.23	**-3.90**	47.69	**48.84**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**
	IFD	69.23	**-46.10**	63.08	**32.34**	0.00	**100.00**	0.00	**100.00**	50.00	**21.05**	0.00	**100.00**
Prec. (%)	**Euclid.**	46.58		38.69		1.77		1.77		1.63		2.51	
	VFD	57.66	**23.79**	54.95	**42.04**	4.81	**171.43**	4.81	**171.43**	3.57	**119.29**	5.45	**117.61**
	CFD	47.14	**1.22**	48.57	**25.54**	5.00	**182.29**	5.00	**182.29**	4.65	**185.59**	4.92	**96.21**
	IFD	44.44	**-4.58**	54.55	**40.98**	11.54	**551.43**	11.54	**551.43**	3.19	**95.96**	5.13	**104.59**
Acc. (%)	**Euclid.**	48.61		51.82		58.83		58.69		58.69		40.88	
	VFD	64.96	**33.63**	60.58	**16.90**	27.01	**-54.09**	27.01	**-53.98**	19.71	**-66.42**	24.09	**-41.07**
	CFD	49.64	**2.10**	51.09	**-1.41**	16.79	**-71.46**	16.79	**-71.39**	10.22	**-82.59**	15.33	**-62.50**
	IFD	48.91	**0.60**	55.47	**7.04**	66.42	**12.90**	66.42	**13.18**	31.39	**-46.52**	18.98	**-53.57**
F1 (%)	**Euclid.**	42.34		11.28		3.39		3.39		3.12		4.80	
	VFD	72.73	**71.78**	69.32	**514.72**	9.09	**167.99**	9.09	**167.99**	6.78	**117.39**	10.34	**115.48**
	CFD	48.89	**15.47**	50.37	**346.69**	9.52	**180.75**	9.52	**180.75**	8.89	**185.02**	9.38	**95.28**
	IFD	36.36	**-14.11**	44.04	**290.52**	20.69	**509.91**	20.69	**509.91**	6.00	**92.39**	9.76	**103.22**

16) Stabuniq Malware – Instance 2

Table 72: Stabuniq Malware – Instance 2 - Malware vs. Normal sample ratio.

	Total	Stabuniq 02 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	353	7	10^0	208.0	81.0	127.0	38.9
			10^1	208.0	81.0	127.0	38.9
			10^2	208.0	81.0	127.0	38.9
			10^3	208.0	81.0	127.0	38.9
			10^4	208.0	81.0	127.0	38.9
			10^5	183.0	78.0	105.0	42.6
			10^6	145.0	67.0	78.0	46.2
			10^7	98.0	52.0	46.0	53.1
			10^8	40.0	31.0	9.0	77.5
			10^9	9.0	9.0	0.0	100.0
Edge	561	12	10^0	208.0	7.0	201.0	3.4
			10^1	208.0	7.0	201.0	3.4
			10^2	208.0	7.0	201.0	3.4
			10^3	208.0	7.0	201.0	3.4
			10^4	208.0	7.0	201.0	3.4
			10^5	183.0	6.0	177.0	3.3
			10^6	145.0	6.0	139.0	4.1
			10^7	98.0	5.0	93.0	5.1
			10^8	40.0	3.0	37.0	7.5
			10^9	9.0	2.0	7.0	22.2

Table 73: Stabuniq Malware – Instance 2 - Goodness of Fit Tests, Kurtosis, VFD, SFD, Sampling frequency.

Stabuniq 02 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	34.75482125	1.103402009	0.684193477	1
	10^1	1	1	1	1	34.75482125	1.103402009	0.684193477	1
	10^2	1	1	1	1	34.75482125	1.103402009	0.684193477	1
	10^3	1	1	1	1	34.75482125	1.103402009	0.684193477	1
	10^4	1	1	1	1	34.75482125	1.103402009	0.684193477	1
	10^5	1	1	1	1	21.922314	1.167405756	0.936666661	1
	10^6	1	1	1	1	20.28730837	1.174564571	0.201897123	1
	10^7	1	0	1	1	38.44241377	1.131206418	0.466611853	1
	10^8	1	0	1	1	29.87659038	NaN	0.467422899	1
	10^9	1	0	1	1	5.316245772	NaN	0.878058977	1
Edge	10^0	1	0	1	1	51.66765146	1.103402009	0.531669823	1
	10^1	1	0	1	1	51.66765146	1.103402009	0.531669823	1
	10^2	1	0	1	1	51.66765146	1.103402009	0.531669823	1
	10^3	1	0	1	1	51.66765146	1.103402009	0.531669823	1
	10^4	1	0	1	1	51.66765146	1.103402009	0.531669823	1
	10^5	1	1	1	1	31.8593637	1.167405756	0.477147899	1
	10^6	1	1	1	1	25.72891594	1.174564571	0.405286155	1
	10^7	1	0	1	1	46.67146161	1.131206418	0.905519617	1
	10^8	1	0	1	1	30.74602491	NaN	0.546154253	1
	10^9	1	0	1	1	4.909717841	NaN	0.537784846	1

Table 74: Stabuniq Malware – Instance 2 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.06	1.06	1.00	1.00	1.00	1.00	1.22	1.00	1.32	1.32	1.58	1.35	1.00
	Normal	1.10	1.10	1.12	1.12	1.09	1.08	1.13	1.13	1.11	1.11	1.11	1.14	1.10
	Delta Normal (%)	**3.8**	**4.2**	**10.3**	**10.3**	**8.0**	**6.9**	**-7.8**	**11.7**	**-18.7**	**-18.7**	**-42.3**	**-18.7**	**9.4**
CFD	Malware	0.11	0.10	0.01	0.01	0.00	0.00	1.07	1.58	1.29	1.29	1.00	1.08	1.58
	Normal	0.16	0.17	0.17	0.17	0.08	0.11	1.17	1.07	1.02	1.02	0.99	0.93	1.08
	Delta Normal (%)	**36.1**	**41.1**	**97.0**	**97.0**	**96.8**	**97.7**	**8.6**	**-48.7**	**-27.3**	**-27.3**	**-1.5**	**-16.1**	**-47.4**
IFD	Malware	0.16	0.15	0.01	0.01	0.00	0.00	1.55	2.29	1.86	1.86	1.44	1.62	2.29
	Normal	0.25	0.25	0.26	0.26	0.12	0.16	1.69	1.54	1.46	1.46	1.43	1.35	1.55
	Delta Normal (%)	**36.1**	**40.8**	**96.9**	**96.9**	**96.9**	**97.7**	**8.6**	**-48.7**	**-27.3**	**-27.3**	**-0.8**	**-20.6**	**-47.4**

Table 75: Stabuniq Malware – Instance 2 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	34.10		31.54		40.00		20.00		80.00		56.67	
	VFD	92.31	**170.68**	92.31	**192.68**	66.67	**66.67**	66.67	**233.33**	100.00	**150.00**	83.33	**47.06**
	CFD	67.95	**99.25**	80.77	**156.10**	100.00	**150.00**	100.00	**400.00**	100.00	**150.00**	83.33	**47.06**
	IFD	62.82	**84.21**	73.08	**131.71**	100.00	**150.00**	100.00	**400.00**	100.00	**150.00**	100.00	**76.47**
TNR (%)	**Euclid.**	66.48		67.24		59.77		78.98		20.56		40.11	
	VFD	14.29	**-78.51**	13.33	**-80.17**	20.34	**-65.97**	20.34	**-74.25**	6.78	**-67.03**	24.29	**-39.44**
	CFD	27.62	**-58.45**	37.14	**-44.76**	16.95	**-71.64**	16.95	**-78.54**	3.95	**-80.77**	9.04	**-77.46**
	IFD	29.52	**-55.59**	37.14	**-44.76**	7.34	**-87.71**	7.34	**-90.70**	6.78	**-67.03**	6.78	**-83.10**
FPR (%)	**Euclid.**	33.52		32.76		40.23		21.02		79.44		59.89	
	VFD	85.71	**-155.68**	86.67	**-164.53**	79.66	**-98.03**	79.66	**-279.03**	93.22	**-17.35**	75.71	**-26.42**
	CFD	72.38	**-115.91**	62.86	**-91.86**	83.05	**-106.46**	83.05	**-295.16**	96.05	**-20.91**	90.96	**-51.89**
	IFD	70.48	**-110.23**	62.86	**-91.86**	92.66	**-130.34**	92.66	**-340.86**	93.22	**-17.35**	93.22	**-55.66**
FNR (%)	**Euclid.**	65.90		68.46		60.00		80.00		20.00		43.33	
	VFD	7.69	**88.33**	7.69	**88.76**	33.33	**44.44**	33.33	**58.33**	0.00	**100.00**	16.67	**61.54**
	CFD	32.05	**51.36**	19.23	**71.91**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**	16.67	**61.54**
	IFD	37.18	**43.58**	26.92	**60.67**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**	0.00	**100.00**
Prec. (%)	**Euclid.**	42.20		37.92		1.33		0.66		2.66		1.87	
	VFD	44.44	**5.32**	44.17	**16.49**	2.76	**107.47**	2.76	**316.09**	3.51	**32.13**	3.60	**92.18**
	CFD	41.09	**-2.64**	48.84	**28.79**	3.92	**194.93**	3.92	**491.50**	3.41	**28.37**	3.01	**60.92**
	IFD	39.84	**-5.60**	46.34	**22.21**	3.53	**165.44**	3.53	**432.35**	3.51	**32.13**	3.51	**87.46**
Acc. (%)	**Euclid.**	52.68		52.02		59.13		77.05		22.51		40.66	
	VFD	47.54	**-9.75**	46.99	**-9.66**	21.86	**-63.03**	21.86	**-71.63**	9.84	**-56.31**	26.23	**-35.48**
	CFD	44.81	**-14.94**	55.74	**7.14**	19.67	**-66.73**	19.67	**-74.47**	7.10	**-68.45**	11.48	**-71.77**
	IFD	43.72	**-17.01**	52.46	**0.84**	10.38	**-82.44**	10.38	**-86.52**	9.84	**-56.31**	9.84	**-75.81**
F1 (%)	**Euclid.**	30.00		26.03		2.57		1.28		5.14		3.62	
	VFD	60.00	**100.02**	59.75	**129.52**	5.30	**105.85**	5.30	**312.80**	6.78	**31.88**	6.90	**90.31**
	CFD	51.21	**70.71**	60.87	**133.81**	7.55	**193.24**	7.55	**488.05**	6.59	**28.26**	5.81	**60.44**
	IFD	48.76	**62.53**	56.72	**117.86**	6.82	**164.91**	6.82	**431.25**	6.78	**31.88**	6.78	**87.08**

17) Nivdort Malware – Instance 1

Table 76: Nivdort Malware – Instance 1 - Malware vs. Normal sample ratio.

	Total	Nivdort 01 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	309	24	10^0	189.0	82.0	107.0	43.4
			10^1	189.0	82.0	107.0	43.4
			10^2	189.0	82.0	107.0	43.4
			10^3	189.0	82.0	107.0	43.4
			10^4	185.0	82.0	103.0	44.3
			10^5	138.0	64.0	74.0	46.4
			10^6	97.0	50.0	47.0	51.5
			10^7	61.0	43.0	18.0	70.5
			10^8	29.0	24.0	5.0	82.8
			10^9	7.0	6.0	1.0	85.7
Edge	477	46	10^0	189.0	32.0	157.0	16.9
			10^1	189.0	32.0	157.0	16.9
			10^2	189.0	32.0	157.0	16.9
			10^3	189.0	32.0	157.0	16.9
			10^4	185.0	32.0	153.0	17.3
			10^5	138.0	20.0	118.0	14.5
			10^6	97.0	17.0	80.0	17.5
			10^7	61.0	17.0	44.0	27.9
			10^8	29.0	14.0	15.0	48.3
			10^9	7.0	5.0	2.0	71.4

Table 77: Nivdort Malware – Instance 1 - Goodness of Fit tests, Kurtosis, VFD, SFD, Sampling frequency.

Nivdort 01 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	13.05804519	1.167683617	0.929669297	1
	10^1	1	1	1	1	13.05804519	1.167683617	0.929669297	1
	10^2	1	1	1	1	13.05804519	1.167683617	0.929669297	1
	10^3	1	1	1	1	13.05804519	1.167683617	0.929669297	1
	10^4	1	1	1	1	11.88597263	1.16757698	0.929669297	1
	10^5	1	1	1	1	9.657051853	1.174736585	0.760075929	1
	10^6	1	1	1	1	12.84410225	1.131081156	0.633032529	1
	10^7	1	1	1	1	15.82744103	NaN	0.633032529	1
	10^8	1	0	1	1	12.41900392	NaN	1.241744704	1
	10^9	1	0	0	1	2.560050993	NaN	1.877124276	1
Edge	10^0	1	1	1	1	21.85330113	1.167683617	0.929669297	1
	10^1	1	1	1	1	21.85330113	1.167683617	0.929669297	1
	10^2	1	1	1	1	21.85330113	1.167683617	0.929669297	1
	10^3	1	1	1	1	21.85330113	1.167683617	0.929669297	1
	10^4	1	1	1	1	19.99332146	1.16757698	0.929669297	1
	10^5	1	1	1	1	15.37742315	1.174736585	0.708496256	1
	10^6	1	1	1	1	13.65548522	1.131081156	0.588321389	1
	10^7	1	1	1	1	20.4135373	NaN	0.588321389	1
	10^8	1	0	1	1	14.20283319	NaN	1.19587036	1
	10^9	1	0	0	1	2.793618037	NaN	1.800039859	1

Table 78: Nivdort Malware – Instance 1 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.07	1.07	1.03	1.03	1.02	1.02	1.22	1.23	1.30	1.30	1.30	1.30	1.29
	Normal	1.10	1.10	1.13	1.13	1.10	1.09	1.13	1.14	1.08	1.08	1.08	1.09	1.18
	Delta Normal (%)	**2.8**	**3.0**	**8.8**	**8.8**	**6.9**	**6.1**	**-7.6**	**-7.9**	**-20.0**	**-20.0**	**-19.9**	**-19.2**	**-10.1**
CFD	Malware	0.11	0.11	0.03	0.03	0.02	0.02	1.08	1.18	1.15	1.15	1.15	1.13	1.00
	Normal	0.15	0.16	0.18	0.18	0.09	0.11	1.12	1.03	1.08	1.08	1.05	0.98	1.06
	Delta Normal (%)	**28.7**	**30.5**	**80.5**	**80.5**	**80.2**	**81.7**	**3.4**	**-14.5**	**-6.9**	**-6.9**	**-9.8**	**-14.8**	**5.6**
IFD	Malware	0.17	0.17	0.05	0.05	0.02	0.03	1.56	1.70	1.66	1.66	1.66	1.63	1.44
	Normal	0.23	0.24	0.27	0.27	0.13	0.16	1.61	1.48	1.55	1.55	1.52	1.43	1.53
	Delta Normal (%)	**28.7**	**30.6**	**80.0**	**80.0**	**80.6**	**81.9**	**3.4**	**-14.5**	**-6.9**	**-6.9**	**-9.2**	**-14.6**	**5.6**

Table 79: Nivdort Malware – Instance 1 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	90.94		55.63		60.00		78.00		79.00		60.00	
	VFD	76.56	-15.81	82.81	48.88	35.00	-41.67	35.00	-55.13	45.00	-25.00	60.00	0.00
	CFD	28.13	-69.07	62.50	12.36	15.00	-75.00	15.00	-80.77	75.00	25.00	60.00	0.00
	IFD	50.00	-45.02	75.00	34.83	50.00	-16.67	50.00	-35.90	75.00	25.00	75.00	25.00
TNR (%)	**Euclid.**	7.03		46.49		40.68		20.51		21.02		39.66	
	VFD	43.24	515.38	27.03	-41.86	20.34	-50.00	20.34	-0.83	22.88	8.87	23.73	-40.17
	CFD	82.43	1073.08	50.00	7.56	51.69	27.08	51.69	152.07	12.71	-39.52	26.27	-33.76
	IFD	59.46	746.15	37.84	-18.60	25.42	-37.50	25.42	23.97	12.71	-39.52	20.34	-48.72
FPR (%)	**Euclid.**	92.97		53.51		59.32		79.49		78.98		60.34	
	VFD	56.76	38.95	72.97	-36.36	79.66	-34.29	79.66	-0.21	77.12	2.36	76.27	-26.40
	CFD	17.57	81.10	50.00	6.57	48.31	18.57	48.31	39.23	87.29	-10.52	73.73	-22.19
	IFD	40.54	56.40	62.16	-16.16	74.58	-25.71	74.58	6.18	87.29	-10.52	79.66	-32.02
FNR (%)	**Euclid.**	9.06		44.38		40.00		22.00		21.00		40.00	
	VFD	23.44	-158.62	17.19	61.27	65.00	-62.50	65.00	-195.45	55.00	-161.90	40.00	0.00
	CFD	71.88	-693.10	37.50	15.49	85.00	-112.50	85.00	-286.36	25.00	-19.05	40.00	0.00
	IFD	50.00	-451.72	25.00	43.66	50.00	-25.00	50.00	-127.27	25.00	-19.05	25.00	37.50
Prec. (%)	**Euclid.**	45.78		48.61		8.85		11.45		31.47		13.61	
	VFD	53.85	17.61	49.53	1.90	6.93	-21.65	6.93	-39.47	9.00	-71.40	11.76	-13.58
	CFD	58.06	26.83	51.95	6.87	5.00	-43.47	5.00	-56.33	12.71	-59.61	12.12	-10.96
	IFD	51.61	12.73	51.06	5.05	10.20	15.36	10.20	-10.88	12.71	-59.61	13.76	1.09
Acc. (%)	**Euclid.**	45.94		50.72		43.48		28.84		29.42		42.61	
	VFD	58.70	27.76	52.90	4.29	22.46	-48.33	22.46	-22.11	26.09	-11.33	28.99	-31.97
	CFD	57.25	24.61	55.80	10.00	46.38	6.67	46.38	60.80	21.74	-26.11	31.16	-26.87
	IFD	55.07	19.87	55.07	8.57	28.99	-33.33	28.99	0.50	21.74	-26.11	28.26	-33.67
F1 (%)	**Euclid.**	60.85		43.56		15.42		19.97		21.90		16.70	
	VFD	63.23	3.90	61.99	42.29	11.57	-24.95	11.57	-42.06	15.00	-31.52	19.67	17.81
	CFD	37.89	-37.73	56.74	30.24	7.50	-51.35	7.50	-62.44	21.74	-0.75	20.17	20.78
	IFD	50.79	-16.53	60.76	39.47	16.95	9.93	16.95	-15.12	21.74	-0.75	23.26	39.27

18) Nivdort Malware – Instance 2

Table 80: Nivdort Malware – Instance 2 - Malware vs. Normal sample ratio.

	Total	Nivdort 02 Malware	Timestamp Resolution (micro-sec)	Total Timestamps (count)	Malware Timestamps (count)	Normal Timestamps (count)	Malware Ratio (%)
Node	264	31	10^0	149.0	83.0	66.0	55.7
			10^1	149.0	83.0	66.0	55.7
			10^2	149.0	83.0	66.0	55.7
			10^3	149.0	83.0	66.0	55.7
			10^4	149.0	83.0	66.0	55.7
			10^5	113.0	67.0	46.0	59.3
			10^6	84.0	54.0	30.0	64.3
			10^7	60.0	47.0	13.0	78.3
			10^8	36.0	33.0	3.0	91.7
			10^9	8.0	8.0	0.0	100.0
Edge	365	60	10^0	149.0	37.0	112.0	24.8
			10^1	149.0	37.0	112.0	24.8
			10^2	149.0	37.0	112.0	24.8
			10^3	149.0	37.0	112.0	24.8
			10^4	149.0	37.0	112.0	24.8
			10^5	113.0	25.0	88.0	22.1
			10^6	84.0	23.0	61.0	27.4
			10^7	60.0	23.0	37.0	38.3
			10^8	36.0	21.0	15.0	58.3
			10^9	8.0	6.0	2.0	75.0

Table 81: Nivdort Malware – Instance 2 - Goodness of Fit Tests, Kurtosis, VFD, SFD, Sampling frequency.

Nivdort 02 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	13.4003862	1.174738463	0.305651303	1
	10^1	1	1	1	1	13.4003862	1.174738463	0.305651303	1
	10^2	1	1	1	1	13.4003862	1.174738463	0.305651303	1
	10^3	1	1	1	1	13.4003862	1.174738463	0.305651303	1
	10^4	1	1	1	1	13.4003862	1.174738463	0.305651303	1
	10^5	1	1	1	1	12.69123537	1.128785959	0.508938677	1
	10^6	1	1	1	1	16.24093807	1.218200793	0.811027261	1
	10^7	1	1	1	1	21.57975498	NaN	0.778109854	1
	10^8	1	0	1	1	23.36371567	NaN	1.160399803	1
	10^9	1	0	0	1	2.418636185	NaN	2.013997671	1
Edge	10^0	1	1	1	1	25.79197854	1.174738463	0.571063478	1
	10^1	1	1	1	1	25.79197854	1.174738463	0.571063478	1
	10^2	1	1	1	1	25.79197854	1.174738463	0.571063478	1
	10^3	1	1	1	1	25.79197854	1.174738463	0.571063478	1
	10^4	1	1	1	1	25.79197854	1.174738463	0.571063478	1
	10^5	1	1	1	1	16.33147908	1.128785959	0.571063478	1
	10^6	1	1	1	1	15.39103613	1.218200793	0.618385937	1
	10^7	1	1	1	1	26.16557426	NaN	0.705326742	1
	10^8	1	0	1	1	25.67854379	NaN	1.077918336	1
	10^9	1	0	0	1	2.065768312	NaN	2.019046992	1

Table 82: Nivdort Malware – Instance 2 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.08	1.08	1.05	1.05	1.03	1.03	1.22	1.24	1.17	1.17	1.18	1.17	1.30
	Normal	1.08	1.08	1.12	1.12	1.09	1.07	1.22	1.10	1.14	1.14	1.14	1.16	1.13
	Delta Normal (%)	**-0.3**	**-0.4**	**6.4**	**6.4**	**5.1**	**4.0**	**0.5**	**-12.9**	**-3.0**	**-3.0**	**-3.2**	**-1.2**	**-15.1**
CFD	Malware	0.14	0.14	0.05	0.05	0.02	0.03	1.08	1.29	1.21	1.21	1.19	1.14	1.05
	Normal	0.11	0.12	0.16	0.16	0.07	0.09	1.01	1.11	1.05	1.05	1.02	0.95	1.13
	Delta Normal (%)	**-25.1**	**-21.1**	**69.4**	**69.4**	**67.7**	**70.3**	**-7.2**	**-16.3**	**-15.3**	**-15.3**	**-16.9**	**-20.3**	**7.4**
IFD	Malware	0.22	0.22	0.07	0.07	0.03	0.04	1.56	1.87	1.75	1.75	1.72	1.67	1.52
	Normal	0.17	0.18	0.24	0.24	0.11	0.13	1.45	1.61	1.52	1.52	1.48	1.38	1.64
	Delta Normal (%)	**-24.6**	**-20.2**	**68.9**	**68.9**	**68.1**	**70.2**	**-7.2**	**-16.3**	**-15.3**	**-15.3**	**-16.4**	**-21.3**	**7.4**

Table 83: Nivdort Malware – Instance 2 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	51.94		34.63		60.00		58.40		59.20		20.00	
	VFD	92.54	78.16	91.04	162.93	40.00	-33.33	40.00	-31.51	60.00	0.00	64.00	220.00
	CFD	67.16	29.31	94.03	171.55	60.00	0.00	60.00	2.74	100.00	66.67	72.00	260.00
	IFD	65.67	26.44	94.03	171.55	48.00	-20.00	48.00	-17.81	92.00	53.33	76.00	280.00
TNR (%)	**Euclid.**	43.91		65.22		40.45		40.23		40.68		79.32	
	VFD	34.78	-20.79	32.61	-50.00	17.05	-57.87	17.05	-57.63	21.59	-46.93	10.23	-87.11
	CFD	36.96	-15.84	10.87	-83.33	21.59	-46.63	21.59	-46.33	9.09	-77.65	18.18	-77.08
	IFD	39.13	-10.89	8.70	-86.67	20.45	-49.44	20.45	-49.15	17.05	-58.10	11.36	-85.67
FPR (%)	**Euclid.**	56.09		34.78		59.55		59.77		59.32		20.68	
	VFD	65.22	-16.28	67.39	-93.75	82.95	-39.31	82.95	-38.78	78.41	-32.18	89.77	-334.07
	CFD	63.04	-12.40	89.13	-156.25	78.41	-31.68	78.41	-31.18	90.91	-53.26	81.82	-295.60
	IFD	60.87	-8.53	91.30	-162.50	79.55	-33.59	79.55	-33.08	82.95	-39.85	88.64	-328.57
FNR (%)	**Euclid.**	48.06		65.37		40.00		41.60		40.80		80.00	
	VFD	7.46	84.47	8.96	86.30	60.00	-50.00	60.00	-44.23	40.00	1.96	36.00	55.00
	CFD	32.84	31.68	5.97	90.87	40.00	0.00	40.00	3.85	0.00	100.00	28.00	65.00
	IFD	34.33	28.57	5.97	90.87	52.00	-30.00	52.00	-25.00	8.00	80.39	24.00	70.00
Prec. (%)	**Euclid.**	53.55		60.04		23.33		13.15		0.00		4.46	
	VFD	67.39	25.86	66.30	10.44	12.05	-48.37	12.05	-8.40	17.86	1786.00	16.84	277.26
	CFD	60.81	13.57	60.58	0.90	17.86	-23.47	17.86	35.76	23.81	2381.00	20.00	348.00
	IFD	61.11	14.13	60.00	-0.06	14.63	-37.28	14.63	11.26	23.96	2396.00	19.59	338.76
Acc. (%)	**Euclid.**	48.67		47.08		44.78		44.25		44.78		66.19	
	VFD	69.03	41.82	67.26	42.86	22.12	-50.59	22.12	-50.00	30.09	-32.81	22.12	-66.58
	CFD	54.87	12.73	60.18	27.82	30.09	-32.81	30.09	-32.00	29.20	-34.78	30.09	-54.55
	IFD	54.87	12.73	59.29	25.94	26.55	-40.71	26.55	-40.00	33.63	-24.90	25.66	-61.23
F1 (%)	**Euclid.**	48.30		32.12		23.25		21.47		22.96		7.30	
	VFD	77.99	61.46	76.73	138.88	18.52	-20.34	18.52	-13.75	27.52	19.89	26.67	265.33
	CFD	63.83	32.15	73.68	129.40	27.52	18.39	27.52	28.19	38.46	67.54	31.30	328.87
	IFD	63.31	31.07	73.26	128.06	22.43	-3.51	22.43	4.47	38.02	65.61	31.15	326.72

19) Poweliks Malware – Instance 1

Table 84: Poweliks Malware – Instance 1 - Malware vs. Normal sample ratio.

	Total	Poweliks 01 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	225	10	10^0	124.0	47.0	77.0	37.9
			10^1	124.0	47.0	77.0	37.9
			10^2	124.0	47.0	77.0	37.9
			10^3	124.0	47.0	77.0	37.9
			10^4	124.0	47.0	77.0	37.9
			10^5	98.0	44.0	54.0	44.9
			10^6	71.0	32.0	39.0	45.1
			10^7	51.0	30.0	21.0	58.8
			10^8	24.0	15.0	9.0	62.5
			10^9	7.0	5.0	2.0	71.4
Edge	315	15	10^0	124.0	8.0	116.0	6.5
			10^1	124.0	8.0	116.0	6.5
			10^2	124.0	8.0	116.0	6.5
			10^3	124.0	8.0	116.0	6.5
			10^4	124.0	8.0	116.0	6.5
			10^5	98.0	7.0	91.0	7.1
			10^6	71.0	6.0	65.0	8.5
			10^7	51.0	6.0	45.0	11.8
			10^8	24.0	2.0	22.0	8.3
			10^9	7.0	2.0	5.0	28.6

Table 85: Poweliks Malware – Instance 1 - Goodness of Fit Tests, Kurtosis, VFD, SFD, Sampling frequency.

Poweliks 01 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	7.189513267	1.129809376	0.666443034	1
	10^1	1	1	1	1	7.189513267	1.129809376	0.666443034	1
	10^2	1	1	1	1	7.189513267	1.129809376	0.666443034	1
	10^3	1	1	1	1	7.189513267	1.129809376	0.666443034	1
	10^4	1	1	1	1	7.189513267	1.129809376	0.666443034	1
	10^5	1	1	1	1	4.981704565	1.131206418	0.666443034	1
	10^6	1	1	1	1	12.56549144	NaN	0.49993956	1
	10^7	1	1	1	1	11.05397235	NaN	0.801921982	1
	10^8	1	0	1	1	16.52353034	NaN	0.408051555	1
	10^9	1	0	0	1	2.8363064	NaN	1.901717998	1
Edge	10^0	1	1	1	1	13.89037088	1.129809376	0.89369585	1
	10^1	1	1	1	1	13.89037088	1.129809376	0.89369585	1
	10^2	1	1	1	1	13.89037088	1.129809376	0.89369585	1
	10^3	1	1	1	1	13.89037088	1.129809376	0.89369585	1
	10^4	1	1	1	1	13.89037088	1.129809376	0.89369585	1
	10^5	1	1	1	1	8.032945722	1.131206418	0.89369585	1
	10^6	1	1	1	1	14.57616668	NaN	0.844486251	1
	10^7	1	1	1	1	13.53997639	NaN	1.098928459	1
	10^8	1	0	1	1	16.99055916	NaN	0.531904577	1
	10^9	1	0	0	1	2.42847808	NaN	1.785574585	1

Table 86: Poweliks Malware – Instance 1 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.06	1.05	1.01	1.01	1.01	1.01	1.30	1.68	1.36	1.36	1.39	1.94	1.58
	Normal	1.12	1.12	1.16	1.16	1.11	1.11	1.23	1.10	1.14	1.14	1.14	1.16	1.13
	Delta Normal (%)	**5.3**	**6.0**	**12.8**	**12.8**	**9.0**	**9.2**	**-6.0**	**-52.1**	**-19.6**	**-19.6**	**-22.2**	**-67.9**	**-40.4**
CFD	Malware	0.12	0.11	0.01	0.01	0.00	0.01	1.15	1.16	1.40	1.40	1.34	0.92	1.00
	Normal	0.19	0.20	0.21	0.21	0.09	0.13	1.06	1.09	1.04	1.04	1.02	0.94	1.15
	Delta Normal (%)	**39.9**	**43.9**	**93.0**	**93.0**	**94.4**	**93.2**	**-8.4**	**-6.1**	**-35.0**	**-35.0**	**-30.7**	**2.5**	**12.7**
IFD	Malware	0.17	0.17	0.02	0.02	0.01	0.01	1.66	1.67	2.03	2.03	1.97	1.39	1.44
	Normal	0.29	0.30	0.31	0.31	0.13	0.19	1.53	1.58	1.50	1.50	1.48	1.37	1.65
	Delta Normal (%)	**40.2**	**43.7**	**92.9**	**92.9**	**94.5**	**93.2**	**-8.4**	**-6.1**	**-35.0**	**-35.0**	**-32.9**	**-1.4**	**12.7**

Table 87: Poweliks Malware – Instance 1 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	11.36		37.27		60.00		60.00		60.00		40.00	
	VFD	97.73	760.00	97.73	162.20	57.14	-4.76	57.14	-4.76	85.71	42.86	71.43	78.57
	CFD	54.55	380.00	59.09	58.54	42.86	-28.57	42.86	-28.57	71.43	19.05	42.86	7.14
	IFD	29.55	160.00	52.27	40.24	42.86	-28.57	42.86	-28.57	71.43	19.05	42.86	7.14
TNR (%)	**Euclid.**	90.74		62.22		39.78		40.22		40.44		59.34	
	VFD	33.33	-63.27	31.48	-49.40	38.46	-3.31	38.46	-4.37	16.48	-59.24	28.57	-51.85
	CFD	38.89	-57.14	44.44	-28.57	68.13	71.27	68.13	69.40	24.18	-40.22	31.87	-46.30
	IFD	83.33	-8.16	57.41	-7.74	38.46	-3.31	38.46	-4.37	29.67	-26.63	31.87	-46.30
FPR (%)	**Euclid.**	9.26		37.78		60.22		59.78		59.56		40.66	
	VFD	66.67	-620.00	68.52	-81.37	61.54	-2.19	61.54	-2.94	83.52	-40.22	71.43	-75.68
	CFD	61.11	-560.00	55.56	-47.06	31.87	47.08	31.87	46.69	75.82	-27.31	68.13	-67.57
	IFD	16.67	-80.00	42.59	-12.75	61.54	-2.19	61.54	-2.94	70.33	-18.08	68.13	-67.57
FNR (%)	**Euclid.**	88.64		62.73		40.00		40.00		40.00		60.00	
	VFD	2.27	97.44	2.27	96.38	42.86	-7.14	42.86	-7.14	14.29	64.29	28.57	52.38
	CFD	45.45	48.72	40.91	34.78	57.14	-42.86	57.14	-42.86	28.57	28.57	57.14	4.76
	IFD	70.45	20.51	47.73	23.91	57.14	-42.86	57.14	-42.86	28.57	28.57	57.14	4.76
Prec. (%)	**Euclid.**	0.00		38.53		4.34		4.36		4.38		2.89	
	VFD	54.43	5443.00	53.75	39.52	6.67	53.44	6.67	52.91	7.32	67.24	7.14	147.45
	CFD	42.11	4211.00	46.43	20.51	9.38	115.77	9.38	115.02	6.76	54.43	4.62	59.89
	IFD	59.09	5909.00	50.00	29.78	5.08	17.03	5.08	16.62	7.25	65.62	4.62	59.89
Acc. (%)	**Euclid.**	55.10		51.02		41.22		41.63		41.84		57.96	
	VFD	62.24	12.96	61.22	20.00	39.80	-3.47	39.80	-4.41	21.43	-48.78	31.63	-45.42
	CFD	45.92	-16.67	51.02	0.00	66.33	60.89	66.33	59.31	27.55	-34.15	32.65	-43.66
	IFD	59.18	7.41	55.10	8.00	38.78	-5.94	38.78	-6.86	32.65	-21.95	32.65	-43.66
F1 (%)	**Euclid.**	16.60		31.69		8.10		8.13		8.16		5.38	
	VFD	69.92	321.26	69.35	118.83	11.94	47.36	11.94	46.88	13.48	65.32	12.99	141.19
	CFD	47.52	186.34	52.00	64.07	15.38	89.86	15.38	89.25	12.35	51.37	8.33	54.76
	IFD	39.39	137.35	51.11	61.27	9.09	12.19	9.09	11.83	13.16	61.33	8.33	54.76

20) Poweliks Malware – Instance 2

Table 88: Poweliks Malware – Instance 2 - Malware vs. Normal sample ratio.

	Total	Poweliks 02 Malware	Timestamp Resolution	Total Timestamps	Malware Timestamps	Normal Timestamps	Malware Ratio
			(micro-sec)	(count)	(count)	(count)	(%)
Node	266	9	10^0	152.0	64.0	88.0	42.1
			10^1	152.0	64.0	88.0	42.1
			10^2	152.0	64.0	88.0	42.1
			10^3	151.0	64.0	87.0	42.4
			10^4	150.0	64.0	86.0	42.7
			10^5	113.0	53.0	60.0	46.9
			10^6	77.0	42.0	35.0	54.5
			10^7	48.0	31.0	17.0	64.6
			10^8	27.0	18.0	9.0	66.7
			10^9	6.0	5.0	1.0	83.3
Edge	399	12	10^0	152.0	7.0	145.0	4.6
			10^1	152.0	7.0	145.0	4.6
			10^2	152.0	7.0	145.0	4.6
			10^3	151.0	7.0	144.0	4.6
			10^4	150.0	7.0	143.0	4.7
			10^5	113.0	7.0	106.0	6.2
			10^6	77.0	6.0	71.0	7.8
			10^7	48.0	4.0	44.0	8.3
			10^8	27.0	3.0	24.0	11.1
			10^9	6.0	2.0	4.0	33.3

Table 89: Poweliks Malware – Instance 2 - Goodness of Fit Tests, Kurtosis, VFD, SFD, Sampling frequency.

Poweliks 02 DataSet	Timestamp Resolution	KStst	Chitst	Lilltst	ttst	Kurtosis	VFD	Spectral Dim.	Normalized Sampling Frequency
	(micro-sec)	0 or 1	0 or 1	0 or 1	0 or 1	absolute			
Node	10^0	1	1	1	1	8.02363061	1.175030527	0.722240631	1
	10^1	1	1	1	1	8.02363061	1.175030527	0.722240631	1
	10^2	1	1	1	1	8.02363061	1.175030527	0.722240631	1
	10^3	1	1	1	1	7.687246667	1.174776103	0.722240631	1
	10^4	1	1	1	1	7.288133978	1.174776103	0.722240631	1
	10^5	1	1	1	1	8.301777107	1.128785959	0.702710897	1
	10^6	1	1	1	1	8.239096516	NaN	-0.481437879	1
	10^7	1	1	1	1	10.16560602	NaN	0.686246926	1
	10^8	1	0	1	1	14.71659203	NaN	1.123084139	1
	10^9	1	0	0	1	2.116252944	NaN	1.723293396	1
Edge	10^0	1	1	1	1	15.26902706	1.175030527	1.022719896	1
	10^1	1	1	1	1	15.26902706	1.175030527	1.022719896	1
	10^2	1	1	1	1	15.26902706	1.175030527	1.022719896	1
	10^3	1	1	1	1	14.58799625	1.174776103	1.022719896	1
	10^4	1	1	1	1	13.94864961	1.174776103	1.022719896	1
	10^5	1	1	1	1	10.40392206	1.128785959	0.828679453	1
	10^6	1	1	1	1	8.36200621	NaN	0.526703091	1
	10^7	1	1	1	1	11.76987612	NaN	1.356487586	1
	10^8	1	0	1	1	16.42681169	NaN	1.297467617	1
	10^9	1	0	0	1	2.346445545	NaN	1.849594891	1

Table 90: Poweliks Malware – Instance 2 - Average VFD, CFD and IFD of features.

Metric	Average Value	CNTS	TSNN	ECTS	EMTS	TSET	ETSD	TSNC	TSNR	TSER	TSEM	NTSE	ETTS	TSNE
VFD	Malware	1.07	1.07	1.01	1.01	1.01	1.00	1.22	1.58	1.32	1.32	1.31	1.36	1.00
	Normal	1.10	1.10	1.15	1.15	1.11	1.09	1.22	1.14	1.08	1.08	1.08	1.09	1.17
	Delta Normal (%)	**2.9**	**3.0**	**12.4**	**12.4**	**9.3**	**8.1**	**-0.3**	**-39.1**	**-22.1**	**-22.1**	**-20.8**	**-25.1**	**14.9**
CFD	Malware	0.12	0.11	0.01	0.01	0.01	0.00	1.00	1.00	1.29	1.29	1.21	0.92	1.58
	Normal	0.15	0.16	0.20	0.20	0.10	0.12	1.11	1.00	1.05	1.05	1.02	0.96	1.04
	Delta Normal (%)	**19.8**	**29.1**	**95.9**	**95.9**	**94.7**	**97.7**	**9.8**	**0.0**	**-23.2**	**-23.2**	**-18.0**	**4.0**	**-52.9**
IFD	Malware	0.18	0.17	0.01	0.01	0.01	0.00	1.44	1.44	1.86	1.86	1.80	1.39	2.29
	Normal	0.23	0.24	0.30	0.30	0.14	0.18	1.60	1.44	1.51	1.51	1.49	1.39	1.50
	Delta Normal (%)	**20.6**	**29.4**	**95.9**	**95.9**	**94.9**	**97.7**	**9.8**	**0.0**	**-23.2**	**-23.2**	**-21.3**	**0.4**	**-52.9**

Table 91: Poweliks Malware – Instance 2 - Evaluation metrics – K-means clustering algorithms.

Metric	Kmeans	CNTS	% improvement from Euclid	TSNN	% improvement from Euclid	ECTS	% improvement from Euclid	EMTS	% improvement from Euclid	ETTS	% improvement from Euclid	ETSD	% improvement from Euclid
TPR (%)	**Euclid.**	32.08		29.43		40.00		60.00		40.00		100.00	
	VFD	98.11	205.88	94.34	220.51	85.71	114.29	85.71	42.86	85.71	114.29	100.00	0.00
	CFD	33.96	5.88	39.62	34.62	71.43	78.57	71.43	19.05	85.71	114.29	100.00	0.00
	IFD	26.42	-17.65	32.08	8.97	100.00	150.00	100.00	66.67	85.71	114.29	100.00	0.00
TNR (%)	**Euclid.**	65.67		68.67		59.25		40.19		59.43		1.13	
	VFD	30.00	-54.31	25.00	-63.59	30.19	-49.04	30.19	-24.88	15.09	-74.60	22.64	1900.00
	CFD	48.33	-26.40	55.00	-19.90	50.00	-15.61	50.00	24.41	10.38	-82.54	28.30	2400.00
	IFD	58.33	-11.17	65.00	-5.34	32.08	-45.86	32.08	-20.19	10.38	-82.54	16.04	1316.67
FPR (%)	**Euclid.**	34.33		31.33		40.75		59.81		40.57		98.87	
	VFD	70.00	-103.88	75.00	-139.36	69.81	-71.30	69.81	-16.72	84.91	-109.30	77.36	21.76
	CFD	51.67	-50.49	45.00	-43.62	50.00	-22.69	50.00	16.40	89.62	-120.93	71.70	27.48
	IFD	41.67	-21.36	35.00	-11.70	67.92	-66.67	67.92	-13.56	89.62	-120.93	83.96	15.08
FNR (%)	**Euclid.**	67.92		70.57		60.00		40.00		60.00		0.00	
	VFD	1.89	97.22	5.66	91.98	14.29	76.19	14.29	64.29	14.29	76.19	0.00	0.00
	CFD	66.04	2.78	60.38	14.44	28.57	52.38	28.57	28.57	14.29	76.19	0.00	0.00
	IFD	73.58	-8.33	67.92	3.74	0.00	100.00	0.00	100.00	14.29	76.19	0.00	0.00
Prec. (%)	**Euclid.**	44.21		42.03		9.01		3.77		2.51		6.26	
	VFD	55.32	25.14	52.63	25.22	7.50	-16.75	7.50	98.81	6.25	148.88	7.87	25.62
	CFD	36.73	-16.90	43.75	4.09	8.62	-4.31	8.62	128.51	5.94	136.56	8.43	34.70
	IFD	35.90	-18.80	44.74	6.44	8.86	-1.65	8.86	134.88	5.94	136.56	7.29	16.46
Acc. (%)	**Euclid.**	49.91		50.27		58.05		41.42		58.23		7.26	
	VFD	61.95	24.11	57.52	14.44	33.63	-42.07	33.63	-18.80	19.47	-66.57	27.43	278.05
	CFD	41.59	-16.67	47.79	-4.93	51.33	-11.59	51.33	23.93	15.04	-74.16	32.74	351.22
	IFD	43.36	-13.12	49.56	-1.41	36.28	-37.50	36.28	-12.39	15.04	-74.16	21.24	192.68
F1 (%)	**Euclid.**	30.47		29.94		8.41		7.10		4.73		11.78	
	VFD	70.75	132.18	67.57	125.64	13.79	64.07	13.79	94.30	11.65	146.53	14.58	23.75
	CFD	35.29	15.83	41.58	38.87	15.38	83.00	15.38	116.72	11.11	135.11	15.56	32.00
	IFD	30.43	-0.12	37.36	24.77	16.28	93.64	16.28	129.32	11.11	135.11	13.59	15.34

4.5 Analysis of Results

4.5.1 Preliminary Characterization

As elaborated in subsection 4.2.5.4, the ratio of malware samples with respect to the normal samples in a particular time window resolution data set indicates the availability of malware vs. normal samples as required for the analysis by any machine learning algorithm (supervised or unsupervised). This in turn is related to the class imbalance problem which is frequently encountered in cyber domain where malware hide their presence by concealing themselves in normal activity patterns. Therefore, an evaluation of the graph based node and edge features with respect to their ratio is imperative to determine the viability of the feature in malware characterization. It is observed across all twenty malware instances that the edge data has considerably lower malware ratio for all time window resolutions. On the other hand, node based features depict better malware to normal samples ratio (Refer: Table 12, Table 16, Table 20, Table 24, Table 28, Table 32, Table 36, Table 40, Table 44, Table 48, Table 52, Table 56, Table 60, Table 64, Table 68, Table 72, Table 76, Table 80, Table 84, and Table 88). Therefore, subsequent analysis of all the features will consider the ratio aspect to address the characterization and clustering performance.

As tabulated in section 4.4, all node and edge based time graph data set of each malware instance indicate the absence of Gaussian distribution for initial five timestamps (windows) as indicated by four statistical significance tests i.e. Kolmogorov-Smirnov (KS) test, Chi^2 test, Lilliefors test and t-test. Further, this can be validated by the Kurtosis test which shows the degree of heaviness in the estimated probability distribution tail. This degree of heaviness depends on the magnitude of Kurtosis value which has a direct relationship with the weight of the distribution tail. The high magnitude of estimated Kurtosis values for each malware data set instance further reinforces the hypothesis of underlying heavy tailed distribution. It is worth-mentioning that optimum heavy tailed behavior with respect to the sufficiency of data set were observed for initial five time windows which is consistent across twenty malware instances (Refer: Table 13, Table 17, Table 21, Table 25, Table 29, Table 33, Table 37, Table 41, Table 45, Table 49, Table 53, Table 57, Table 61, Table 65, Table 69, Table 73, Table 77, Table 81, Table 85, and Table 89).

Further, as discussed in subsection 4.2.5.4, it is significantly important to validate the stationarity of dataset empirically. Due to the presence of heavy tailed distribution, it is not expected that the dataset will depict stationarity globally. Nevertheless, using power-law relationship of fractals, the stationarity in a local sense was evaluated. For this purpose the VFD values were computed for each time resolution of every data instance which were found to be within the bounds of embedded dimensions i.e. 1 and 2. This proves a weak sense stationarity with respect to the sampling time interval locally. Moreover, the estimation of optimum sampling time is necessary and should follow the Nyquist sampling criteria as described in subsection 4.2.5.4. For this purpose, SFD was estimated for each malware dataset instance and its values specify that

all the features represent fractional pink noise with higher long term correlation than white noise. The range of frequencies for of the estimated SFD were used for the optimum sampling frequency. Further, the estimated normalized sampling frequency numbers validate the stationarity concepts as discussed above and therefore, only initial five timestamp resolutions are considered. The lower sampling frequency values indicate under sampling while the larger values represent over sampling (Refer: Table 13, Table 17, Table 21, Table 25, Table 29, Table 33, Table 37, Table 41, Table 45, Table 49, Table 53, Table 57, Table 61, Table 65, Table 69, Table 73, Table 77, Table 81, Table 85, and Table 89).

In addition, selected individual time series of thirteen different features (refer subsection 4.2.4) for all the twenty malware instances have been evaluated to measure cognitive complexity and its relationship between malware and normal samples using the multiscale fractal measures of VFD, CFD and IFD as tabulated in Table 14, Table 18, Table 22, Table 26, Table 30, Table 34, Table 38, Table 42, Table 46, Table 50, Table 54, Table 58, Table 62, Table 66, Table 70, Table 74, Table 78, Table 82, and Table 86, and Table 90. As already discussed in subsection 2.6, the measured malware complexity is different from legitimate process tree complexity which is attributed towards their malicious behavior independent of normal dynamics of the operating system.

As can be observed by nodes based feature of CNTS, values of VFD, CFD and IFD for normal samples are greater than that of malware samples for almost all malware samples, which depict a difference of at least 2%. The only exceptions is Nivdort 2, where all fractal dimensions for malware are larger than normal data. In addition, IFD and CFD values for Hupigon 2 and Citadel 2 are greater than the normal data. Also, Citadel 2, Hupigon 1, and Hupigon 2 show a similarly close value for malware and normal samples for VFD which indicate the difficulty in measuring the complexity of malware in differentiating from normal data.

For the feature of TSNN, fractal dimensions i.e. VFD, CFD and IFD values are mostly lower for malware than the normal data with the exceptions of Nivdort 2 and Citadel 2. Also, for the edge based features of ECTS, EMTS, TSET and ETSD, the values of VFD, CFD and IFD are distinctively and consistently lower for malware samples compared to normal samples. In addition, for the features of TSNC, TSNR, TSER, TSEM, NTSE, ETTS and TSNE, the values of VFD, CFD and IFD are not consistently greater or lesser for malware samples which implies an absence of a unique pattern.

It can be safely deduced from the analysis of these tables that whenever malware samples outnumber the normal samples such that the resulting malware to normal sample ratio exceeds 50%, the complexity measures of VFD, CFD and IFD for malware samples becomes greater than that of normal samples. Above analysis also implies that if the inherent complexity of edge and node clusters with respects to malware and normal samples become similar, they will have a similarly closer ratio as well. So, when the normal samples in a dataset are in majority compare to malware samples, they will tend to have higher fractal dimension values and vice versa.

4.5.2 Unsupervised Cognitive Characterization

In this subsection, a detailed empirical analysis of the results of single scale (Euclidean distance) and multiscale (Fractal Dimensions i.e. VFD, IFD, and CFD) based k-means clustering algorithm for the selected feature set consisting of CNTS, TSNN, ECTS, EMTS, ETTS and ETSD across all twenty data instances is provided for the characterization results in Table 15, Table 19, Table 23, Table 27, Table 31, Table 35, Table 39, Table 43, Table 47, Table 51, Table 55, Table 59, Table 63, Table 67, Table 71, Table 75, Table 79, Table 83, Table 87, and Table 91. There are two reasons for the selection of these features; (1) as already shown empirically, these features have shown a tendency to consistently possess a distinct malware fractal dimension which is lower from normal samples thus, exhibiting uniqueness in malware complexity, and (2) these features provide a time window based analysis (as evident from the heat-maps of relevant features in subsection appendix 7.1 and therefore, offers a convenient way for CSOC cyber experts to monitor the possibility of malware activity in near real time at micro level. For the sake of completeness, first time window resolution is selected for this analysis because it is the best resolution available for the experiment.

A summarized version of these selected features for twenty malware instances where they depict an optimum performance with respect to the clustering evaluation criteria of TPR, TNR, FPR, FNR, Accuracy, Precision and F1-Score is tabulated in Table 92 and Table 93. This approach can be used to determine an optimum feature set, which when combined together, provides best analysis option to the CSOC team. It is expected that these features will perform well in the absence of a-priori knowledge about the malware with the assumptions of; (1) malware sample ratio lesser than normal samples ratio (class imbalance property), and (2) malware mimics legitimate behavior to remain stealthy (class inseparability property) and hence, the selection of clustering approach for validation.

For the following discussion, the primary performance evaluation metrics of TPR, TNR, FPR and FNR are given additional considerations as the other three metrics of Precision, Accuracy and F1-score are derived from these. Again, the objective is to determine the feature set which when input to the single scale and multiscale clustering algorithms, optimum values of these evaluation parameters are attained which in other words refers to the accurate determination of malicious time instance. To further elaborate, consider the case of Zeus 1 (i.e. first row of Table 92) for which feature of CNTS is able to optimally cluster the malicious instances represented by a TPR value of 96.23%. In contrast, for Hupigon 1 (i.e. fifth row of Table 92), the maximum TPR is achieved by using the feature of TSNN. Similar deductions can be made for other performance measures. It is worth-mentioning that all these features will be input to the four algorithms simultaneously and in a practical environment, a confidence value will be attached to the results of each of them that will serve as an indicator for the presence of advanced threats in a particular window. For further details, refer subsections 4.5.5 and 4.5.5.

An interesting observation is that node based feature contributed more towards the improvement of TPR and reduction of FNR while mostly edge based features led to the

improvement in TNR and reduction in FPR. As node based features have better class balance compared to edge based features, therefore, clustering performance works well on node based features using VFD fractal similarity measure. Further, mostly Euclidean single scale analysis provided best optimum results for TNR and FPR using edge based features because of the tendency of Euclidean metric to produce characterization results with respect to the majority group. Also, it can be attributed to the fact that edge based features, despite having high class imbalance indicates normal samples (negative samples) better than malware samples and thus, depict a statistical bias towards majority class which are negative samples. Also, it is observed that FPR variability is bounded between 1.46% and 31.33% while FNR variability lies between 1.54% and 18.27%. However, an average variability for FNR is approximately 20% and for FPR it is about 30%.

Another important objective is to discover best performing similarity metric (Euclidean, VFD, CFD, and IFD) in k-means which can be found by a close inspection of the F1-score in Table 93. For almost all twenty malware instances, the optimum F1-score, whose value is an indication of the overall algorithmic suitability (in terms of its performance) for the required objective, is achieved with VFD based k-means algorithm with the exception of Stabuniq Malware – Instance 2 where CFD based k-means outperforms others. Also, it can be deduced that node based features contribute more towards the improvement of F1-score as compared to the edge based features which do not bring any value to this evaluation metric. This is evident from the F1-score where except for the Hupigon Malware – Instance 1, all other instances use a node based feature as an input to the k-means algorithms for the clustering of malicious and normal data instances. This behavior can be attributed to the high class imbalance ratio of the edge based data compared to the more balanced node based data.

It is observed in Table 93 that there may exist a direct relationship between the malware ratio in the feature and F1-score obtained with it. As shown, the best F1-score value of 78.15% is achieved for Proteus Malware – Instance 1, where the malware to normal samples ratio for the node feature of CNTS is approximately 50%. Also, it can be observed that best performing F1 score is measured when node based features are used with VFD as clustering algorithm. F1 score varies from 54.81% to 78.15% whereas the worst situation occurs when node ratio is the lowest i.e. 34% for Carperb Malware – Instance 1. This reaffirms the inference that class imbalance reduces F1 score because on average it increases false alarm rate either due to increase in false positive or false negative rates.

Similar argument can be made to infer the performance pattern observed for precision metric in which optimum performance is achieved with the use of node based features with a multiscale clustering approach. In other words, it can be deduced that using node based features and fractal similarity measures, it is possible to predict a more consistent estimate due to relatively better balanced data of node features compared to that of edge ones. It is especially important for the heavy tailed distributions like the data in hand, where the random variability is much higher and the outliers are abundant. However, it can be observed that VFD is not the only multiscale complexity evaluation approach that brings out the better performance rather other methods like CFD and IFD render good results as well.

Moreover, as for the accuracy metric, which is an indicator of the bias in an estimate, mostly edge based features render optimum performance with a Euclidean measure for characterization. However, there are a few exceptions like Nivdort and Poweliks where node based features provide superior results with fractal based complexity measure such as VFD for characterization. The primary reason for edge based features revealing higher accuracy is because the data for edge based features is highly imbalanced where malware class is under-represented as compared to the normal class which is over-represented and hence, the bias in the results. This bias is further compounded by the use of single scale Euclidean metric which has an averaging effect on the results such that it weighs the majority (normal samples) more heavily which in turn leads to ignoring malware instances which are in minority. In addition, the values for the accuracy measure varies between 58.69% and 96.28% with most of them in lies in the range of 70%.

Table 92: Best performing evaluation metrics (TPR, TNR, FPR, FNR) of each data set with their K-means measures and features.

No	Malware	Node Malware Ratio	Edge Malware Ratio	K-means	Feature	TPR (%)	K-means	Feature	TNR (%)	K-means	Feature	FPR (%)	K-means	Feature	FNR (%)
1	Zeus 1	38.4	2.1	VFD	CNTS	96.23	Euclid.	TSNN	98.02	Euclid.	ETTS	1.98	VFD	CNTS	3.77
2	Zeus 2	39.6	2.1	VFD	CNTS	90.38	Euclid.	ECTS	79.43	Euclid.	ECTS	20.57	VFD	CNTS	9.62
3	Citadel 1	40.3	6.0	VFD	CNTS	95.92	Euclid.	ETTS	79.33	Euclid.	ETTS	20.67	VFD	CNTS	4.08
4	Citadel 2	53.4	6.0	VFD	CNTS	83.93	IFD	ECTS	77.78	IFD	ECTS	22.22	VFD	ECTS	16.67
5	Hupigon 1	47.9	3.0	VFD	TSNN	86.57	Euclid.	TSNN	83.39	Euclid.	TSNN	16.61	VFD	TSNN	13.43
6	Hupigon 2	48.0	6.9	VFD	TSNN	86.25	Euclid.	ETSD	79.29	Euclid.	ETSD	20.71	VFD	TSNN	13.75
7	Zurgop 1	47.2	4.1	VFD	TSNN	95.95	Euclid.	ECTS	99.30	Euclid.	CNTS	23.95	VFD	TSNN	4.05
8	Zurgop 2	39.8	5.0	VFD	CNTS	96.08	Euclid.	ETTS	98.26	Euclid.	ETTS	1.74	VFD	CNTS	3.92
9	Carperb 1	34.2	2.0	VFD	TSNN	84.09	Euclid.	TSNN	76.07	Euclid.	ETTS	23.93	VFD	TSNN	15.91
10	Carperb 2	37.7	2.1	VFD	CNTS	88.24	Euclid.	ECTS	78.73	Euclid.	ECTS	21.27	VFD	CNTS	11.76
11	Alina 1	34.0	4.6	VFD	CNTS	90.54	IFD	TSNN	87.07	IFD	TSNN	12.93	VFD	CNTS	9.46
12	Alina 2	41.8	4.1	VFD	CNTS	81.73	Euclid.	EMTS	79.51	Euclid.	EMTS	20.49	VFD	CNTS	18.27
13	Proteus 1	49.3	4.1	VFD	CNTS	89.39	Euclid.	ECTS	78.92	Euclid.	ECTS	21.08	VFD	CNTS	10.61
14	Proteus 2	43.2	6.8	VFD	CNTS	98.08	Euclid.	ETTS	94.54	Euclid.	ETTS	1.46	VFD	CNTS	1.92
15	Stabuniq 1	37.1	3.8	VFD	CNTS	98.46	Euclid.	TSNN	92.50	Euclid.	TSNN	7.50	VFD	CNTS	1.54
16	Stabuniq 2	38.9	3.4	VFD	CNTS	92.31	Euclid.	EMTS	78.98	Euclid.	EMTS	21.02	VFD	CNTS	7.69
17	Nivdort 1	43.4	16.9	Euclid.	CNTS	90.94	CFD	CNTS	82.43	CFD	CNTS	17.57	Euclid.	CNTS	9.06
18	Nivdort 2	55.7	24.8	VFD	CNTS	92.54	Euclid.	ETSD	79.32	Euclid.	ETSD	20.68	CFD	TSNN	5.97
19	Poweliks 1	37.9	6.5	VFD	CNTS	97.73	Euclid.	CNTS	90.74	Euclid.	CNTS	9.26	VFD	CNTS	2.27
20	Poweliks 2	42.1	4.6	VFD	CNTS	98.11	Euclid.	TSNN	68.67	Euclid.	TSNN	31.33	VFD	CNTS	1.89

Table 93: Best performing evaluation metrics (Precision, Accuracy and F1 score) of each data set with their K-means measures and features.

No	Malware	Node Malware Ratio	Edge Malware Ratio	K-means	Feature	Precision (%)	K-means	Feature	Accuracy (%)	K-means	Feature	F1 (%)
1	Zeus 1	38.4	2.1	IFD	TSNN	69.23	Euclid.	ETTS	96.28	VFD	CNTS	69.86
2	Zeus 2	39.6	2.1	CFD	TSNN	57.14	Euclid.	ECTS	78.33	VFD	CNTS	67.63
3	Citadel 1	40.3	6.0	IFD	TSNN	59.18	Euclid.	ETTS	74.85	VFD	CNTS	70.68
4	Citadel 2	53.4	6.0	VFD	CNTS	66.20	IFD	ECTS	76.04	VFD	CNTS	74.02
5	Hupigon 1	47.9	3.0	VFD	TSNN	55.24	Euclid.	ETTS	77.78	VFD	ECTS	67.44
6	Hupigon 2	48.0	6.9	VFD	TSNN	57.50	Euclid.	ETSD	75.73	VFD	TSNN	69.00
7	Zurgop 1	47.2	4.1	VFD	TSNN	60.17	Euclid.	ECTS	94.00	VFD	TSNN	73.96
8	Zurgop 2	39.8	5.0	IFD	TSNN	53.13	Euclid.	ETTS	93.39	VFD	TSNN	68.00
9	Carperb 1	34.2	2.0	VFD	TSNN	40.66	Euclid.	ETTS	75.32	VFD	TSNN	54.81
10	Carperb 2	37.7	2.1	VFD	CNTS	58.44	Euclid.	ECTS	77.68	VFD	CNTS	70.31
11	Alina 1	34.0	4.6	IFD	TSNN	62.50	Euclid.	ECTS	76.84	VFD	CNTS	59.03
12	Alina 2	41.8	4.1	IFD	TSNN	61.29	Euclid.	EMTS	77.35	VFD	CNTS	64.64
13	Proteus 1	49.3	4.1	VFD	CNTS	69.41	Euclid.	ECTS	76.87	VFD	CNTS	78.15
14	Proteus 2	43.2	6.8	VFD	CNTS	62.20	Euclid.	ETTS	89.25	VFD	CNTS	76.12
15	Stabuniq 1	37.1	3.8	VFD	CNTS	57.66	IFD	ECTS	66.42	VFD	CNTS	72.73
16	Stabuniq 2	38.9	3.4	CFD	TSNN	48.84	Euclid.	EMTS	77.05	CFD	TSNN	60.87
17	Nivdort 1	43.4	16.9	CFD	CNTS	58.06	VFD	CNTS	58.70	VFD	CNTS	63.23
18	Nivdort 2	55.7	24.8	VFD	CNTS	67.39	VFD	CNTS	69.03	VFD	CNTS	77.99
19	Poweliks 1	37.9	6.5	IFD	CNTS	59.09	CFD	ECTS	66.33	VFD	CNTS	69.92
20	Poweliks 2	42.1	4.6	VFD	CNTS	55.32	VFD	CNTS	61.95	VFD	CNTS	70.75

Another way to analyze this situation is by counting the occurrences of VFD based k-means as an optimum clustering algorithm for each evaluation criteria across all malware instances. It is observed that VFD based k-means is effective in improving the TPR where using it as a similarity metric produces optimum results for 90% of the time. This in turn is connected to the FNR where its utilization produces minimum FNR value for 95% of the time. On the other hand, VFD algorithm is not effective in decreasing FPR or consequently improving TNR as evident from Table 92. Instead, either single scale Euclidean distance based k-means or IFD and CFD based clustering schemes are more successful for achieving optimum FPR and TNR. However, it can be argued that the better TNR values are due to the bias of the other approaches towards assigning every sample to the negative cluster or the majority class. This is also obvious with the accuracy measure where Euclidean metric dominatingly exhibits relevant performance. The simple fact that negative (normal) samples are in majority and their correct identification irrespective of the accurate clustering of malicious samples can lead to higher accuracy values is the primary rationale behind the superior performance of single scale measure which are biased toward the majority class while ignoring the minority class. Likewise, better precision which deals with the lesser variation in the output is achieved with multiscale fractal measures.

Following are the key takeaway points from the above discussion:

1) The most suitable similarity metric to be used in k-means based clustering is VFD which is multiscale in nature and is therefore, able to trace the stealthy malware activity in a process tree graph. The combined analysis of variance at different scales reveal the delicate changes in the system which otherwise are not discovered by single scale Euclidean metric

due to the averaging effect and the class inseparability issue. This superior discriminatory property of VFD is already visually established in Figure 57 to Figure 62.

2) Better performance in terms of accuracy measure is driven by the correct clustering of majority class which is easily achieved by single scale k-means. Therefore, emphasis on this metric only may lead the system to ignore minority samples thus, producing biased results.
3) Better precision values are attainable by the consistency of the algorithm in its clustering approach and multi scale k-means which may use VFD, CFD or IFD similarity metric depicts better results.
4) Node based features contribute more towards the improvement of F1-score which is directly dependent on TPR where again node based features dominate the optimum performance.
5) Edge based features plays an important role in achieving maximum accuracy values which is dependent on correct clustering of normal samples. It is therefore related to the optimum TNR values as well which are mostly achieved by edge based features as observed in experiments.

4.5.3 Significance of the Proposed Characterization

Considering the contribution of node and edge based features towards the improvement of TPR and TNR respectively as discussed in previous sub-section, it can be established that if node based features are processed through VFD based clustering algorithm and edge based features are processed through single scale based Euclidean clustering algorithm simultaneously, it is possible to detect the presence of a zero-day malware with high confidence. Further, if the objective of a CSOC is to reduce false positives (during threat investigation/forensics), edge based features can serve the purpose. However, if the objective is to reduce FNR and detect zero day threats (such as threat hunting), then node based features can be an effective candidates to achieve optimum threat hunting using unsupervised clustering. Therefore, the proposed characterization technique can be embedded as a cognitive intelligent tool for threat hunting particularly for the case of mutating malware. Further, edge and node based features using VFD and Euclidean clustering mechanisms can be further embedded together in a weighted decision making system (ensemble machine learning) to provide both threat hunting and investigation together. A use case of this methodology is described in subsections 4.5.4 and 4.5.5.

As already mentioned in subsection 2.5.3, cognitive load of processing alerts in a CSOC is already above 50% to manage false alerts. It is observed that the proposed Malvidence framework provides better performance in terms of reducing both false positives and false negatives simultaneously. Based on empirical results, the false positives rate is in the range of 30% and false negatives rate is less than 20%. Compared to existing manual methodologies, Malvidence framework is able to reduce both false alerts by more than 40% (where manual methods generates more than 50% false alerts) and is also an cognitive intelligent method, which relieves CSOC experts from manual analysis of each event.

4.5.4 First Use Case of the Proposed Malware Characterization Framework in CSOC

A cyber security operations center (CSOC) is a centralized facility in an organization to monitor, investigate and respond to cyber threats [430]. A CSOC is different from network operations center (NOC) which is responsible for managing network connectivity and ensuring smooth operations of computing infrastructures e.g. installation of software, maintaining network links and server administration. A CSOC employs cyber security experts such as incidence response (IR) teams, threat intelligence (TI) and forensic experts, firewall managers and penetration testers. CSOC personnel are responsible for mitigating any cyber threat and are the major line of defense against any cyber event.

The recent evolution of cyber security from a traditional network based security facility (packet based firewalls, IDS and IPS) to a mix of network and host based cyber security facility has provided major benefits to CSOC experts in terms of better visibility and investigation capabilities. Now it is possible to detect symptoms of threats using network traffic first and then drill down to the individual host and user level using various rules and event management systems. These symptoms of threats are also known as indicator of threats and can represent a compromise (indicator of compromise) or attack (indicator of attack). These indicators are based on rule configurations of various cyber devices such as firewalls, network and host based intrusion detection systems. If a rule is triggered, a relevant indicator will appear over the CSOC SIEM device. These rules provide a filter to a chain of events (such as network packets or host data) and are typically part of an event stream management (SIEM) of a cyber-security device. An event is any cyber object of interest that requires configuration of the cyber security device. For example, a rule can be configured to stop an event which is defined by an ingress flow of IP traffic from a source address 192.168.0.1 using HTTP protocol. Therefore, configuring a firewall rule to deny HTTP traffic from 192.168.0.1 will block any event generated from this source IP and protocol. Similarly, events can be defined for host based operating system which are further processed in a rule based host intrusion detection system (HIDS). For example, an event can be defined to user login activity in an operating system and a rule can be defined such that it block any unauthorized user login if it exceeds 3 consecutive attempts. These events are sent as operations system logs to CSOC SIEM devices so that CSOC experts can monitor and investigate these logs.

As shown in Figure 63, a connectivity diagram of SIEM device [431] [432] is shown. There are two types of events namely host based events and network based events. Therefore, there is a middleware system of servers called data collector that collects host events and network events in separate servers. These collector systems can be any proprietary or open source technology that is responsible for efficient scalable, and optimized collection of events such as ELK (Elastic Search, Log Stash and Kabana) [433]. Collectors are responsible for low level processing of events for SIEM operations. Afterwards these events are sent to a centralized aggregator that is responsible for providing indexing and searching service for SIEM device. Aggregators are supported by various log storing and management mechanisms such as syslog servers. Afterwards, a Graphical User Interface is provided to the CSOC users for investigation, analysis and response purpose. Malvidence framework can be integrated with the log servers to characterize host events processed

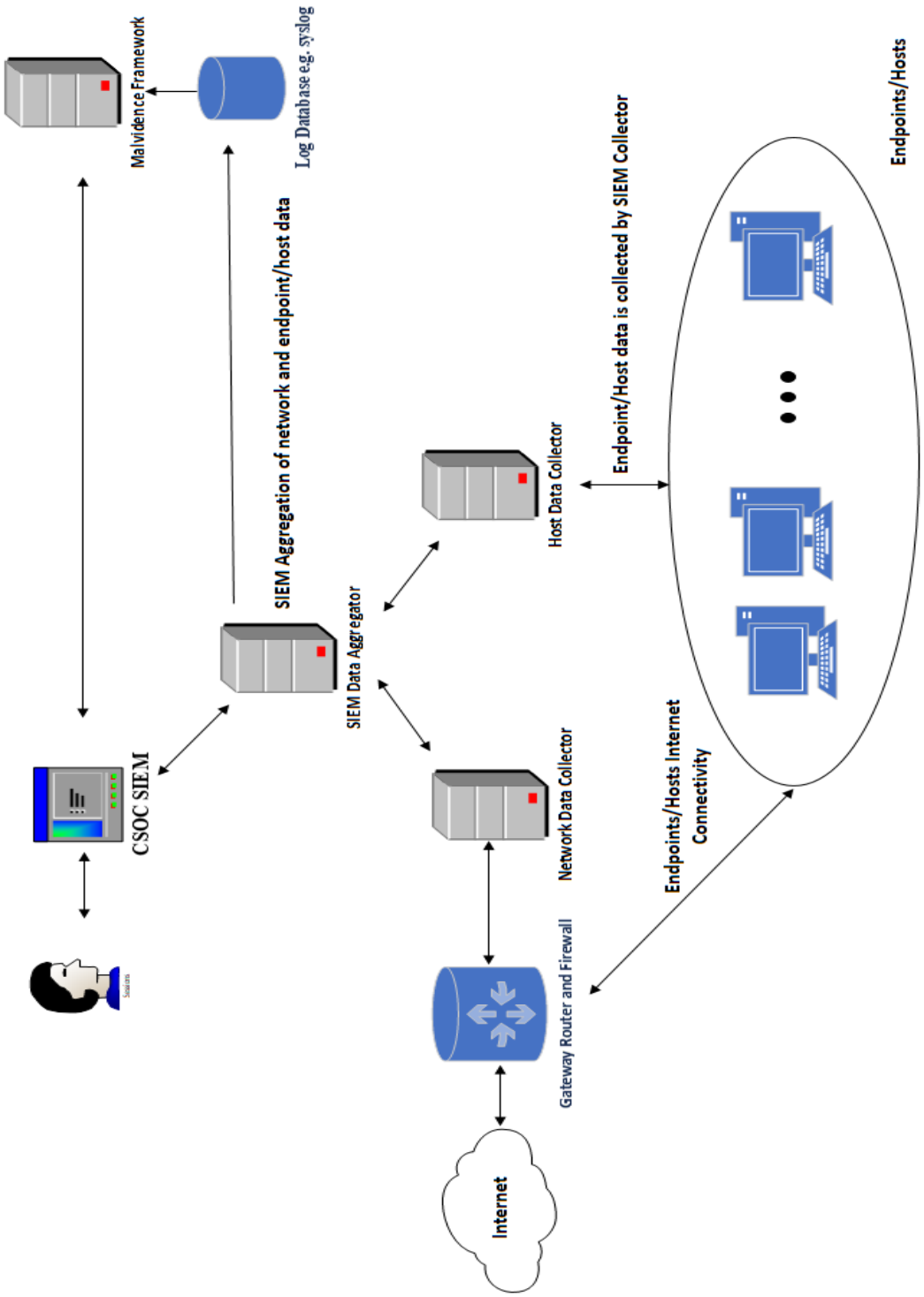


Figure 63: SIEM connectivity diagram and Malvidence framework.

by collectors and aggregator and can be configured for threat hunting purpose. This integration will offload the data acquisition and processing load to SIEM collector and aggregator and will optimize implementation performance of characterization.

4.5.5 Second Use Case of the Proposed Malware Characterization Framework

In this section, a practical use-case study of the proposed malware characterization framework is presented. This study serves as a recommendation of one possible application of the proposed work and does not cover other possible cases exhaustively.

As Cyber Security Operation Center (CSOC) experts analyze large volumes of alerts generated from heterogeneous data sources such as endpoint hosts, network monitoring devices, and databases, therefore, a CSOC expert is faced with large volume of alerts (alarms) which adds up the cognitive load on human in terms of analysis and reliable detection. In this situation, there is a high probability of missing a true alert.

As shown in Figure 64, a conceptual model with possible data flow diagram is shown for the proposed malware characterization framework. Following are the proposed steps to use the framework in a CSOC environment:

1) Step 1: A network of Windows 7 based endpoints is connected to the Internet in an organization. Organization has implemented various cyber security measures including but not limited to network firewalls, IDS/IPS and antimalware technologies. In this step, an advanced cyber kill chain is executed by an intelligent adversary using a mutated malware payload which is successfully delivered to the given endpoint bypassing existing cyber defenses.
2) Step 2: The proposed data acquisition sandbox is implemented. It has two components; (i) Sandbox agent installed on the Windows 7 endpoint systems which is collecting high resolution process tree information and is sending this data set to the Sandbox server after a certain interval of time using data pipes. In this step, the sandbox server is processing the operating system process tree which is populating a database in a Syslog server having the required data attributes as proposed in this dissertation.
3) Step 3: There is a SIEM management layer between the Sandbox and the Malvidence framework. This layer is responsible for ensuring optimum performance and scalability features (data collectors and aggregators) by using advanced processing technologies such as Hadoop, Spark and ELK.
4) Step 4: The proposed framework is transforming the process tree events into time graphs continuously which are subsequently sent to the graph extraction module to extract the proposed node and edge based features. These features are divided into 2 sets; (i) Feature set 1, which includes CNTS, TSNN, ECTS, EMTS, ETTS, ETSD, which are used for clustering for malware characterization, (ii) Feature set 2, which includes TSET, TSNE, TSER, TSEM, NTSE, TSNC, TSNR. These features are used for validating the integrity of the first set of features.

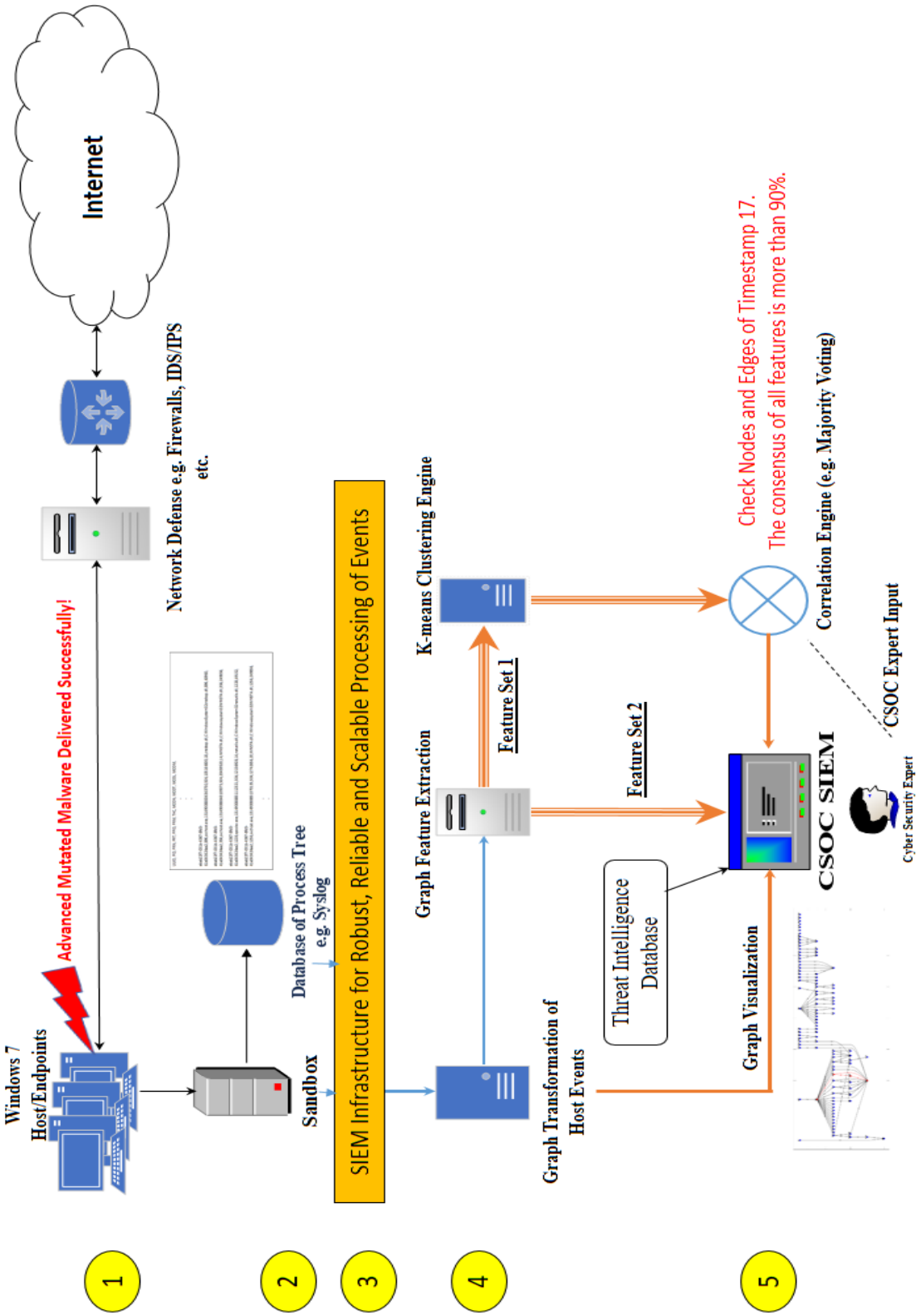


Figure 64: Use Case - Proposed malware characterization framework in a Cyber Security Operation Center.

5) Step 5: In this step, a CSOC expert can visualize the time graph of particular events on its security dashboard which may be a SIEM console and can see the proposed characterization of feature set 1. Further, the expert can also access feature set 2. The results of the characterization of feature set 1 are fused using any data aggregation and correlation technique to provide a level of confidence to the results. For example, according to equation (46), a linear combination of the normalized features using user-defined weights α_i (where $i = 1,2,3, \dots$) can be a proposed model which is already suggested in [1]. As shown in Figure 64, suggested output of the correlation engine as per user configured equation (46) would be able to provide a probability (p) metric for a particular time instance in the time graph alerting the expert to further evaluate each node and edge in that time window. If the time resolution has lower time windows, then the expert only need to check a few nodes and their edges of the time window to figure out if the process and modules are malicious or not. Increasing time window size, will increase the graph nodes and edges and thus the complexity of analysis, which will overload the analyst cognitively. Using a threat intelligence and situational awareness database, those processes can be attributed with high confidence.

$$p = \alpha_1 \mathrm{CNTS} + \alpha_2 \mathrm{TSNN} + \alpha_3 \mathrm{ECTS} + \alpha_4 \mathrm{EMTS} + \alpha_5 \mathrm{ETTS} + \alpha_6 \mathrm{ETSD} \quad (46)$$

$$\sum_{i=1}^{6} \alpha_i = 1 \quad (47)$$

6) In sum, using fractals, a combined macro and micro analysis is done on each feature concurrently and thus provides a measureable and bounded metric to evaluate and indicate the exact malicious node/edge in the relevant time window which represents actual processes and their relationships inside an operating system process tree.

To keep perspective, average time to deploy and fine-tune CSOC SIEM solutions is 6 months [434], therefore, the proposed characterization method will take at least 6 months (or more) to configure the confidence interval based on the ensemble algorithm selected with the assumption that scalability optimization is achieved with efficient implementation schemes such as using Hadoop or Spark based hyper parallelization techniques.

5. Conclusions

This section concludes the dissertation by elaborating the key points in the following two subsections:

Subsection 5.1 Contributions

In this subsection, a summary of the main contributions of this dissertation work is summarized.

Subsection 5.2 Summary of Conclusions

In this subsection, conclusive remarks for each of the research question will be established.

Subsection 5.3 Limitations and Future Work

In this subsection, limitations of the proposed Malvidence characterization framework and the research work are provided. These limitations are based on the premise that this research is expected to serve as a proof of concept framework or methodology and is not limited to any particular underlying technology. Each limitation is followed by a proposed extension of this work in the future.

5.1 Contributions

This subsection concludes the research, study and analysis of this dissertation and addresses the formal research questions and problem definition in subsection 1.2. In this work, a graph based cognitive analysis framework called Malvidence is proposed to characterize mutated malware using fractal based clustering approaches. This approach utilizes multiple time graph based features to not only improve the cognitive performance of clustering based machine intelligence algorithms but also helps reduce the cognitive analysis load of a human cyber expert.

Following are the key contributions of this dissertation:

1) The proposed Malvidence framework claims to contribute the following:
    a. A new cognitive cyber kill chain based threat analysis model is proposed to address the limitations of the existing cyber kill chain where analysis is based on traditional sequential evaluation of the threat stages. The proposed model reduces the seven stages into four stages with the concurrent analysis of Reconnaissance, Delivery, Persistence and CnC stages in an iterative way. At each time step of the proposed iteration, the proposed kill chain stages are analyzed altogether because the indicators of threats can reveal multiple stages of the progression of an attack. Therefore, this model supports threat hunting approaches since it introduces the analysis of four stages in a continuum fashion. Further, the cognitive analysis framework on malware in this work supports this kill chain analysis by analyzing and characterizing multiple features as proposed in the use case.
    b. To the best of my knowledge, the proposed cognitive time graph based complexity analysis of the operating system process tree dynamic behavior to characterize mutated malware is not presented by any publicly available research or industrial work yet; therefore, contributes to the claims of this dissertation. This graph based analysis is validated using mathematical statistical analysis which is subsequently investigated to characterize malware objects. Using this statistical approach, an autonomous feature extraction and malware characterization process is proposed which is intended to reduce the cognitive analysis load of human cyber experts as shown in the use case study. Further, process trees constitutes a fundamental working principle of an operating system and this analysis does not preclude the application of the proof of concept provided in this dissertation for other operating systems. Therefore, this work provides an overarching guideline in developing a proposed analysis framework for any operating system. Therefore, this framework is unique and new in the research community.
    c. The proposed analytical framework identifies multiple features based on the nodes and edges of the process tree time graph. These features are used to perform a first level of cognitive characterization and a statistical analysis shows that a subset of these features (CNTS, TSNN, ECTS, EMTS, ETTS and ETSD) can be used consistently to differentiate malware uniquely form normal processes. Note that this work does not claim to provide a silver bullet solution as malware deception techniques are being evolved continuously. However, with the proposed cognitive

analysis framework, it is possible to use different features for characterization of a particular subset of mutating malware families which is better in performance than using signature based or known behavior based machine learning mechanisms for individual malware, which require continuous human analysis and is not reliable for unknown malware objects. Further, Malvidence framework for malware characterization provides sufficient cognitive tools and methodologies which can be subsequently used in any cyber detection mechanism such as CSOC, IDS, firewall and anomaly detection.

d. This dissertation provides a working proof of concept of the applicability and validity of cognitive fractal algorithms in analyzing and characterizing unknown mutating malware inside an operating system process tree using a set of features extracted from the transformed time graph of the process tree data set. Although, fractal algorithms have been researched for many years, but using fractals in characterization of malware in a Windows 7 operating system is not reported in the published literature yet. Using fractals and the graph features, the malware activities, which are mutating inside an operating system process tree, are characterized uniquely. This uniqueness is driven by the statistical self-similarity extracted by simultaneous micro and macro level analysis of the relevant fractal analysis of the features. This analysis captures inherent complexity of the malware activities, which are different from normal operating system process tree mechanism. Further, it is also shown that VFD is better in performance due to the Hurst parameter which captures changes in multiscale variance better than other statistical measures. Also, as observed through empirical results on both mathematical fBm dataset and real world malware data sets, VFD outperforms single scale Euclidean based clustering algorithm in detecting unknown mutating malware. To the best of my knowledge, this has not been reported in the cyber security literature, and, as such, it is a novel and significant contribution.

2) The proposed Malvidence framework addresses the challenge of class inseparability due to mutation in malware and despite having inseparability over a particular feature at single scale, characterization using fractal measures at multiple scales shows that it is possible to sufficiently extract behavior of malware from normal processes. In this work, class inseparability of the mutating malware is shown using thirteen different features and shows that using single scale machine intelligence techniques e.g. k-means, it is not possible to detect the presence of unknown malware which renders mutation to evade detection. Further, visualization of these features for each malware data set also empirically proves that a cyber-expert cannot detect such malware using visual cues or manual thresholding techniques using traditional single scale methods. However, using multiscale based fractal techniques, these class inseparable (mutating) malware can be characterized uniquely which is due to the fact that malware processes introduces complexity which is different from normal complexity of the legitimate process tree and therefore, fractals identify malware complexity by analyzing malware behavior both at macro and micro level simultaneously.

3) This research contributes a data set of twenty mutated malware instances and serves as a foundational ground for the proposed analysis and the malware characterization framework. This data set is generated in a controlled experimental environment and malware activities are labelled based on observed attribute in the data set. There is no such data set available in the research community and therefore, contributes to the claims of this dissertation. Also, the process tree data set shows heavy tailed distribution which is evident for both normal and malware processes and their relevant modules. Therefore, it also warrants the analysis of cognitive complexity based fractal analysis due to the presence of complex long range correlation and self-similarity in the dataset.

4) Most of the traditional and single scale machine learning mechanisms can either reduce false negatives or false positives. This dissertation claims to address the challenge of improving both false negatives and false positives concurrently using a set of multiple features for mutating malware. As shown in the results, with a single feature, it is not possible to address this challenge. However, using a complexity based analysis applied on multiple features separately and then aggregating the analysis results has shown to improve both false positives and false negatives concurrently in characterizing a malware instance inside an operating system process tree. As shown in the use case section, this will help CSOC experts in reducing cognitive load of analyzing false alerts in near real time and improving their security postures by performing intelligent analysis quickly so that the opportunity window for malicious threat actors is reduced in terms of launching another wave of attacks by distracting the cyber security experts due to false alerts.

5) This dissertation also contributes a comprehensive study of the available research and industrial malware detection toolboxes and contributes to develop a taxonomy of such tools and techniques with their limitations in detecting malware mutation. This taxonomy directs the research to understand the concept of complexity and subsequently generates the need to analyze and differentiate complexity of malware behavior from normal behavior.

5.2 Summary of Conclusions

This subsection provides conclusions to the formal research questions posed in the subsection 1.2.1 as follows:

1) Can cognitive complexity measures be used to distinguish objects from an overlapping set of objects? A corollary of this question would be: Is it possible that mutating malware behavior can be distinguishable from legitimate behavior?

As observed in the sub-sections 4.3, 4.4 and 4.5, advanced mutating malware behavior is inseparable from normal behavior on individual graph features. However, multiscale fractal based VFD, CFD and IFD analysis provide higher fractal dimensions for normal process behavior than malware behavior. Further, VFD provides high resiliency against variations than CFD and IFD. Therefore, fractal based multiscale cognitive complexity analysis is able to discriminate malware behavior distinctively from normal behavior on all malware data set.

2) Is there a unique set of features that can be used for characterizing mutating malware behavior reliably and demonstrates better generalization capabilities?

As observed in the sub-section 4.5, there is no single feature that can provide better discriminatory characterization of mutating malware behavior. However, most suitable metric for k-means clustering is VFD as it is able to successfully identify mutating malware activity which is inseparable from normal behavior on single scale analysis. Further, single scale Euclidean based k-means is most suitable for accuracy measure as it is driven by majority class due to bias. Also, multiscale (VFD, IFD, CFD) measures are suitable for precision measure as it depends on the consistency of the clustering algorithmic approach. In addition, node based feature contribute more towards the improvement of F1 score and is directly dependent on TPR. Finally, edge based features contribute more towards improving the accuracy due to their direct dependence on TNR.

3) Given the limitations of conventional methods of analyzing cyber threats, is there a way to improve the modeling of mutated malware and to reinforce reliability in cyber forensic analysis?

No, conventional cyber kill chain analysis is not effective in the onslaught of advanced and intelligent mutating malware due to lack of analysis of persistence and multiple kill chain effects. Therefore, a new cognitive and concurrent cyber kill chain is proposed that modifies the 7 stages of traditional sequential cyber kill chain into a temporal and four stage cyber kill chain. Due to time based analysis, it addresses the correlation of various temporal events and thus addresses the effects of multiple cyber kill chain. Further, it adds a persistence stage in the analysis.

4) What are the data driven challenges of cognitive computing in mutating malware characterization?

As mentioned in the sub-section 2.5, there are two major challenges of mutating malware characterization; (1) class imbalance, and (2) class inseparability. The challenge of class imbalance is addressed by using node based features which provide better class balance compared to edge based features. The challenge of class inseparability is addressed using multiscale fractal analysis

that provides an elegant mechanism to distinguish hidden malware activities using non-integer fractal dimensions.

5) What is the appropriate data set of an operating system that can be used to ensure full visibility on malware and normal activities?

Computer operating systems provide various level of abstraction for the end users including low and high (application) levels. However, the invariance is the visibility of all activities using process tree data. Any program or software that executes inside an operating system will be attached to a process of an operating system, and will therefore be analyzed by Malvidence framework for possible malware activities.

6) Can we reliably characterize activities of new (zero-day) malware in a host operating system?

Malvidence framework provides elegant mathematical and cognitive computing based mechanism to analyze the activities of malware on multiple scales. As demonstrated in the results section and the use cases, using both node and edge based features will help providing a high confidence interval indicator of a mutating malware activity using multiscale analysis.

5.3 Limitations and Future Work

Some limitations of the proposed cognitive malware characterization framework called Malvidence are mentioned as follows:

1) The design and the corresponding development of the proposed characterization model is carried out for Microsoft Windows 7 desktop operating system. Assuming that the basic operating system level implementation details in terms of process tree structure remain same across different Windows distribution, it is expected that similar performance can be obtained. However, as this research work serves as a proof of concept, this experimental validation is out of the scope of this work.

2) There are other computer operating systems available in the market such as Linux/Unix, Android, QNX, iOS and macOS, to name a few, which are different in their technological implementation but may have similar operating system principles. This implies that they may have a different process tree structure (e.g. process dependencies) and the proposed Malvidence data acquisition framework for the sandbox will need corresponding modifications in the implementation. Nevertheless, the procedure of the feature extraction, aggregation and analysis for malware characterization will hold valid for each process tree across different OS. Moreover, the principles and claims of cognitive characterization using multiple features and their statistical analysis are expected to hold valid as well.

3) The threat model for this framework disregard certain stages of the cyber kill chain which can be included in the analysis to improve the performance. An important aspect of this proposition is to use Command and Control (CnC) server communications with the infected host to decipher exfiltration event which is left as an extension of this work in the future.

4) For this work, the collected network information of the process tree was not considered. Nevertheless, as a future objective it can be used independently and to correlate the results between host and network to achieve better performance holistically. Additionally, it will require extension of this design to incorporate extraction of network based features and their related analysis.

5) This model is applied on the characterization of mutated attacks which mimic normal behavior and therefore are inherently complex. It is not tested to identify threats which are simpler and can be uniquely distinguished from the normal behavior easily such as replicating (non-mutating) viruses and worms.

6) The proposed Malvidence characterization framework is evaluated for a single user operating system environment with complete administrative privileges and there may

be some changes in process tree behavioral activity with multi user considerations due to varying degree of administrative policy enforcement which can be explored further.

7) The average time to generate complete set of space and time graph for each malware dataset is 58 hours on Intel Quad core machine with 16GB of RAM. Although, the optimization of implementation aspects of this system is not part of the presented work, it can be considered as a future work to convert it into a market-ready product by using Hadoop, Spark and other big data technologies to process data in near real time. Further, possibilities of using reconfigurable FPGA (Field Programmable Gate Arrays) or reconfigurable ASIC (Application Specific Integrated Circuits) can be explored to implement this framework in real time.

8) The proposed Malvidence characterization framework tested k-means based clustering schemes, however, there are other unsupervised learning methodologies and semi-supervised techniques with reinforcement learning which can be explored as a future task.

9) The proposed Malvidence framework provides empirical cyber threat hunting analysis. There is a vase domain of cognitive intelligence research and efforts are being undertaken to formulate mathematical algebra such as real time algebra to formally describe system architecture, static and dynamic behaviors. Further, there is a large mathematical knowledge base in the research of semantic analysis and morphism in software engineering. The Mavlidence framework can be extended to develop mathematical foundations and theoretical models.

6. References

[1] Muhammad Salman Khan, Sana Siddiqui, Robert D. McLeod, Ken Ferens and Witold Kinsner, "Fractal based adaptive boosting algorithm for cognitive detection of computer malware," in *proc. of IEEE Intl. Conference on Cognitive Informatics and Cognitive Computing (ICCI*CC)*, Stanford University, CA, USA, Aug. 2016.

[2] Muhammad Salman Khan, Sana Siddiqui and Ken Ferens, "A cognitive and concurrent cyber kill chain model," in *Computer and Network Security Essentials Book*, Springer International Publishing AG, Aug. 2017, pp. 585-602.

[3] Sana Siddiqui, Muhammad Salman Khan and Ken Ferens, "Cognitive computing and multiscale analysis for cyber security," in *Computer and Network Security Essentials Book*, Springer International Publishing AG, Aug. 2017, pp. 507-519.

[4] Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "Multifractal singularity spectrum for cognitive cyber defence in Internet time series," *International Journal of Software Science and Computational Intelligence*, vol. 7, no. 3, pp. 17-45 , Jul 2015.

[5] Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "A chaotic complexity measure for cognitive machine classification of cyber-attacks on computer networks," *International Journal of Cognitive Informatics and Natural Intelligence*, vol. 8, no. 3, pp. 45-69, Jul. 2014.

[6] Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "A chaotic measure for cognitive machine classification of Distributed Denial of Service attacks," in *proc. of 2014 IEEE 13th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC 2014)*, Southbank University, London, UK, Aug. 2014.

[7] Muhammad Salman Khan, Sana Siddiqui, Ken Ferens and Witold Kinsner, "Spectral Fractal Dimension Trajectory (SFDT) to measure complexity of malicious attacks," in *proc. of the Intl. Conference on Security and Management (SAM'16), WorldComp'16*, Nevada, USA, 2016.

[8] Sana Siddiqui, Muhammad Salman Khan and Ken Ferens, "Multiscale Hebbian neural network for cyber threat detection," in *proc. of 2017 IEEE Intl. Joint Conference on Neural Networks (IJCNN)*, May 2017.

[9] Sana Siddiqui, Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "Fractal based cognitive neural network to detect obfuscated and indistinguishable Internet threats," in *proc. of IEEE Intl. Conference on Cognitive Informatics and Cognitive Computing (ICCI*CC)*, Jul. 2017.

[10] Muhammad Salman Khan, Sana Siddiqui and Ken Ferens, "Using information fractal dimension as temperature in restricted Boltzmann Machine," in *proc. of IEEE2017 International Joint Conference on Neural Networks*, Anchorage, AK, USA, May 2017.

[11] Sana Siddiqui, Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "Detecting advanced persistent threats using fractal dimension based machine learning classification," in *proc. of the 2016 ACM on International Workshop on Security And Privacy Analytics, CODASPY'16*, New Orleans, Louisiana, USA, Mar. 2016.

[12] Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "A cognitive multifractal approach to characterize complexity of non-stationary and malicious DNS data traffic using adaptive sliding window,"

in *proc. of IEEE 14th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC 2015)*, Beijing, China, Jul. 2015.

[13] Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "A polyscale based autonomous sliding window algorithm for cognitive machine classification of malicious Internet traffic," in *proc. of International Conference on Security and Management (SAM), WordComp 2015*, Nevada, USA, Jul. 2015.

[14] Muhammad Salman Khan, Sana Siddiqui and Ken Ferens, "Cognitive modeling of polymorphic malware using fractal based semantic characterization," in *proc. of IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, USA, Apr. 2017.

[15] Eric M. Hutchins, Michael J. Clopperty and Rohan M. Amin, "Intelligence-driven computer network defence informed by analysis of adversary campaigns and intrusion Kill Chains," in *proc. of the 6th International Conference on Information Warfare and Security*, Washington, DC, USA, Mar. 2011.

[16] NTT Group Security, "Global Threat Intelligence Report 2017," NTT Group Security, 2017.

[17] Stefan Achleitner, Thomas La Porta, Patrick McDaniel, Shridatt Sugrim, Srikanth V. Krishnamurthy and Ritu Chadha, "Cyber Deception: Virtual networks to defend insider reconnaissance," in *proc. of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, Vienna, Austria, Oct. 2016.

[18] PhishMe , "Q1 2016 sees 93% of phishing emails contain ransomware," Cofense, 4 Jun. 2016. [Online]. Available: https://cofense.com. [Accessed 19 May 2017].

[19] Stephen Cobb and Andrew Lee, "Malware is called malicious for a reason: The risks of weaponizing code," in *proc. of 2014 6th IEEE International Conference On Cyber Conflict*, Tallinn, Estonia, Jun. 2014.

[20] Cammy Harbison , "New ransomware installers can infect computers without users clicking anything, say researchers," iDigitalTimes, 29 Mar 2016. [Online]. Available: http://www.idigitaltimes.com. [Accessed 24 Jan. 2017].

[21] Darlene Storm, "Dogspectus: Android ransomware silently installs, demands $200 iTunes gift card ransom," Computerworld from IDG, 25 Apr. 2016. [Online]. Available: https://www.computerworld.com. [Accessed 24 Nov. 2017].

[22] Tarun Yadav and Rao Arvind Mallari, "Technical aspects of cyber kill chain," in *proc. of International Symposium on Security in Computing and Communication*, Kochi, India, Jun. 2016.

[23] NIST, "National Vulnerability Database," DHS/NCCIC/US-CERT, [Online]. Available: https://nvd.nist.gov/. [Accessed 29 Dec. 2016].

[24] Krzysztof Cabaj and Wojciech Mazurczyk, "Using software-defined networking for ransomware mitigation: The case of CryptoWall," *IEEE Network*, vol. 30, no. 6, pp. 14 - 20, Aug. 2016.

[25] Yong Ling Xue, "Systems and methods for pre-installation detection of malware on mobile devices". Patent US9256738 B2, 11 Mar. 2014.

[26] James B. Fraley and James Cannady, "Enhanced detection of advanced malicious software," in *proc. of IEEE Annual Conference on Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, USA, Oct. 2016.

[27] Alert Logic , "The Cyber Kill Chain: Understanding Advanced Persistent Threats," 30 Dec. 2016. [Online]. Available: https://www.alertlogic.com. [Accessed 23 Jan. 2017].

[28] Lionel Payet, "Hearthstone add-ons, cheating tools come with data-stealing malware," Symantec Corporation, 9 Feb 2014. [Online]. Available: https://www.symantec.com. [Accessed 23 Jan. 2017].

[29] Sana Siddiqui, Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "Detecting advanced persistent threats using fractal dimension based machine learning classification," in *proc. of the 2016 ACM on International Workshop on Security And Privacy Analytics*, New Orleans, Louisiana, USA, Mar. 2016.

[30] Vindu Goel and Nicole Perlroth, "Yahoo says 1 billion user accounts were hacked," Dec. 2016. [Online]. Available: http://www.nytimes.com. [Accessed 23 Jan. 2017].

[31] Martin Ussath, David Jaeger, Feng Cheng and Christoph Meinel, "Advanced persistent threats: Behind the scenes," in *proc. of IEEE 2016 Annual Conference onInformation Science and Systems (CISS)*, Princeton, NJ, USA, Mar. 2016.

[32] Dell Secureworks, "Understand the Threat," Dell, 2014. [Online]. Available: http://www.secureworks.com/. [Accessed 12 Jan. 2017].

[33] Tim Greene , "Why the 'cyber kill chain' needs an upgrade," Network World, Aug. 2016. [Online]. Available: http://www.networkworld.com. [Accessed 23 Jan. 2017].

[34] Marc Laliberte, "A new take on the Cyber Kill Chain," 22 Sep. 2016. [Online]. Available: https://www.secplicity.org. [Accessed 21 Apr. 2018].

[35] Jassim Happa and Graham Fairclough, "A model to facilitate discussions about cyber attacks," in *Ethics and Policies for Cyber Operations*, vol. 124, Mariarosaria Taddeo and Ludovica Glorioso, Eds., Springer International Publishing, Dec. 2016, pp. 169-185.

[36] CERT-UK, "Code Obfuscation," National Cyber Security Center, GCHQ, UK, 2014.

[37] Christian Collberg, Clark Thomborson and Douglas Low, "A taxonomy of obfuscating transformations," Computer Science Technical Reports, The University of Auckland, Auckland, New Zealand, Jul. 1997.

[38] Kris Mikael Krister, "Automated analyses of malicious code (Masters Thesis)," Norwegian University of Science and Technology, Trondheim, Norway, Jun. 2009.

[39] Mike Schiffman , "A brief history of malware obfuscation," Cisco Blogs, 22 Feb. 2010. [Online]. Available: https://blogs.cisco.com/security/a_brief_history_of_malware_obfuscation_part_2_of_2. [Accessed 2 Mar. 2018].

[40] Wei Wang, "Virus Obfuscation," 2016. [Online]. Available: http://www.cs.virginia.edu/~ww6r/CS4630/lectures/Virus_Obfuscation.pdf.

[41] Peter Szor, The Art of Computer Virus Research and Defense, Addison-Wesley Professional, 2005.

[42] Chet Hosmer, "Polymorphic and Metamorphic Malware," in *Black Hat USA 2008*, Las Vegas, 2008.

[43] Carey Nachenberg, "Understanding and Managing Polymorphic Viruses," Symantec, Cupertino, 1996.

[44] Michalis Polychronakis, Kostas G. Anagnostakis and Evangelos P. Markatos, "An empirical study of real-world polymorphic code injection attacks," in *proc. of the 2nd USENIX Conference on Large-Scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More*, Boston, MA, 2008.

[45] Frédéric Perriot, Peter Ferrie and Péter Ször, "Virus Analysis," Symantecc, Oxfordshire, 2002.

[46] Jana Stastna and Martin Tomasek, "Exploring malware behaviour for improvement of malware signatures," in *proc. of IEEE 13th International Scientific Conference on Informatics*, Poprad, Slovakia, Jan. 2016.

[47] Gregoire Jacob, Herve Debar and Eric Filiol, "Behavioral detection of malware: from a survey towards an established taxonomy," *Journal in Computer Virology*, vol. 4, no. 3, p. 251–266, Feb. 2008.

[48] Kyriakos K. Ispoglou and Mathias Payer, "malWASH: washing malware to evade dynamic analysis," in *proc. of the 10th USENIX Conference on Offensive Technologies*, Austin, TX, USA, Aug. 2016.

[49] Ethan M. Rudd, Andras Rozsa, Manuel Günther and Terrance E. Boult, "A survey of stealth malware attacks, mitigation measures, and steps toward autonomous open world solution," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1145 - 1172, Dec. 2016.

[50] Pat Belcher, "Hash Factory: New Cerber Ransomware Morphs Every 15 Seconds," Jun. 2016. [Online]. Available: https://www.invincea.com.

[51] Hyrum S. Anderson, Anant Kharkar, Bobby Filar, David Evans and Phil Roth, "Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning," *Journal of Computer Science Cryptography and Security - Cornell University Library - arXiv:1801.08917*, Jan. 2018.

[52] Michele Bombardieri, Salvatore Castano, Fabrizio Curcio, Angelo Furfaro and Helen D. Karatza, "Honeypot-Powered Malware Reverse Engineering," in *proc. of 2016 IEEE International Conference onCloud Engineering Workshop*, Berlin, Germany, Apr. 2016.

[53] Wei Yang, Xusheng Xiao, Benjamin Andow, Sihan Li, Tao Xie and William Enck, "AppContext: Differentiating malicious and benign mobile App behaviors using Context," in *proc. of 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering*, Florence, Italy, May 2015.

[54] Boyana Peeva, "Remove Zeus Trojan Virus," Sensors TechForum, 1 Jun. 2017. [Online]. Available: https://sensorstechforum.com/remove-zeus-trojan-virus/. [Accessed 10 Feb. 2018].

[55] "Zeus Virus," Kaspersky Lab, [Online]. Available: https://usa.kaspersky.com/resource-center/threats/zeus-virus.

[56] "Trojan.Zbot," Symantec, 10 January 2010. [Online]. Available: https://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99&tabid=2.

[57] Geethu Babu, Shayan Parhite, Jaiteerth Patil and Rajesh S Gill, "King of Trojans - Zeus".

[58] "How a Citadel Trojan Developer Got Busted," 25 July 2017. [Online]. Available: https://krebsonsecurity.com/tag/citadel-trojan/.

[59] Jerome Segura, "Citadel: A Cyber-Criminal's Ultimate Weapon?," Malwarebytes Labs, 30 Mar. 2016. [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/. [Accessed 6 Oct. 2017].

[60] Jason Milletary, "Citadel Trojan Malware Analysis," Dell SecureWorks Counter Threat Unit Intelligence Services, Sep. 2012.

[61] Ashkan Rahimian, Raha Ziarati, Stere Preda and Mourad Debbabi, "On the Reverse Engineering of the Citadel Botnet," in *The Sixth International Symposium on Foundations & Practice of Security*, La Rochelle, 2013.

[62] "NJCCIC," 10 March 2017. [Online]. Available: https://www.cyber.nj.gov/threat-profiles/trojan-variants/poweliks.

[63] Benjamin S. Rivera and Rhena U. Inocencio, "Doing More with Less: A Study of Fileless Infection Attacks," TrendMicro, 2015.

[64] "Trojan:W32/Poweliks - Threat description," [Online]. Available: https://www.f-secure.com/v-descs/trojan_w32_poweliks.shtml.

[65] Masaki Suenaga, "Trojan.Poweliks," Symantec, [Online]. Available: https://www.symantec.com/security_response/writeup.jsp?docid=2014-080408-5614-99.

[66] Kevin Gossett, "Poweliks click-fraud malware goes fileless in attempt to prevent removal," 09 June 2015. [Online]. Available: https://www.symantec.com/connect/blogs/poweliks-click-fraud-malware-goes-fileless-attempt-prevent-removal.

[67] Adam Kujawa, "No More Poweliks!," 11 November 2014. [Online]. Available: https://blog.malwarebytes.com/cybercrime/2014/11/no-more-poweliks/.

[68] "McAfee Labs Threat Advisory - Trojan Poweliks," Intel Security, 2016.

[69] Windows Dev Center, "CLSID Key," [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/ms691424(v=vs.85).aspx. [Accessed 5 Oct. 2017].

[70] Liam O'Murchu and Fred P. Gutierrez, "The evolution of the fileless click-fraud malware Poweliks," Symantec, 2015.

[71] "DiamondFox, Nivdort, ProxyBack malware families added to Botnet Analysis and Reporting Service," Mar. 2016. [Online]. Available: https://blog.team-cymru.org/2016/03/diamondfox-nivdort-proxyback-malware-families-added-to-botnet-analysis-and-reporting-service-bars/.

[72] Goldsparrow, "Nivdort," [Online]. Available: https://www.enigmasoftware.com/nivdort-removal/.

[73] "Email Campaigns During the 2015 Holiday Season," FireEye, 2015.

[74] "TrojanSpy:Win32/Nivdort.V," [Online]. Available: https://malwarefixes.com/threats/trojanspywin32nivdort-v/.

[75] "TrojanSpy:Win32/Nivdort.A," 15 September 2017. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanSpy:Win32/Nivdort.A.

[76] Lior Kohavi, "Automated Threat Intelligence: The Key to Preventing, Mitigating, and Identifying Cyber Breaches," Cyren Inc., 2016.

[77] "Threat landscape report Q2 2017," Fortinet, 2017.

[78] Nino Fred Gutierrez and Alan Neville, "Trojan.Stabuniq," 18 December 2012. [Online]. Available: https://www.symantec.com/security_response/writeup.jsp?docid=2012-121809-2437-99&tabid=2.

[79] Graeme McMillan, "Beware Trojan.Stabuniq, a new malware targeting American banks," Digital Trends, 24 Dec. 2012. [Online]. Available: https://www.digitaltrends.com. [Accessed 21 Nov. 2017].

[80] Domesticus, "Trojan.Stabuniq," [Online]. Available: https://www.enigmasoftware.com/trojanstabuniq-removal/.

[81] Emanuele De Lucia, "Stabuniq in depth," INFOSEC Institute, 2013.

[82] Donna Wang and Jacob (Kuan Long) Leong, "A New All-in-One Botnet: Proteus," Fortinet, 28 Nov. 2016. [Online]. Available: https://blog.fortinet.com/2016/11/28/a-new-all-in-one-botnet-proteus. [Accessed 10 Apr. 2018].

[83] Douglas Bonderud, "New Proteus Malware: Jerk of All Trades?," 1 December 2016. [Online]. Available: https://securityintelligence.com/news/new-proteus-malware-jerk-of-all-trades/.

[84] Catalin Cimpanu, "New Proteus Malware Can Mine for Crypto-Currency, Log Keystrokes, and More," 30 November 2016. [Online]. Available: https://www.bleepingcomputer.com/news/security/new-proteus-malware-can-mine-for-crypto-currency-log-keystrokes-and-more/.

[85] Check Point Research Team, "What's the Proteus botnet and how does it work?," Check Point, [Online]. Available: https://blog.checkpoint.com/2017/01/19/whats-proteus-botnet-work/. [Accessed 19 Jan. 2017].

[86] State of New Jersey, "Alina - PoS Malware Variants," New Jersy Cyber Security and Information Communication Cell, 6 Jul. 2016. [Online]. Available: https://www.cyber.nj.gov/threat-profiles/pos-malware-variants/alina. [Accessed 12 Sep. 2018].

[87] Trend Micro, "Threat Encyclopedia - Malware ALINA," Trend Micro, 12 Sep. 2014. [Online]. Available: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/alina. [Accessed 12 Sep. 2017].

[88] Numaan Huq, "PoS RAM Scraper Malware - Past, Present, and Future," TrendMicro, Irving, 2014.

[89] Josh Grunzweig, "Alina: Casting a Shadow on POS," Spider Labs - Trustware, 8 May 2013. [Online]. Available: https://www.trustwave.com/Resources/SpiderLabs-Blog/Alina--Casting-a-Shadow-on-POS/. [Accessed 13 Sep. 2018].

[90] Domesticus, "Win32/TrojanDownloader.Zurgop.AZ," Enigma Software - Applications for the masses, [Online]. Available: https://www.enigmasoftware.com/win32trojandownloaderzurgopaz-removal/.

[91] "Win32/TrojanDownloader.Zurgop," Virus Radar, 11 May 2014. [Online]. Available: http://www.virusradar.com/en/Win32_TrojanDownloader.Zurgop.BK/description.

[92] Microsoft, "Backdoor:Win32/Hupigon," Microsoft, 15 Sep. 2017. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Backdoor%3AWin32%2FHupigon. [Accessed 20 Apr. 2018].

[93] F-Secure, "Backdoor:W32/Hupigon," F-Secure, [Online]. Available: https://www.f-secure.com/v-descs/backdoor_w32_hupigon.shtml. [Accessed 20 Apr. 2018].

[94] "Hupigon," Trend Micro, 12 July 2013. [Online]. Available: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/hupigon.

[95] Trend Micro, "A brief history of notable online banking Trojans," Trend Micro, 31 Aug. 2015. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/online-banking-trojan-brief-history-of-notable-online-banking-trojans. [Accessed 2 Mar. 2018].

[96] TrendMicro, "Carberp," TrendMicro, 27 Feb. 2014. [Online]. Available: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/carberp. [Accessed 12 Dec. 2018].

[97] Eduard Kovacs, "New Variant of Carberp Trojan Discovered by Researchers," Security Weeks, 15 January 2015. [Online]. Available: http://www.securityweek.com/new-variant-carberp-trojan-discovered-researchers.

[98] Roberto Sponchioni, "New Carberp variant heads down under," Symantec, 13 January 2015. [Online]. Available: https://www.symantec.com/connect/blogs/new-carberp-variant-heads-down-under.

[99] "The Carberp Information Stealing Trojan," Jisc, [Online]. Available: https://community.jisc.ac.uk/library/janet-services-documentation/carberp-information-stealing-trojan.

[100] Peter Kálnai and Jaromír Hořejší, "Dissecting Banking Trojan Carberp2," RSA Conference 2013, 2013.

[101] Mary Landesman, "What is a Virus Signature?," Lifewire, 3 October 2017. [Online]. Available: https://www.lifewire.com/what-is-a-virus-signature-153629.

[102] "Signature based vs behaviour-based malware detection," stackoverflow, 9 October 2016. [Online]. Available: https://stackoverflow.com/questions/39932564/signature-based-vs-behaviour-based-malware-detection.

[103] Zahra Bazrafshan, Hashem Hashemi, Seyed Mehdi Hazrati Fard and Ali Hamzeh, "A survey on heuristic malware detection techniques," in *proc. of 2013 5th Conference on Information and Knowledge Technology*, Shiraz, Iran, May. 2013.

[104] Khalid Mohamed Abdelrahman Y Alzarooni, "Malware Variant Detection," University College London, London, 2012.

[105] Pat Belcher, "Hash Factory: New Cerber ransomware morphs every 15 seconds," Jun. 2016. [Online]. Available: https://www.invincea.com. [Accessed 3 May 2018].

[106] Ashu Sharma and S. K. Sahay. , "Evolution and Detection of Polymorphic and Metamorphic Malwares: A Survey," *International Journal of Computer Applications,* vol. 90, no. 2, pp. 7-11, 2014.

[107] McAfee, "Build a Better Sandbox - A working strategy for comprehensive malware protection," McAfee Inc., Santa Clara, CA, USA, Jul. 2014.

[108] David Harley and Andrew Lee, "Heuristic Analysis - Detecting Unknown Viruses," ESET, 2009.

[109] Curtis Cade, "Understanding Heuristic-based Scanning vs. Sandboxing," OPSWAT, 13 July 2015. [Online]. Available: https://www.opswat.com/blog/understanding-heuristic-based-scanning-vs-sandboxing.

[110] Gustav Lundsgard and Victor Nedstrom, "Bypassing modern sandbox technologies - An experiment on sandbox evasion techniques," Lund University, Lund, Sweden, Jun. 2016.

[111] Chris Walker, "Detecting Malware and Sandbox Evasion Techniques," The SANS Institute, 2016.

[112] Nwokedi Idika and Aditya P. Mathur, "A survey of malware detection techniques," Department of Computer Science, Purdue University, West Lafayette, USA, Feb. 2007.

[113] Sana Siddiqui, Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "Fractal based cognitive neural network to detect obfuscated and indistinguishable internet threats," in *proc. of IEEE 16th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC)*, Oxford, UK, Jul. 2017.

[114] Yingxu Wang and Kendal Hu, "Semantic Manipulations and Formal Ontology for Machine Learning based on Concept Algebra," *International Journal of Cognitive Informatics and Natural Intelligence (IJCINI),* vol. 5, no. 4, 2011.

[115] Sanjeev Das , Yang Liu and Wei Zhang , "Semantics-Based Online Malware Detection: Towards Efficient Real-Time Protection Against Malware," *IEEE Transactions on Information Forensics and Security,* pp. 289 - 302, Oct. 2015.

[116] Yu Feng, Osbert Bastani, Ruben Martins, Isil Dilli and Saswat Anand, "Automated synthesis of semantic malware signatures using maximum satisfiability," *ArXiv*, Jun. 2017.

[117] Mihai Christodorescu, Somesh Jha, Sanjit A. Seshia, Dawn Song and Randal E. Bryant, "Semantics-Aware Malware Detection," in *proc. of the 2005 IEEE Symposium on Security and Privacy*, May 2005.

[118] Mu Zhang, Yue Duan, Heng Yin and Zhiruo Zhao, "Semantics-Aware Android malware classification using weighted contextual API Dependency Graphs," in *proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Scottsdale, Arizona, USA, Nov. 2014.

[119] Tobias Wuechner , Aleksander Cislak and Martin Ochoa, "Leveraging Compression-based Graph Mining for Behavior-based Malware Detection," *IEEE Transactions on Dependable and Secure Computing,* Mar. 2017.

[120] Ali Feizollah, Nor Badrul Anuar, Rosli Salleh, Guillermo Suarez-Tangil and Steven Furnell, "AndroDialysis: Analysis of Android intent effectiveness in malware detection," *Computers & Security,* vol. 65, pp. 121-134, Mar. 2017.

[121] Mila Dalla Preda, Mihai Christodorescu, Somesh Jha and Saumya Debray, "A semantics-based approach to malware detection," in *proc. of the 34th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, Nice, France, Jan. 2007.

[122] Khalid Alzarouni, David Clark and Laurence Tratt, "Semantic Malware Detection," Faculty of Natural and Mathematical Scienses, Kings College London, London, UK, Feb. 2010.

[123] M. Christodorescu, S. Jha and S.A. Seshia, "Semantics-aware malware detection," in *proc. of 2005 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2005.

[124] Robert Luh, Stefan Marschalek, Manfred Kaiser, Helge Janicke and Sebastian Schrittwieser, "Semantics-aware detection of targeted attacks: a survey," *Journal of Computer Virology and Hacking Techniques,* vol. 13, no. 1, p. 47–85, May 2016.

[125] Guozhu Meng, Yinxing Xue, Zhengzi Xu, Yang Liu, Jie Zhang and Annamalai Narayanan, "Semantic modelling of Android malware for effective malware comprehension, detection, and classification," in *proc. of the 25th International Symposium on Software Testing and Analysis*, Saarbrucken, Germany, Jul. 2016.

[126] Nur Syuhada Selamat, Fakariah Hani Mohd Ali and Noor Ashitah Abu Othman, "Polymorphic Malware Detection," in *International Conference on IT Convergence and Security (ICITCS)*, Prague, 2016.

[127] James B. Fraley and Marco Figueroa, "Polymorphic malware detection using topological feature extraction with data mining," in *IEEE SoutheastCon*, Norfolk, 2016.

[128] Gerald R. Thompson and Lori A. Flynn, "Polymorphic malware detection and identification via context-free grammar homomorphism," *Bell Labs Technical Journal*, vol. 12, no. 3, pp. 139-147, 2007.

[129] Fahad Bin Muhaya, Muhammad Khurram Khan and Yang Xiang, "Polymorphic malware detection using hierarchical Hidden Markov Model," in *proc. of IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*, Sydney, NSW, Australia, Dec. 2011.

[130] Mina Gharacheh, Vali Derhami, Sattar Hashemi and Seyed Mehdi Hazrati Fard, "Proposing an HMM-based approach to detect metamorphic malware," in *proc. of the fourth Iranian Joint Congress on Fuzzy and Intelligent Systems*, Zahedan, Iran, Sep. 2015.

[131] Silvio Cesare and Yang Xiang, "A fast flowgraph based classification system for packed and polymorphic malware on the endhost," in *proc. of 24th IEEE International Conference on Advanced Information Networking and Applications (AINA 2010)*, Perth, WA, Australia, Apr. 2010.

[132] Silvio Cesare and Yang Xiang, "Malware variant detection using similarity search over sets of Control Flow Graphs," in *proc. of IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Changsha, China, Nov. 2011.

[133] Avijit Mondal, Subrata Paul, Anirban Mitra and Biswajit Gope, "Automated signature generation for polymorphic worms using substrings extraction and principal component analysis," in *proc. of IEEE International Conference on Computational Intelligence and Computing Research*, Madurai, India, Dec. 2015.

[134] Yong Tang and Shigang Chen, "An automated signature-based approach against polymorphic Internet worms," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 7, Jul. 2007.

[135] Serge Chaumette, Olivier Ly and Renaud Tabary, "Automated extraction of polymorphic virus signatures using abstract interpretation," in *proc. of 5th International Conference on Network and System Security (NSS)*, Milan, Italy, 2011.

[136] Yong Tang, Bin Xiao and Xicheng Lu, "Signature tree generation for polymorphic worms," *IEEE Transactions on Computers*, vol. 60, no. 4, pp. 565 - 579, Jun. 2011.

[137] Zhichun Li, Lanjia Wang, Yan Chen and Zhi Fu, "Network-based and attack-resilient length signature generation for zero-day polymorphic worms," in *proc. of IEEE International Conference on Network Protocols*, Beijing, China, Nov. 2007.

[138] Jake Drew, Tyler Moore and Michael Hahsler, "Polymorphic malware detection using sequence classification methods," in *proc. of IEEE Security and Privacy Workshop*, San Jose, CA, USA, May 2016.

[139] Royi Ronen, Marian Radu, Corina Feuerstein, Elad Yom-Tov and Mansour Ahmadi, "Microsoft malware classification challenge," *Cryptography and Security*, Feb. 2018.

[140] P. Vinod, V. Laxmi, M. S. Gaur and Grijesh Chauhan, "MOMENTUM: MetamOrphic malware exploration techniques using MSA signatures," in *proc. of International Conference on Innovations in Information Technology*, Abu Dhabi, United Arab Emirates, Jun. 2012.

[141] Yanzhen Qu and Kelly Hughes, "Detecting metamorphic malware by using behavior-based aggregated signature," in *proc. of World Congress on Internet Security (WorldCIS)*, London, UK, Dec. 2013.

[142] Haniye Razeghi Borojerdi and Mahdi Abadi, "MalHunter: Automatic generation of multiple behavioral signatures for polymorphic malware detection," in *proc. of International Conference on Computer and Knowledge Engineering (ICCKE)*, Mashhad, Iran, Nov. 2013.

[143] Eeza Mirzazadeh, Mohammad Hossein Moattar and Majid Vafaei Jahan, "Metamorphic malware detection using Linear Discriminant Analysis and Graph similarity," in *proc. of International Conference on Computer and Knowledge Engineering (ICCKE)*, Mashhad, Iran, Oct. 2015.

[144] Vishakha Mehra, Vinesh Jain and Dolly Uppal, "DaCoMM: Detection and Classification of Metamorphic Malware," in *proc. of Fifth International Conference on Communication Systems and Network Technologies*, Gwalior, India, Apr. 2015.

[145] Qinghua Zhang and Douglas S. Reeves, "MetaAware: Identifying metamorphic malware," in *proc. of 23rd Annual Computer Security Applications Conference (ACSAC)*, Miami Beach, FL, USA, Dec. 2007.

[146] Felix Leder, Bastian Steinbock and Peter Martini, "Classification and detection of metamorphic malware using value set analysis," in *proc. of 4th International Conference on Malicious and Unwanted Software (MALWARE)*, Montreal, QC, Canada, Oct. 2009.

[147] Jikku Kuriakose and Vinod P., "Discriminant features for metamorphic malware detection," in *proc. of seventh International Conference on Contemporary Computing*, Noida, India, Sep. 2014.

[148] Jikku Kuriakose and P. Vinod, "Metamorphic virus detection using feature selection techniques," in *proc. of International Conference on Computer and Communication Technology*, Allahabad, India, Sep. 2014.

[149] Jikku Kuriakose and P. Vinod, "Ranked linear discriminant analysis features for metamorphic malware detection," in *proc. of IEEE International Advance Computing Conference (IACC)*, Gurgaon, India, Feb. 2014.

[150] Duaa Ekhtoom, Mahmoud Al-Ayyoub, Mohammed Al-Saleh, Mohammad Alsmirat and Ismail Hmeidi, "A compression-based technique to classify metamorphic malware," in *proc. of 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir, Morocco, Dec. 2016.

[151] Jared Lee, Thomas H. Austin and Mark Stamp, "Compression-based analysis of metamorphic malware," *International Journal of Security and Networks*, vol. 10, no. 2, pp. 124-136, Jul. 2015.

[152] Peyman Khodamoradi, Mahmood Fazlali, Farhad Mardukhi and Masoud Nosrati, "Heuristic metamorphic malware detection based on statistics of assembly instructions using classification algorithms," in *proc. of 18th CSI International Symposium on Computer Architecture and Digital Systems (CADS)*, Tehran, Iran, Jan. 2015.

[153] Fereidoon Rezaei, Masoud Khalil Nezhad, Saeid Rezaei and Ali Payandeh, "Detecting encrypted metamorphic viruses by hidden Markov Models," in *proc. of International Conference on Fuzzy Systems and Knowledge Discovery*, Xiamen, China, Aug. 2014.

[154] Essam Al Daoud, "Metamorphic viruses detection using artificial immune system," in *proc. of International Conference on Communication Software and Networks*, Macau, China, Feb. 2009.

[155] Shahid Alam, R. Nigel Horspool and Issa Traore, "MARD: A framework for metamorphic malware analysis and real-time detection," in *proc. IEEE International Conference on Advanced Information Networking and Applications*, Victoria, BC, Canada, May 2014.

[156] Adiel Aviad, Krzysztof Wecel and Witold Abramowicz, "The semantic approach to cyber security towards ontology based body of knowledge," in *proc. of the 14th European Conference on Cyber Warfare and Security*, Hatfield, UK, Jul. 2015.

[157] Victor Raskin, Christian F. Hempelmann , Katrina E. Triezenberg and Sergei Nirenburg, "Ontology in information security: a useful theoretical foundation and methodological tool," in *proc. of the 2001 workshop on New security paradigms*, Cloudcroft, New Mexico, Sep. 2001.

[158] Salvatore J. Stolfo, Shlomo Hershkop, Chia-Wei Hu, Wei-Jen Li, Olivier Nimeskern and Ke Wang, "Behavior-based modeling and its application to Email analysis," *ACM Transactions on Internet Technology*, vol. 6, no. 2, pp. 187-221, May 2006.

[159] Phong H. Nguyen, Cagatay Turkay, Gennady Andrienko, Natalia Andrienko and Olivier Thonnard, "A visual analytics approach for User behaviour understanding through action sequence analysis," in *proc. of EuroVis Workshop on Visual Analytics*, Barcelona, Spain, Jun. 2017.

[160] Cheng Wang, Bo Yang and Jing Luo, "Identity theft detection in mobile social networks using behavioral semantics," in *proc. of IEEE International Conference on Smart Computing*, Hong Kong, China, May 2017.

[161] Wu Xin, Qingni Shen, Yahui Yang and Zhonghai Wu, "SeEagle: Semantic-enhanced anomaly detection for securing eagle," *Digital Forensics and Cyber Crime* , vol. 216, pp. 221-227, Jan. 2018.

[162] Guangquan Xu, Yan Cao, Yuanyuan Ren, Xiaohong Li and Zhiyong Feng, "Network security situation awareness based on semantic ontology and user-defined rules for Internet of Things," *IEEE Access*, vol. 5, pp. 21046 - 21056, 01 Aug. 2017.

[163] Monnappa K. A., "Automating Linux Malware Analysis Using Limon Sandbox," [Online]. Available: https://www.blackhat.com/docs/eu-15/materials/eu-15-KA-Automating-Linux-Malware-Analysis-Using-Limon-Sandbox-wp.pdf. [Accessed 2 May 2018].

[164] Luis MartinGarcia, "TCPDump & LibPCAP," Tcpdump/Libpcap, [Online]. Available: http://www.tcpdump.org/. [Accessed 19 Dec. 2016].

[165] GITHUB, "Yara," GITHUB, [Online]. Available: https://github.com/plusvic/yara. [Accessed 25 Feb. 2018].

[166] The Volatility Foundation, "Releases," The Volatility Foundation, [Online]. Available: http://www.volatilityfoundation.org/#!releases/component_71401/. [Accessed 23 Feb. 2018].

[167] VirusTotal, "VirusTotal Public API v2.0," VirusTotal, [Online]. Available: https://www.virustotal.com/en/documentation/public-api/. [Accessed 1 Mar. 2018].

[168] Mihai Vasilescu, Laura Gheorghe and Nicolae Tapus, "Practical malware analysis based on sandboxing," in *proc. of Networking in Education and Research, Joint Event 13th RoEduNet & 8th RENAM Conference*, Chisinau, Moldova, Sep. 2014.

[169] S. L. Shiva Darshan, M. A. Ajay Kumara and C. D. Jaidhar, "Windows malware detection based on cuckoo sandbox generated report using machine learning algorithm," in *proc. of 11th International Conference on Industrial and Information Systems*, Roorkee, India, Dec. 2016.

[170] Ivan Firdausi, Charles lim, Alva Erwin and Anto Satriyo Nugroho, "Analysis of machine learning techniques used in behavior-based malware detection," in *proc. of 2nd International Conference on Advances in Computing, Control and Telecommunication Technologies (ACT)*, Jakarta, Indonesia, Dec. 2010.

[171] Lastline, "Anubis," Lastline, [Online]. Available: https://anubis.iseclab.org/. [Accessed 15 Aug. 2017].

[172] Qian Chen and Robert A. Bridges, "Automated behavioral analysis of malware - A case study of wannacry ransomware," in *proc. of 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Cancun, Mexico, Dec. 2017.

[173] Peter M. Wrench and Barry V. W. Irwin, "Towards a sandbox for the deobfuscation and dissection of PHP malware," in *proc. of Information Security for South Africa*, Johannesburg, South Africa, Aug. 2014.

[174] Ulrich Bayer, Andreas Moser, Christopher Kruegel and Engin Kirda, "Dynamic analysis of malicious code," *Journal of Computer Virology*, vol. 2, no. 1, pp. 67-77, May 2006.

[175] Qemu, "QEMU – Complete, independent and fast processor simulator," Qemu, [Online]. Available: https://www.qemu.org/. [Accessed 5 May 2018].

[176] Carsten Willems, Thorsten Holz and Felix Freiling, "Toward automated dynamic malware analysis using CWSandbox," *IEEE Security and Privacy*, vol. 5, no. 2, pp. 32-39, Apr. 2007.

[177] Norman , "Norman Sandbox Analyzer," Norman, [Online]. Available: http://download01.norman.no/product_sheets/eng/SandBox_analyzer.pdf. [Accessed 25 Jan. 2018].

[178] Heng Yin, Dawn Song, Manuel Egele, Christopher Kruegel and Engin Kirda, "Panorama: Capturing system-wide information flow for malware detection and analysis," in *proc. of the ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, Nov. 2007.

[179] Radu S. Pirscoveanu, Steven S. Hansen, Thor M. T. Larsen, Matija Stevanovic, Jens Myrup Pedersen and Alexandre Czech, "Analysis of malware behavior: Type classification using machine learning," in *proc. of International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, London, UK, Jun. 2015.

[180] Sean Kilgallon, Leonardo De La Rosa and John Cavazos, "Improving the effectiveness and efficiency of dynamic malware analysis with machine learning," in *proc. of Resilience Week*, Wilmington, DE, USA, Sep. 2017.

[181] Najmeh Miramirkhani, Mahathi Priya Appini, Nick Nikiforakis and Michalis Polychronakis, "Spotless Sandboxes: Evading malware analysis systems using wear-and-tear artifacts," in *proc. of IEEE Symposium on Security and Privacy*, San Jose, CA, USA, May 2017.

[182] Joao Marcelo Ceron, Cintia Borges Margi and Lisandro Zambenedetti Granville, "MARS: An SDN-based malware analysis solution," in *proc. of IEEE Symposium on Computers and Communication*, Messina, Italy, Jun. 2016.

[183] Artem Dinaburg, Paul Royal, Monirul Sharif and Wanke Lee, "Ether: Malware analysis via hardware virtualization extensions," in *proc. of the ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, Oct. 2008.

[184] Thomas Bläsing, Leonid Batyuk, Aubrey-Derrick Schmidt, Seyit Ahmet Camtepe and Sahin Albayrak, "An Android application Sandbox system for suspicious software detection," in *proc. of International Conference on Malicious and Unwanted Software (MALWARE)*, Nancy, France, Oct. 2010.

[185] Mohammed K. Alzaylaee, Suleiman Y. Yerima and Sakir Sezer, "DynaLog: An automated dynamic analysis framework for characterizing Android applications," in *proc. of International Conference On Cyber Security And Protection Of Digital Services*, London, UK, Jun. 2016.

[186] Katsunari Yoshioka, Yoshihiko Hosobuchi, Tatsunori Orii and Tsutomu Matsumoto, "Vulnerability in Public Malware Sandbox Analysis Systems," in *proc. of IEEE/IPSJ International Symposium on Applications and the Internet*, Seoul, South Korea, Jul. 2010.

[187] Fernando C. Colon Osorio, Hongyuan Qiu and Anthony Arrott, "Segmented sandboxing - A novel approach to Malware polymorphism detection," in *proc. of International Conference on Malicious and Unwanted Software (MALWARE)*, Fajardo, Puerto Rico, Oct. 2015.

[188] Crowd Strike, "Automated Malware Analysis Services," Falcon Sandbox - Crowd Strike, [Online]. Available: https://www.falcon-sandbox.com/. [Accessed 21 Feb. 2018].

[189] Cuckoo Foundation, "Cuckoo Sandbox Book (Revision a756c188)," Cuckoo Foundation, [Online]. Available: https://cuckoo.sh/docs/index.html. [Accessed 19 Oct. 2017].

[190] Threat Track, "Threat Analyzer," Threat Track, [Online]. Available: https://www.threattrack.com. [Accessed 2 May 2018].

[191] Threat Track, "Threat Analyzer - Dynamic Malware Analysis," Threat Track, [Online]. Available: https://www.threattrack.com/. [Accessed 2 May 2018].

[192] Joe Sandbox Ultimate, "Automated Malware Analysis," Joe Sandbox Ultimate, [Online]. Available: https://joesecurity.org/joe-sandbox-ultimate#key-features. [Accessed 29 Jan. 2018].

[193] Forcepoint , "Advanced Malware Detection," Forcepoint - Raytheon, [Online]. Available: https://www.forcepoint.com/sites/default/files/resources/files/datasheet_advanced_malware_detection_en.pdf. [Accessed 23 Dec. 2017].

[194] ForcePoint, "System Requirements," ForcePoint, [Online]. Available: https://www.websense.com. [Accessed 2 May 2018].

[195] Fortinet, "FortiSandbox - Administration Guide," Fortinet, [Online]. Available: https://docs.fortinet.com/uploaded/files/2682/fortisandbox-2.1.1-administration-guide.pdf. [Accessed 2 May 2018].

[196] FireEye, "Forensic Analysis AX Series," FireEye, [Online]. Available: https://www.fireeye.com/. [Accessed 2 May 2018].

[197] LastLine, "Lastline Analyst: Give Your Incident Responders the Information They Need," LastLine, [Online]. Available: https://www.lastline.com/. [Accessed 2 May 2018].

[198] LastLine, "Technology Alliance Partnerships," LastLine, [Online]. Available: https://www.lastline.com. [Accessed 2 May 2018].

[199] Symantec , "Symantec Malware Analysis Service," Symantec , [Online]. Available: https://www.symantec.com. [Accessed 2 May 2018].

[200] Symantec , "Symantec Malware Analysis S400/S500," Symantec, [Online]. Available: https://www.symantec.com. [Accessed 2 May 2018].

[201] Symantec , "Symantec Content Analysis - S200/S400/S500," Symantec , [Online]. Available: https://www.symantec.com. [Accessed 2 May 2018].

[202] SecondWrite, "SecondWrite Sandbox," Second Write, [Online]. Available: https://www.secondwrite.com. [Accessed 2 May 2018].

[203] Binary Guard, "True Bare Metal (TBM) Cloud Sandbox," Binary Guard, [Online]. Available: http://www.binaryguard.com. [Accessed 2 May 2018].

[204] Malek Ben Salem, "Towards effective masquerade attack detection (Ph.D. Dissertation)," Columbia University, USA, New York, USA, 2012.

[205] Hiba Zuhair, Ali Selamat and Mazleena Salleh , "Feature selection for phishing detection: a review of research," *International Journal of Intelligent Systems Technologies and Applications,* vol. 15, no. 2, pp. 147-162, May 2016.

[206] Mohit Virendra , Qi Duan and Shambhu Upadhyaya, "Detecting cheating aggregators and report dropping attacks in Wireless Sensor Networks," *Journal of Wireless Technologies: Concepts, Methodologies, Tools and Applications,* pp. 565-586, 2012.

[207] Stanislav Ponomarev, Nathan Wallace and Jan Durand, "Evaluation of random projection for malware classification," in *proc. of IEEE Seventh International Conference on Software Security and Reliability Companion*, Gaithersburg, MD, USA, Jun. 2013.

[208] Ziv Katzir and Yuval Elovici, "Quantifying the resilience of machine learning classifiers used for cyber security," *Expert Systems with Applications,* vol. 92, pp. 419-429, Feb. 2018.

[209] Muzzamil Noor, Haider Abbas and Waleed Bin Shahid, "Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis," *Journal of Network and Computer Applications,* vol. 103, no. 1, pp. 249-261, Oct. 2017.

[210] Yanfang Ye, Dingding Wang, Tao Li and Dongyi Ye, "IMDS: intelligent malware detection system," in *proc. of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Jose, California, USA, Aug. 2007.

[211] Larry Loeb, "Cerber ransomware uses fast-changing hash signatures to evade detection," IBM Security Intelligence, June 7, 2016.

[212] Michal Wozniak, Manuel Grana and Emilio Corchado, "A survey of multiple classifier systems as hybrid systems," *Journal of Information Fusion - Special Issue on Information Fusion in Hybrid Intelligent Fusion Systems,* vol. 16, p. 3–17, Mar. 2014.

[213] C. R. Dean, L. Wang, P. Maher, C. Forsythe, F. Ghahari, Y. Gao, J. Katoch, M. Ishigami, P. Moon, M. Koshino, T. Taniguchi, K. Watanabe, K. L. Shepard, J. Hone and P. Kim, "Hofstadter's butterfly and the fractal quantum Hall effect in moiré superlattices," *Nature - International Journal of Science,* vol. 497, p. 598–602, May 2013.

[214] Toshio Mori, Yoshimichi Endou and Akira Nakayama, "Fractal analysis and aesthetic evaluation of geometrically overlapping patterns," *Textile Research Journal,* Sep. 1996.

[215] Hiroshi Sasaki, Fang-Hsiang Su, Teruo Tanimoto and Simha Sethumadhavan, "Why do programs have heavy tails?," in *proc. of 2017 IEEE International Symposium on Workload Characterization*, Seattle, WA, USA , Oct. 2017.

[216] Borjana Racheva-Iotova and Gennady Samorodnitsky, "Chapter 16 – Long Range Dependence in Heavy Tailed Stochastic Processes," *Handbook of Heavy Tailed Distributions in Finance,* vol. 1, p. 641–662, Apr. 2008.

[217] Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "Multifractal singularity spectrum for cognitive cyber defence in internet time series," *International Journal of Software Science and Computational Intelligence,* vol. 7, no. 3, pp. 17-45, 2015.

[218] Burr Settles, "Active Learning Literature Survey," Computer Sciences - University of Wisconsin–Madison, Madison, University of Wisconsin, USA, Jan. 2009.

[219] Thu Yein Win, Huaglory Tianfield and Quentin Mair, "Big data based security analytics for protecting virtualized infrastructures in cloud computing," *IEEE Transactions on Big Data,* vol. 4, no. 1, pp. 11 - 25, Jun. 2017.

[220] Sofia Visa and Anca L. Ralescu, "Issues in Mining Imbalanced Data Sets - A Review Paper," in *proc. of the Sixteen Midwest Artificial Intelligence and Cognitive Science Conference*, Cincinnati, Ohio, USA, Jan. 2005.

[221] Guo Haixiang, Li Yijing, Jennifer Shang, Gu Mingyun, Huang Yuanyue and Gong Bing, "Learning from class-imbalanced data: Review of methods and applications," *Expert Systems with Applications,* vol. 73, no. 1, pp. 220-239, Dec. 2016.

[222] Xu-Ying Liu, Jianxin Wu and Zhi-Hua Zhou, "Exploratory undersampling for class-imbalance learning," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics),* vol. 39, no. 2, pp. 539 - 550, Apr. 2009.

[223] Philip K. Chan and Salvatore J. Stolfo, "Toward scalable learning with non-uniform class and cost distributions: a case study in credit card fraud detection," in *proc. of the Fourth International Conference on Knowledge Discovery and Data Mining*, New York, NY, USA, Aug. 1998.

[224] Charles X. Ling and Chenghui Li, "Data mining for direct marketing: problems and solutions," in *proc. of Fourth International Conference on Knowledge Discovery and Data Mining*, New York, USA, Aug. 1998.

[225] Nitesh V. Chawla, Kevin W. Bowyer, Lawrence O. Hall and W. Philip Kegelmeyer, "Smote: Synthetic minority over-sampling technique," *Journal Of Artificial Intelligence Research,* vol. 16, no. 1, pp. 321-357, Jun. 2011.

[226] Andrew Estabrooks, Taeho Jo and Nathalie Japkowic, "A multiple resampling method for learning from imbalanced data sets," *Computational Intelligence,* vol. 20, no. 1, pp. 18-36, Jan. 2004.

[227] Marcus A. Maloof, "Learning when data sets are imbalanced and when costs are unequal and unknown," in *proc. of Workshop on Learning from Imbalanced Data Sets II*, Washington, DC, USA, Jul. 2003.

[228] Leo Breiman, Jerome Friedman, Charles J. Stone and R.A. Olshen, Classification and Regression Trees, Chapman and Hall/CRC, 1984.

[229] Pedro Domingos, "MetaCost: A General Method for Making Classifiers Cost-Sensitive," in *proc. of the fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Diego, California, USA, Aug. 1999.

[230] Charles Elkan, "The Foundations of Cost-Sensitive Learning," in *proc. of the 17th International Joint Conference on Artificial Intelligence - Volume 2*, Seattle, WA, USA, Aug. 2001.

[231] Dan Kobialka, "Are MSSP Incident Responders over-whelmed by false-positive alerts?," MSSP Alert, 13 Feb. 2018. [Online]. Available: https://www.msspalert.com/cybersecurity-news/are-mssp-incident-responders-overwhelmed-by-false-positive-alerts/. [Accessed 8 Oct. 2018].

[232] Sam Erdheim, "A SOC Under Siege: Alert Overload and Cyber Skills Shortage," Idelis Cybersecurity, 22 Mar. 2018. [Online]. Available: https://www.fidelissecurity.com/threatgeek/soc/industry-professional-shortage. [Accessed 8 Oct. 2018].

[233] Miscrosoft Windows Support, "High memory usage by the Svchost.exe process after you install Windows Management Framework 3.0 on a Windows-based computer," Miscrosoft Windows Support, 19 Mar. 2015. [Online]. Available: https://support.microsoft.com. [Accessed 15 Jun. 2018].

[234] Nour Moustafa and Jill Slay, "ADFA-NB15-Datasets - UNSW-NB15 network packets and flows captures," Cyber Range Lab of the Australian Centre for Cyber Security, University of New South Wales, New South Wales, Australia, 2014.

[235] Jianqing Fan, Quefeng Li and Yuyan Wang, "Estimation of high dimensional mean regression in the absence of symmetry and light tail assumptions," *Journal of the Royal Statistical Society: Series B Statistical Methodology*, vol. 79, no. 1, pp. 247-265, Apr. 2016.

[236] Yingxu Wang, "On Cognitive Informatics," in *proc of First IEEE International Conference on Cognitive Informatics*, Aug. 2003.

[237] Roberto Colom, Sherif Karama, Rex E. Jung and Richard J. Haier, "Human intelligence and brain networks," *Dialogues Clin Neurosci*, vol. 12, no. 4, p. 489–501, Dec. 2010.

[238] Shane Legg and Marcus Hutter, "A collection of definitions of Intelligence," *proc. of the 2007 conference on Advances in Artificial General Intelligence: Concepts, Architectures and Algorithms*, pp. 17-24, Jun. 2007.

[239] Jan Glascher, Daniel Tranel, Lynn K. Paul, David Rudrauf, Chris Rorden, Amanda Hornaday, Thomas Grabowski, Hanna Damasio and Ralph Adolphs, "Lesion mapping of cognitive abilities linked to intelligence," *Neuron*, vol. 61, no. 5, pp. 681-691, Mar. 2009.

[240] Yoed N. Kenett, John D. Medaglia, Roger E. Beaty, Qunlin Chen, Richard F. Betzel, Sharon L. Thompson-Schill and Jiang Qiu, "Driving the brain towards creativity and intelligence: A network control theory analysis," *Neuropsychologia*, Jan. 2018.

[241] Andrew D. Norden, Irene Dankwa-Mullan, Alexandra Urman, Fernando Suarez and Kyu Rhee, "Realizing the promise of cognitive computing in cancer care: Ushering in a new era," *JCO Clinical Cancer Informatics*, vol. 2, pp. 1-6, Feb. 2018.

[242] Huimin Lu, Yujie Li, Min Chen, Hyoungseop Kim and Seiichi Serikawa, "Brain Intelligence: Go beyond Artificial Intelligence," *Mobile Networks and Applications*, vol. 23, no. 2, p. 368–375, Apr. 2018.

[243] Emmanuel Dupoux, "Cognitive science in the era of artificial intelligence: A roadmap for reverse-engineering the infant language-learner," *Cognition,* vol. 173, pp. 43-59, Apr. 2018.

[244] Yingxu Wang, Newton Howard, Janusz Kacprzyk, Ophir Frieder, Phillip Sheu, Rodolfo A. Fiorini, Marina L. Gavrilova, Shushma Patel, Jun Peng and Bernard Widrow, "Cognitive Informatics: Towards Cognitive Machine Learning and Autonomous Knowledge Manipulation," *International Journal of Cognitive Informatics and Natural Intelligence (IJCINI),* vol. 12, no. 1, 2018.

[245] IBM-Research, "Cognitive Computing," IBM, 2015. [Online]. Available: http://www.research.ibm.com/cognitive-computing/#fbid=D_rsB_1iSZi. [Accessed 2 Sep. 2015].

[246] George A. Miller, "The cognitive revolution: a historical perspective," *Trends in Cognitive Sciences,* vol. 7(3), pp. 141-144, Mar. 2003.

[247] Tom Griffiths, "Manifesto for a new (computational) cognitive revolution," *Cognitiion,* pp. 21-23, Feb. 2015.

[248] Witold Kinsner, "Challenges in the design of adaptive, intelligent and cognitive systems," in *proc. of 6th IEEE International Conference on Cognitive Informatics*, Lake Tahoo, CA, USA, Aug. 2007.

[249] Yingxu Wang, Du Zhang and Witold Kinsner, "Advances in the Fields of Cognitive Informatics and Cognitive Computing," in *Advances in Cognitive Informatics and Cognitive Computing*, vol. SCI 323, Springer Verlag, 2010, pp. 265-295.

[250] Shelly XiaonanWu and Wolfgang Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *Applied Soft Computing,* vol. 10, no. 1, pp. 1-35, Jan. 2010.

[251] Witold Kinsner, "Towards cognitive security systems," in *proc. of IEEE 11th International Conference on Cognitive Informatics & Cognitive Computing*, Kyoto, Japan, Aug. 2012.

[252] Simon S. Haykin, Cognitive Dynamic Systems: Perception-Action Cycle, Cambridge, UK: Cambridge University Press, 2012.

[253] Pentti O. Haikonen, The Cognitive Approach to Consious Machines, Imprint Academic, 2003.

[254] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel and Muttukrishnan Rajarajan, "A survey of intrusion detection techniques in Cloud," *Journal of Network and Computer Applications,* vol. 36, no. 1, pp. 42-57, Jan. 2013.

[255] P.K. Harmer, P.D. Williams, G.H. Gunsch and G.B. Lamont, "An artificial immune system architecture for computer security applications," *IEEE Transactions on Evolutionary Computation,* vol. 6, no. 3, pp. 252-280, Jun. 2002.

[256] Jung Won Kim, "Integrating artificial immune algorithms for intrusion detection (Ph.D. Dissertation)," Department of Computer Science, University College London, London, England, 2002.

[257] Witold Kinsner, "Complexity and its measures in cognitive and other complex systems," in *proc. of the IEEE International Conference on Cognitive Informatics and Cognitive Computing*, Stanford, CA, USA, Aug. 2008.

[258] Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "Multifractal singularity spectrum for cognitive cyber defence in internet time series," *International Journal of Software Science and Computational Intelligence (IJSSCI),* vol. 7, no. 3, pp. 17-45, 2015.

[259] Henri Cohen and Claire Lefebvre, Handbook of Categorization in Cognitive Science, Elsevier, 2017, pp. 141-163.

[260] Matthias Rauterberg, "A method of a quantitative measurement of cognitive complexity," in *proc. of the 6th European Conference on Cognitive Ergonomics (ECCE 1992)*, Eindhoven, Netherlands, Jan. 1992.

[261] Charles H. Bennet, "How to define complexity in physics, and why," in *Complexity, Entropy, and the Physics of Information*, Oxford, UK, Addison-Wesley, 1990, pp. 137-148.

[262] Lourdes Mattos Brasil, Fernando Mendes de Azevedo, Jorge Muniz Barreto and Monique Noirhomme-Fraiture, "Complexity and cognitive computing," *Methodology and Tools in Knowledge-Based Systems* , vol. 1415, pp. 408-417, Jul. 2005.

[263] Bruce Edmonds, "Syntactic measures of complexity (Ph.D. Dissertation)," University of Manchester, Manchester, UK, 1999.

[264] Witold Kinsner, "System complexity and its measures: How complex is complex.," *Advances in Cognitive Informatics and Cognitive Computing*, vol. 323, pp. 265-295, 2010.

[265] Scott E. Jasper, "U.S. cyber threat intelligence sharing frameworks," *International Journal of Intelligence and CounterIntelligence*, pp. 53-65, Nov 2016.

[266] Fahmida Y. Rashid, "How IBM's Watson will change cybersecurity," Nov 2016. [Online]. Available: http://www.infoworld.com.

[267] Kaj Grahn, Magnus Westerlund and Goran Pulkkis, "Analytics for network security: A survey and taxonomy," in *Information Fusion for Cyber-Security Analytics*, vol. 691, Springer, Oct. 2016, pp. 175-193.

[268] Bhavani Thuraisingham, Murat Kantarcioglu, Kevin Hamlen, Latifur Khan, Tim Finin, Anupam Joshi, Tim Oates and Elisa Bertino, "A data driven approach for the science of cyber security: Challenges and directions," in *proc. of IEEE 17th International Conference on Information Reuse and Integration*, Pittsburgh, PA, USA, Jul. 2016.

[269] Robin Ruefle, Audrey Dorofee and David Mundie, "Computer security incident response team development and evolution," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 16-26, 15 Oct Oct. 2014.

[270] Abirami Sivaprasad and Smita Jangale, "A complete study on tools & techniques for digital forensic analysis," in *proc. of 2012 IEEE International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, Kumaracoil, India, Mar. 2012.

[271] G. Mansfield, T.K. Roy and N. Shiratori, "Self-similar and fractal nature of Internet traffic data," in *proc. of 15th International Conference on Information Networking*, Beppu City, Oita, Japan, Feb. 2001.

[272] D. Chakraborty, A. Ashir, T. Suganuma, G. Mansfield Keeni, T. K. Roy and N. Shiratori, "Self-similar and fractal nature of internet traffic," *International Journal of Network Management*, vol. 14, no. 2, pp. 119-129, Mar. 2004.

[273] Gyorgy Terdik and Tibor Gyires, "Does the Internet still demonstrate fractal nature?," in *proc. of 8th. International Conference on Networks*, Gosier, Guadeloupe, Mar. 2009.

[274] Muhammad Salman Khan, Ken Ferens and Witold Kinsner, "Multifractal singularity spectrum for cognitive cyber defence in internet time series," *International Journal of Software Science and Computational Intelligence (IJSSCI) 7(3)*, vol. 7, no. 3, pp. 17-45, 2015.

[275] Eung-Soo Kim, Masaki San and Yasuji Sawada, "Fractal Neural Network: Computational performance as an associative memory," *Progress of Theoretical Physics,* vol. 89, no. 5, pp. 965-972, May 1993.

[276] Erhard Bieberich, "Recurrent fractal neural networks: a strategy for the exchange of local and global information processing in the brain," *Biosystems,* vol. 66, no. 3, pp. 145-164, Sep. 2002.

[277] Li Zhao, Weidong Li, Liqing Geng and Yanzhen Ma, "Artificial neural networks based on fractal growth," *Advances in Automation and Robotics,* vol. 2, pp. 323-330, Dec. 2011.

[278] Benoit B. Mandelbrot, Fractals: Form, Chance and Dimension, Freeman, 1977.

[279] Witold Kinsner, "A unified approach to fractal dimensions," *International Journal of Cognitive Informatics and Natural Intelligence (IJCINI),* vol. 1, no. 4, pp. 26-46, 2007.

[280] Saipraneeth Gouravaraju and Ranjan Ganguli, "Estimating the Hausdorff–Besicovitch dimension of boundary of basin of attraction in helicopter trim," *Applied Mathematics and Computation,* vol. 218, no. 21, pp. 10435-10442, May 2012.

[281] Witold Kinsner, Graduate lectures of Chaos and Fractal Engineering course at University of Manitoba, Canada, Winnipeg, Manitoba, Canada: Witold Kinsner, Winter 2015.

[282] Paul Embrechts and Makoto Maejima, Selfsimilar Processes, Princeton University Press, 2002.

[283] Peng Zhang, Herb Barad and Andrew Martinez, "Fractal dimension estimation of fractional Brownian motion," in *IEEE proceedings of Southeastcon*, 1990.

[284] Joao B. Florindo and Odemir M. Bruno , "Fourier fractal descriptors for colored texture analysis," *Advanced Concepts for Intelligent Vision Systems,* vol. 6915, pp. 284-292, Aug. 2011.

[285] Joao B. Florindo and Odemir M. Bruno, "Closed contour fractal dimension estimation by the fourier transform," *Chaos, Solitons and Fractals,* vol. 44, no. 10, pp. 851--861, Oct. 2011.

[286] Michael Potter and Witold Kinsner, "Multifractal characterization of synthetic ECG in the presence of coloured noise," in *proc. of IEEE Canadian Conference on Electrical and Computer Engineering*, Ontario, Canada, Nov. 2004.

[287] Witold Kinsner, *Graduate lectures on Fractal and Chaos Engineering,* Winnipeg, MB, Canada, 2015.

[288] Ivan Gutman and Oskar E. Polansky, "Fundamentals of graph theory," *Mathematical Concepts in Organic Chemistry,* pp. 23-41, 1986.

[289] Ch. Sobhan Babu and Ajit A. Diwan, "Subdivisions of graphs: A generalization of paths and cycles," *Discrete Mathematics,* vol. 308, no. 19, pp. 4479-4486, Oct. 2008.

[290] G. Blelloch and M. Reid-Miller, "Chapter 9: Graphs: Definition, Applications,Representation," School of Computer Science - Carnegie Mellon University, USA, Spring 2014. [Online]. Available: http://www.cs.cmu.edu/afs/cs/academic/class/15210-s14/www/lectures/graphs.pdf. [Accessed 3 Feb. 2018].

[291] Jeremy Martin, "Complete graphs (Math 105 - Topics in Mathematics - Fall 2011 Course Chapter 6, Part 2)," Department of Mathematics, University of Kansas, [Online]. Available: http://people.ku.edu/~jlmartin/courses/math105-F11/Lectures/chapter6-part2.pdf. [Accessed 3 Oct. 2017].

[292] Grant A. Cheston and Tjoen Seng Jap, "A survey of the algorithmic properties of simplicial, upper bound and middle graphs," *Journal of Graph Algorithms and Applications,* vol. 10, no. 2, pp. 159-190, Jan. 2006.

[293] Ioannis G.Tollis, "Connectivity in Graph (Course HY-583 Graph Algorithms)," Computer Science Department, University of Crete, Greece, 22 Sep. 2014. [Online]. Available: http://www.csd.uoc.gr/~hy583/papers/ch17.pdf. [Accessed 3 Jan. 2018].

[294] Robert Sedgewick and Kevin Wayne, Undirected Graph, Addison-Wesley Professional, 2011.

[295] Douglas B. West, Introduction to Graph Theory, 2 ed., Pearson, Sep. 2000.

[296] Wu Guohua, "Basics of Graph Theory (Summer 2016 Course)," Division of Mathematical Sciences, School of Physical & Mathematical Science, College of Science, Nanyang Technological University, Singapore, 2016.

[297] Ravindra B. Bapat, Graphs and Matrices, Springer-Verlag London, 2014.

[298] Michael Freeze, "Lecture Notes on Adjacency and Incidence Matrices (course MAT 375. Combinatorics)," Matheamtics Department - University of North Carolina at Wilmington, Fall 2015. [Online]. Available: https://mathcourses.nfshost.com/archived-courses/mat-375-001-2015-fall/lectures/lec-23-adjacency-and-incidence-matrices.pdf. [Accessed 4 May 2018].

[299] Jonathan L. Gross and Jay Yellen, Graph Theory and its Application, Chapman and Hall, 1999.

[300] D. A. Holton and J. Sheehan, The Petersen Graph, Cambridge University Press, 1993.

[301] Jonathan L. Gross and Thomas W. Tucker, Topological Graph Theory, Dover Publications, Jun. 2012.

[302] Gabriel Valiente, Algorithms on Trees and Graphs, Springer-Verlag Berlin Heidelberg, 2002.

[303] Leman Akoglu, Hanghang Tong and Danai Koutra, "Graph based anomaly detection and description: A survey," *Data Mining and Knowledge Discovery,* vol. 29, no. 3, p. 626–688, May 2015.

[304] David Easley and Jon Kleinberg, "Graphs," in *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*, Cambridge University Press, 2010.

[305] Ian Robinson, Jim Webber and Emil Eifrem, Graph Databases: New Opportunities for Connected Data, 2 ed., O'Reilly Media, Inc., 2015.

[306] Arijit Khan, Sourav S. Bhowmick and Francesco Bonchi, "Summarizing Static and Dynamic Big Graphs," *proc. of the VLDB Endowment*, vol. 10, no. 12, pp. 1981-1984, 2017.

[307] K.J. Wijnands, "Using endpoints process information for malicious behavior detection," TU Delft, Delft, Netherlands, Sep. 2015.

[308] Jon Clayden, "Connectomics and Graph Theory (DIBS Teaching Seminar)," Neuroimaging and Biophysics, Institute of Child Health, University College London, 18 Nov. 2016. [Online]. Available: http://www.homepages.ucl.ac.uk/~sejjjd2/slides/Connectomics2016.pdf. [Accessed 2 Dec. 2017].

[309] HongYun Cai, Vincent W. Zheng and Kevin Chang, "A comprehensive survey of Graph Embedding: Problems, techniques and applications," *IEEE Transactions on Knowledge and Data Engineering,* pp. 1041-4347, Feb. 2018.

[310] Nadya T. Bliss and Matthew C. Schmidt , "Confronting the Challenges of Graphs and Networks," *MIT Lincoln Laboratory Journal*, vol. 20, no. 1, May 2013.

[311] Jose Cadena, Feng Chen and Anil Vullikanti, "Graph anomaly detection based on Steiner connectivity and density," *Proceedings of the IEEE*, vol. 106, no. 5, pp. 829 - 845, May 2018.

[312] Stephen Ranshous, Shitian Shen, Danai Koutra, Steve Harenberg, Christos Faloutsos and Nagiza F. Samatova, "Anomaly detection in dynamic networks: A survey," *WIREs Computational Statistics*, vol. 7, no. 3, pp. 223-247, 2015.

[313] Dmitry Vengertsev and Hemal Thakkar, "Anomaly Detection in Graph: Unsupervised Learning, Graph-based Features and Deep Architecture," Social and Information Network Analysis - Stanford, Stanford, California, USA, 2015.

[314] Keith Henderson, Tina Eliassi-Rad, Christos Faloutsos, Leman Akoglu, Lei Li, Koji Maruhashi, B. Aditya Prakash and Hanghang Tong, "Metric forensics: a multi-level approach for mining volatile graphs," in *proc. of 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, New York, NY, USA, Jul. 2010.

[315] Luca Becchetti, Carlos Castillo, Debora Donato, Stefano Leonardi and Ricardo Baeza-Yates, "Link-based characterization and detection of Web Spam," in *proc. of the Second International Workshop on Adversarial Information Retrieval on the Web*, Seattle, Washington, USA, Aug. 2006.

[316] Qi Ding, Natallia Katenka, Paul Barford, Eric Kolaczyk and Mark Crovella, "Intrusion as (anti)social communication: characterization and detection," in *proc. of 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Beijing, China, Aug. 2012.

[317] Leman Akoglu, Pedro O. S. Vaz de Melo and Christos Faloutsos, "Quantifying reciprocity in large weighted communication networks," in *proc. of 16th Pacific-Asia Conference on Advances in Knowledge Discovery and Data Mining - Volume Part II*, Kuala Lumpur, Malaysia, Jun. 2012.

[318] Mangesh Gupte and Tina Eliassi-Rad, "Measuring tie strength in implicit social networks," in *proc. of the 4th Annual ACM Web Science Conference*, Evanston, Illinois, USA, Jun. 2012.

[319] Sergey Brin and Lawrence Page, "The anatomy of a large-scale hypertextual Web search engine," *proc. of the Seventh International Conference on World Wide Web 7*, vol. 30, no. 1, pp. 107-117, Apr. 1998.

[320] Jimeng Sun, Huiming Qu, D. Chakrabarti and C. Faloutsos, "Neighborhood formation and anomaly detection in bipartite graphs," in *proc. of Fifth IEEE International Conference on Data Mining*, Houston, TX, USA, Nov. 2005.

[321] Deepayan Chakrabart, "Autopart: parameter-free graph partitioning and outlier detection," in *proc. of the 8th European Conference on Principles and Practice of Knowledge Discovery in Databases* , Pisa, Italy, Sep. 2004.

[322] Caleb C. Noble and Diane J. Cook., "Graph-based anomaly detection," in *proc. of 9th ACM International Conference on Knowledge Discovery and Data Mining*, Washington, DC, USA, Aug. 2003.

[323] Chao Liu, Xifeng Yan, Hwanjo Yu, Jiawei Han and Philip S. Yu, "Mining Behavior Graphs for “Backtrace” of Noncrashing Bugs," in *proc. of the 2005 SIAM International Conference on Data Mining*, Newport Beach, CA, USA, Apr. 2005.

[324] Zhan Chuan, Lu Xianliang, Hou Mengshu and Zhou Xu, "A LVQ-based neural network anti-spam email approach," *ACM SIGOPS Operating Systems Review*, vol. 39, no. 1, pp. 34-39, Jan. 2005.

[325] F. Harary and G. Gupta, "Dynamic graph models," *Mathematical and Computer Modelling: An International Journal*, vol. 25, no. 7, pp. 79-87, Apr. 1997.

[326] Camil Demetrescu, David Eppstein, Zvi Galil and Giuseppe F. Italiano, "Dynamic graphs," in *Algorithms and Theory of Computation Handbook*, Chapman & Hall, 2010.

[327] Valery Guralnik and Jaideep Srivastava, "Event detection from time series data," in *proc. of Fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Diego, California, USA, Aug. 1999.

[328] Cemal Cagatay Bilgin and Bulent Yener, "Dynamic network evolution: Models, clustering, anomaly detection," *IEEE Networks*, 2006.

[329] Leman Akoglu and Christos Faloutsos, "Event detection in time series of mobile communication graphs," in *proc. of 27th Army Science Conference*, Orlando, Florida, USA, Dec. 2010.

[330] Brandon Pincombe, "Anomaly detection in time series of graphs using ARMA processes," *ASOR Bulletin*, vol. 24, no. 4, Jan. 2005.

[331] Tsuyoshi Ide and Hisashi Kashima, "Eigenspace-based anomaly detection in computer systems," in *proc. of 10th ACM International Conference on Knowledge Discovery and Data Mining*, Seattle, WA, USA, Aug. 2004.

[332] Hanghang Tong and Ching-Yung Lin, "Non-negative residual matrix factorization: problem definition, fast solutions, and applications," *Statistical Analysis and Data Mining*, vol. 5, no. 1, pp. 3-15, Feb. 2012.

[333] Jimeng Sun, Dacheng Tao and Christos Faloutsos, "Beyond streams and graphs: dynamic tensor analysis," in *proc. of 12th ACM International Conference on Knowledge Discovery and Data Mining (SIGKDD)*, Philadelphia, PA, USA, Aug. 2006.

[334] Charu Aggarwal and Karthik Subbian, "Evolutionary network analysis: A survey," *ACM Computing Surveys*, vol. 47, no. 1, p. New York, Jul. 2014.

[335] William Eberle and Lawrence Holder, "Identifying anomalies in graph streams using change detection," in *proc. of KDD Workshop on Mining and Learning in Graphs*, San Francisco, CA, USA, Aug. 2016.

[336] Manish Gupta, Jing Gao, Yizhou Sun and Jiawei Han, "Integrating community matching and outlier detection for mining evolutionary community outliers," in *proc. of 18th ACM International Conference on Knowledge Discovery and Data Mining*, Beijing, China, Aug. 2012.

[337] Leto Peel and Aaron Clauset, "Detecting change points in the large-scale structure of evolving networks," in *proc. of 29th International Conference on Artificial Intelligence*, Austin, TX, USA, Mar. 2014.

[338] Carey E. Priebe, John M. Conroy, David J. Marchett and Youngser Park, "Scan statistics on Enron graphs," *Computational & Mathematical Organization Theory*, vol. 11, no. 3, pp. 229-247, Oct. 2005.

[339] Joseph I. Naus, "Approximations for distributions of scan statistics," *Journal of the American Statistical Association*, vol. 77, no. 377, pp. 177-183, Mar. 1982.

[340] Maurice C. Bryson , "Heavy-Tailed Distributions: Properties and Tests," *Technometrics,* vol. 16, no. 1, pp. 61-68, 1974.

[341] Frank J. Massey Jr. , "The Kolmogorov-Smirnov Test for goodness of fit," *Journal of the American Statistical Association,* vol. 46, no. 253, 1951.

[342] Hubert Lilliefors, "On the Kolmogorov–Smirnov test for the exponential distribution with mean unknown," *Journal of the American Statistical Association,* vol. 64, pp. 387-389, 1969.

[343] Hubert W. Lilliefors , "On the Kolmogorov-Smirnov Test for normality with mean and variance unknown," *Journal of the American Statistical Association,* vol. 62, no. 318, 1967.

[344] E. S. Pearson, Karl Pearson and H. O. Hartley, Biometrika Tables for Statisticians, vol. 2, Cambridge University Press, 1954, p. 117–123.

[345] NIST, "Kolmogorov-Smirnov Goodness-of-Fit Test," Engineering Statistics Handbook, [Online]. Available: https://www.itl.nist.gov/div898/handbook/eda/section3/eda35g.htm. [Accessed 14 Jun. 2018].

[346] Statistics How To , "Kolmogorov-Smirnov Goodness of Fit Test," Statistics How To - Statistics for the rest of us!, [Online]. Available: http://www.statisticshowto.com/kolmogorov-smirnov-test/#pvalue. [Accessed 13 Jun. 2018].

[347] Student, "The probable error of a mean," *Biometrika,* vol. 6, no. 1, pp. 1-25, Mar. 1908.

[348] Joan Fisher Box, "Guinness, Gosset, Fisher, and Small Samples," *Statistical Science,* vol. 2, no. 1, pp. 45-52, 1987.

[349] Sander Greenland, Stephen J. Senn, Kenneth J. Rothman, John B. Carlin, Charles Poole, Steven N. Goodman and Douglas G. Altman, "Statistical tests, P values, confidence intervals, and power: a guide to misinterpretations," *European Journal of Epidemiology,* vol. 31, p. 337–350, May 2016.

[350] Karl Pearson, "On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling," *Philosophical Magazine,* vol. 50, no. 5, pp. 157-175, 1900.

[351] Todd Michael Franke, Timothy Ho and Christina A. Christie, "The Chi-Square Test - Often Used and More Often Misinterpreted," *American Journal of Evaluation,* vol. 33, no. 3, Nov. 2011.

[352] Hubert Lilliefors , "On the Kolmogorov–Smirnov test for normality with mean and variance unknown," *Journal of the American Statistical Association,* vol. 62, pp. 399-402, 1967.

[353] Nornadiah Mohd Razali, "Power comparisons of Shapiro-Wilk, Kolmogorov-Smirnov, Lilliefors and Anderson-Darling tests," *Journal of Statistical Modeling and Analytics,* vol. 2, no. 1, pp. 21-33, 2011.

[354] Gerard E. Dallal and Leland Wilkinson, "An analytic approximation to the distribution of Lilliefors's test statistic for normality," *The American Statistician,* vol. 40, no. 4, pp. 294-296, Nov. 1986.

[355] Kevin P. Balanda and H.L. MacGillivray, "Kurtosis: A critical review," *The American Statistician,* vol. 42, no. 2, pp. 111-119, May 1988.

[356] Ian H. Witten , Eibe Frank, Mark A. Hall and Christopher J. Pal, Data Mining: Practical Machine Learning Tools and Techniques, 4 ed., Elsevier, Nov. 2016.

[357] Garima, Hina Gulati and P. K. Singh, "Clustering techniques in data mining: A comparison," in *proc. of IEEE 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, Mar. 2015.

[358] Nikhit Mago, Rudresh D. Shirwaikar, U. Dinesh Acharya, K. Govardhan Hegde, Leslie Edward S. Lewis and M. Shivakumar, "Partition and Hierarchical Based Clustering Techniques for Analysis of Neonatal Data," in *proc. of International Conference on Cognition and Recognition*, Sep. 2017.

[359] Qingchen Zhang, Laurence T.Yang, Zhikui Chen and Peng Li, "High-order possibilistic c-means algorithms based on tensor decompositions for big data in IoT," *Information Fusion*, vol. 39, pp. 72-80, Apr. 2017.

[360] Moises Noe Sanchez Garcia, "Fractal dimension for clustering and unsupervised and supervised feature selection," Cardiff University, Cardiff, Wales, U.K., Mar. 2011.

[361] S. Santini and R. Jain, "Similarity measures," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 21, no. 9, pp. 871 - 883, Sep. 1999.

[362] David Martin Ward Powers, "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation," *International Journal of Machine Learning Technology*, vol. 2, no. 1, pp. 37-63, Dec. 2011.

[363] Michael D. Rich, Robert F. Mills, Thomas E. Dube and Steven K. Rogers, "Evaluating Machine Learning Classifiers for Defensive Cyber Operations," *The Journal of the Military Cyber Professionals Association*, vol. 2, no. 1, 2016.

[364] Matt Weinberger, "The Equifax breach resulted in the leak of 56,200 drivers' licenses, passports, and other forms of ID," Insider Inc., 8 May 2018. [Online]. Available: http://www.businessinsider.com/equifax-breach-check-details-update-2018-5. [Accessed 19 Jun. 2018].

[365] Elias Bou-Harb, Walter Lucia, Nicola Forti, Sean Weerakkody, Nasir Ghani and Bruno Sinopoli, "Cyber meets control: A novel federated approach for resilient CPS leveraging real cyber threat intelligence," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 198 - 204, May 2017.

[366] Guofei Gu, Vinod Yegneswaran, Phillip Porras, Jennifer Stoll and Wenke Lee, "Active botnet probing to identify obscure command and control channels," in *proc. of 2009 Annual Computer Security Applications Conference*, Honolulu, HI, USA, Dec. 2009.

[367] Shih-Yao Dai and Sy-Yen Kuo, "MAPMon: A host-based malware detection tool," in *proc. of 13th Pacific Rim International Symposium on Dependable Computing*, Melbourne, Qld., Australia, Dec. 2007.

[368] Lucian Constantin, "Hacking Team's malware uses a UEFI rootkit to survive operating system reinstalls," PCWorld , 14 Jul. 2015. [Online]. Available: https://www.pcworld.com/article/2948092/security/hacking-teams-malware-uses-uefi-rootkit-to-survive-os-reinstalls.html. [Accessed 19 Jun. 2018].

[369] Oracle, "Oracle VM VirtualBox," Oracle Corporation, [Online]. Available: http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html. [Accessed 5 Mar. 2017].

[370] MySQL, "MySQL Community Server 5.7.11," Oracle Corporation, [Online]. Available: https://dev.mysql.com/downloads/mysql/.

[371] MSDN Library, "UuidCreate function," [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/aa379205(v=vs.85).aspx. [Accessed 27 Nov. 2017].

[372] MSDN Library, "CreateToolhelp32Snapshot function," [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/ms682489(v=vs.85).aspx. [Accessed 27 Nov. 2017].

[373] MSDN Library, "OpenProcess function," [Online]. Available: https://msdn.microsoft.com/en-ca/library/windows/desktop/ms684320(v=vs.85).aspx. [Accessed 5 Mar. 2016].

[374] Raimund Hocke and Open Source Community, "Sikulix 1.1.1 Desktop Automating Software," Sikuli, 2017.

[375] Visgean Skeloru, "Zeus," GITHub, 23 Feb. 2014. [Online]. Available: https://github.com/Visgean/Zeus. [Accessed 19 Feb. 2018].

[376] Yuval tisf Nativ and Shahak Shalev, "A repository of LIVE malwares for your own joy and pleasure," theZoo at GitHub, 14 Dec. 2014. [Online]. Available: https://github.com/ytisf/theZoo. [Accessed 3 Sep. 2017].

[377] Marco Riccardi, Roberto Di Pietro and Jorge Aguila Vila, "Taming Zeus by leveraging its own crypto internals," in *proc. of IEEE eCrime Researchers Summit*, San Diego, CA, USA, Nov. 2011.

[378] H. Binsalleeh, T. Ormerod and A. Boukhtouta, "On the analysis of the Zeus botnet crimeware toolkit," in *proc. of IEEE 2010 8th International Conference on Privacy, Security and Trust*, Ottawa, ON, Canada, Aug. 2010.

[379] Robert Layton and Ahmad Azab, "Authorship analysis of the Zeus Botnet source code," in *proc. of IEEE 2014 Fifth Cybercrime and Trustworthy Computing Conference*, Auckland, New Zealand, Nov. 2014.

[380] Yogita Deepak Mane, "Detect and deactivate P2P Zeus bot," in *proc. of IEEE 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Delhi, India, Jul. 2017.

[381] V. Mendez-Garcia, P. Jimenez-Ramirez and M. A. Melendez-Ramirez, "Comparative analysis of banking malware," in *proc. of 2014 IEEE Central America and Panama Convention (CONCAPAN XXXIV)*, Panama City, Panama, Nov. 2014.

[382] Prashant J. Nair, David A. Roberts and Moinuddin K. Qureshi, "Citadel: Efficiently protecting stacked memory from large granularity failures," in *proc. of 47th Annual IEEE/ACM International Symposium onMicroarchitecture (MICRO)*, Cambridge, UK, Dec. 2014.

[383] Jianwen Fu, Jingfeng Xue, Yong Wang, Zhenyan Liu and Chun Shan, "Malware visualization for fine-grained classification," *IEEE Access - Internet-of-Things (IoT) Big Data Trust Management* , vol. 6, pp. 14510 - 14523, Feb. 2018.

[384] Guanhua Yan, "Finding common ground among experts' opinions on data clustering: With applications in malware analysis," in *proc. of 2014 IEEE 30th International Conference on Data Engineering (ICDE)*, Chicago, IL, USA, Apr. 2014.

[385] ESET Canada, "Win32/TrojanDownloader.Zurgop," ESET Virus Radar, Mar. 2014. [Online]. Available: http://www.virusradar.com/en/Win32_TrojanDownloader.Zurgop.BK/description. [Accessed 19 Feb. 2018].

[386] Hybrid Analysis , "Zurgop.exe," Falcon Sandbox Services and Products - Crowdstrike, Jul. 2016. [Online]. Available: https://www.hybrid-analysis.com. [Accessed 1 Mar. 2018].

[387] Christian Rossow, Christian J. Dietrich, Chris Grier, Christian Kreibich, Vern Paxson, Norbert Pohlmann, Herbert Bos and Maarten van Steen, "Prudent practices for designing malware experiments: Status quo and outlook," in *proc. of 2012 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, May 2012.

[388] Panda Security, "Alina, the Latest POS Malware," Panda Labs, Nov. 2017. [Online]. Available: https://www.pandasecurity.com. [Accessed 12 Dec. 2018].

[389] Eric Merritt, "Alina POS malware "sparks" off a new variant," Spider Labs - Trustwave, Dec. 2014. [Online]. Available: https://www.trustwave.com. [Accessed 12 Sep. 2018].

[390] Chad Robertson, "Indicators of Compromise in Memory Forensics," SANS Institute InfoSec Reading Room, Feb. 2013. [Online]. Available: https://uk.sans.org. [Accessed 1 Mar. 2018].

[391] Hybrid Analysis, "Stabuniq," Falcon Sandbox Services and Products - Crowdstrike, Jan. 2017. [Online]. Available: https://www.hybrid-analysis.com. [Accessed 4 Jan. 2018].

[392] Hybrid Analysis, "Nivdort," Falcon Sandbox Services and Products - Crowdstrike, Mar. 2016. [Online]. Available: https://www.hybrid-analysis.com. [Accessed 19 Jan. 2018].

[393] Konstantin Berlin,, "An AI Approach to Malware Similarity Analysis: Mapping the Malware Genome With a Deep Neural Network," Invincea Labs, Aug. 2016. [Online]. Available: https://www.blackhat.com. [Accessed 23 Sep. 2018].

[394] Igor Korkin and Iwan Nesterow, "Acceleration of statistical detection of Zero-Day malware in the memory dump using CUDA-Enabled GPU Hardware," in *proc. of the 11th ADFSL Conference on Digital Forensics, Security and Law*, Jun. 2016.

[395] Thorsten Eisenhofer, "Poweliks Malware – Filelessly Persistent," VMRay Threat Analysis and Detection, Aug. 2017. [Online]. Available: https://www.vmray.com/blog/poweliks-fileless-malware-analysis/. [Accessed 21 Jan. 2018].

[396] Gidon Eshel and J. Michael Steele, "The Yule Walker equations for the AR coefficients," The Wharton School, The University of Pennsylvania, [Online]. Available: http://www-stat.wharton.upenn.edu/~steele/Courses/956/Resource/YWSourceFiles/YW-Eshel.pdf. [Accessed 21 Jun. 2018].

[397] Tsay Young Lin, "Attribute (feature) completion - The theory of attributes from data mining prospect," in *proc. of IEEE International Conference on Data Mining*, Maebashi City, Japan, Dec. 2002.

[398] Wei Wang, Yan Yan and Stefan Winkler, "Category Specific Dictionary Learning for Attribute Specific Feature Selection," *IEEE Transactions on Image Processing*, vol. 25, no. 3, pp. 1465 - 1478, Jan. 2016.

[399] Aron Yu and Kristen Grauman, "Just Noticeable Differences in Visual Attributes," in *Proc. of IEEE International Conference on Computer Vision (ICCV) 2015*, Santiago, Chile, Dec. 2015.

[400] Yang Long, Li Liu and Ling Shao, "Towards Fine-Grained Open Zero-Shot Learning: Inferring Unseen Visual Features from Attributes," in *Proc. of 2017 IEEE Winter Conference on Applications of Computer Vision (WACV)*, Santa Rosa, CA, USA, Mar. 2017.

[401] Rudy Setiono and Huan Liu, "Neural-network feature selector," *IEEE Transactions on Neural Networks*, vol. 8, no. 3, pp. 654 - 662, May 1997.

[402] Huan Liu and R. Setiono, "Chi2: feature selection and discretization of numeric attributes," in *Proc. of 1995 7th. IEEE International Conference on Tools with Artificial Intelligence*, Herndon, VA, USA, Nov. 1995.

[403] Jihoon Yang and Vasant Honavar, "Feature Subset Selection Using a Genetic Algorithm," in *Feature Extraction, Construction and Selection, The Springer International Series in Engineering and Computer Science*, vol. 453, Springer, Boston, MA, 1998, pp. 117-136.

[404] A. Verikas and M. Bacauskiene, "Feature selection with neural networks," *Pattern Recognition Letters*, vol. 23, no. 11, p. 1323–1335, 2002.

[405] Maysam Toghraee, Mohammad Esmaeili and Hamid Parvin, "Evaluation neural networks on selected feature by meta heuristic algorithms," *Artifical Intelligent Systems and Machine Learning*, vol. 8, no. 3, 2016.

[406] Ganesh Ram Santhanam, Benjamin Holland, Suresh Kothari and Jon Mathews, "Interactive visualization toolbox to detect sophisticated android malware," in *proc. of 2017 IEEE Symposium on Visualization for Cyber Security*, Phoenix, AZ, USA, Oct. 2017.

[407] Louise Axon, Bushra Alahmadi, Jason Nurse, Michael Goldsmith and Sadie Creese, "Sonification in Security Operations Centres: What do security practitioners think?," in *proc. of 2018 Workshop on Usable Security at Network and Distributed System Security Symposium (NDSS)*, San Diego, California, USA, Feb. 2018.

[408] J.J.Shah, "Assessment of features technology," *Computer-Aided Design*, vol. 23, no. 5, pp. 331-343, Jun. 1991.

[409] Keith Henderson, Brian Gallagher, Lei Li , Leman Akoglu, Tina Eliassi-Rad, Hanghang Tong and Christos Faloutsos, "It's Who You Know: Graph Mining Using Recursive Structural Features," in *proc. of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Diego, California, USA, Aug. 2011.

[410] Jianbo Shi and Tomasi, "Good features to track," in *proc of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1994. Proceedings CVPR 1994*, Seattle, WA, USA, Jun. 1994.

[411] C. Lee and D.A. Landgrebe, "Feature extraction based on decision boundaries," *IEEE Transactions on Pattern Analysis and Machine Intelligence* , vol. 15, no. 4, pp. 388 - 400, Apr. 1993.

[412] A. Jain and D. Zongker, "Feature selection: evaluation, application, and small sample performance," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 2, pp. 153 - 158, Feb. 1997.

[413] Steven Cheng-Xian Li and Benjamin Marlin, "Classification of sparse and irregularly sampled time series with mixtures of expected Gaussian kernels and random features," in *proc. of the Thirty-First Conference on Uncertainty in Artificial Intelligence*, Amsterdam, Netherlands, Jul. 2015.

[414] Thomas H. Grandy, Douglas D. Garrett, Florian Schmiedek and Markus Werkle-Bergner, "On the estimation of brain signal entropy from sparse neuroimaging data," *Nature*, vol. 6, no. 23073, Mar. 2016.

[415] Songbing Tao, Nan Li, Shanbi Wei and Yi Chai, "Weighted window sliding multivariate empirical mode decomposition for online multichannel filtering," *IEEE Access*, vol. 6, pp. 43170 - 43178, Jul. 2018.

[416] Tiancheng Zhang, Dejun Yue, Yu Gu, Yi Wang and Ge Yu, "Adaptive correlation analysis in stream time series with sliding windows," *Computers & Mathematics with Applications,* vol. 57, no. 6, pp. 937-948, Mar. 2009.

[417] Evgenia S. Novikova, Yana A. Bekeneva and Andrey V. Shorov, "Towards visual analytics tasks for the security information and event management," in *proc. of 2017 IEEE International Conference Quality Management, Transport and Information Security, Information Technologies*, St. Petersburg, Russia, Sept. 2017.

[418] John J. Bruer, Joel A. Tropp, Volkan Cevher and Stephen R. Becker, "Designing Statistical Estimators That Balance Sample Size, Risk, and Computational Cost," *IEEE Journal of Selected Topics in Signal Processing,* vol. 9, no. 4, pp. 612-624, Jun. 2015.

[419] Robert M. Kaplan, David A. Chambers and Russell E. Glasgow, "Big Data and Large Sample size: A cautionary note on the potential for bias," *Clinical and Translational Science,* vol. 7, no. 4, Jul. 2014.

[420] S.J. Raudys and A.K. Jain, "Small sample size effects in statistical pattern recognition: recommendations for practitioners," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 13, no. 3, pp. 252 - 264, Mar. 1991.

[421] Ahmed Elgammal, Ramani Duraiswami, David Harwood and Larry S. Davis, "Background and foreground modeling using nonparametric kernel density estimation for visual surveillance," *proc. of IEEE,* vol. 90, no. 7, pp. 1151 - 1163, Jul. 2002.

[422] Wlodzimierz Greblicki and Adam Krzyzak, "Asymptotic properties of kernel estimates of a regression function," *Journal of Statistical Planning and Inference,* vol. 4, no. 1, pp. 81-90, 1980.

[423] P. Cheng and R. Serfling, "Asymptotic mean integrated squared errors of some nonparametric density estimators (Corresp.)," *IEEE Transactions on Information Theory,* vol. 27, no. 2, pp. 239 - 242, Mar. 1981.

[424] Lawrence T. DeCarlo, "On the meaning and use of kurtosis," *Psychological Methods,* vol. 2, no. 3, pp. 292-307, 1997.

[425] A. Mansour and C. Jutten, "What should we say about the kurtosis?," *IEEE Signal Processing Letters,* vol. 6, no. 12, pp. 321 - 322, Dec. 1999.

[426] Camillo Gentile, "Using the Kurtosis Measure to Identify Clusters in Wireless Channel Impulse Responses," *IEEE Transactions on Antennas and Propagation,* vol. 61, no. 6, pp. 3392 - 3395, Jun. 2013.

[427] Vladik Kreinovich and Olga Kosheleva, "How to Define Mean, Variance, etc., for Heavy-Tailed Distributions: A Fractal-Motivated Approach," *International Journal of Innovative Management Information & Production,* vol. 5, no. 1, pp. 1-9, Mar. 2014.

[428] Maarten L. Wijnants, R. F. A. Cox, F. Hasselman, A. M. T. Bosman and Guy Van Orden, "Does sample rate introduce an artifact in spectral analysis of continuous processes?," *Frontiers in Physiology,* vol. 3, no. 495, 2012.

[429] Witold Kinsner and Hong Zhang, "Multifractal analysis and feature extraction of DNA sequences," in *proc. of 8th IEEE International Conference on Cognitive Informatics*, Jun. 2009.

[430] Sitaram Kowtha, Laura A. Nolan and Rosemary A. Daley, "Cyber security operations center characterization model and analysis," in *proc. of IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, USA, Nov. 2012.

[431] Igor Kotenko, Artem Kuleshov and Igor Ushakov, "Aggregation of elastic stack instruments for collecting, storing and processing of security information and events," in *proc. of IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*, San Francisco, CA, USA, Aug. 2017.

[432] McAfee, "McAfee Enterprise Security Manager 10.2.0 Product Guide," McAfee LLC., 2018. [Online]. Available: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/27000/PD27452/en_US/ESM_1020_pg_0-00_en-us.pdf. [Accessed 7 October 2018].

[433] Tarun Prakash, Misha Kakkar and Kritika Patel, "Geo-identification of web users through logs using ELK stack," in *proc. of IEEE 6th International Conference - Cloud System and Big Data Engineering*, Noida, India, Jan. 2016.

[434] Spencer Engleson, "What Makes SIEMs So Challenging?," Rapid 7, 10 May 2016. [Online]. Available: https://blog.rapid7.com/2016/05/10/why-are-siems-so-hard/. [Accessed 2 October 2018].

[435] World Economic Forum, "These are the biggest risks the world faces," 2018.

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

7. Appendix

7.1 Visualization of Features for Each Malware Instance

In this subsection, visual plots of all time graph based statistical features are presented. Although discussed already in subsection 4.2.4, for convenience, these features are presented again in the following Table 94. As observed, all features are highly sparse which is represented by white space. Further, observing each feature closely reveals the fact that the malware and normal samples are highly overlapping and if not overlapping then are following the normal sample closely (diminishing inter-sample distance) in the feature space. Through visual analysis of each feature in every malware instance, it can be deduced that all these malware are successfully able to hide their presence within the statistical pattern of the normal data and therefore, as analyzed in this dissertation already, it is not possible to characterize these malware instances uniquely using any of these features separately. This trait of the selected malware instances is attributed to the high degree of mutation in their behavior inside a Windows 7 operating system and therefore, it can also be deduced that each of these features is not able to characterize this mutation behavior uniquely with traditional single scale based analysis.

Table 94: Summary of time graph features.

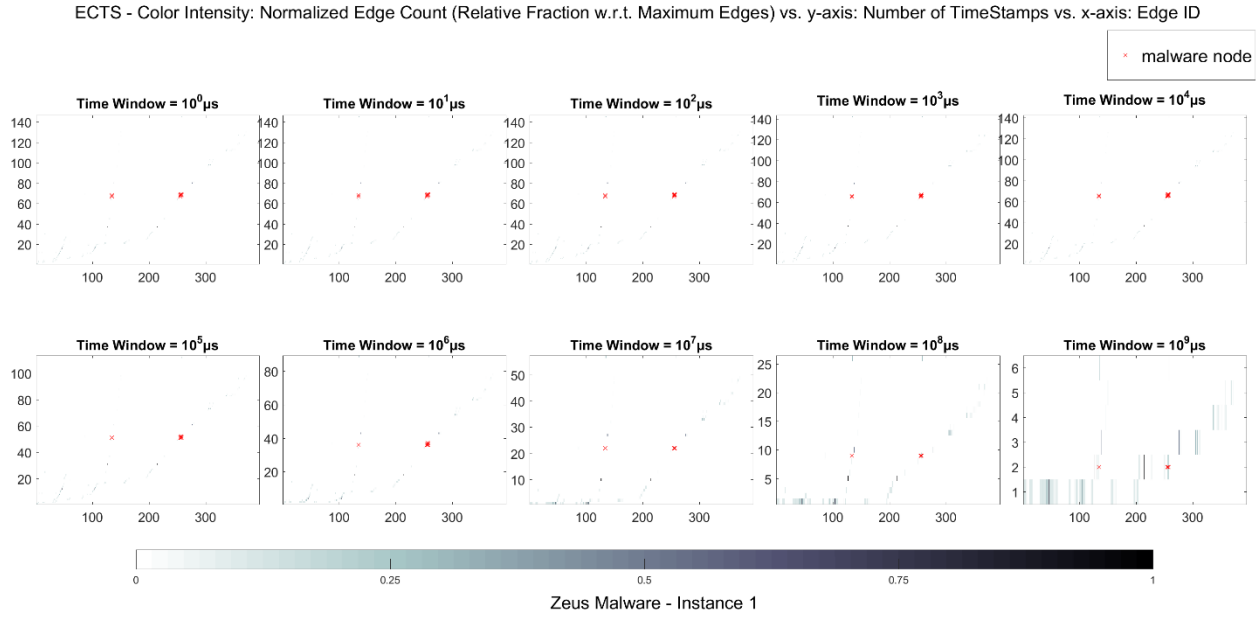
No.	Feature Definition	Feature Notation	Notation Definition
1	Edge Count	ECTS	**E**dge **C**ount vs. **T**ime **S**tamp
2	Edge Memory	EMTS	**E**dge **M**emory vs. **T**ime **S**tamp
3	Edge Time	ETSD	**E**dge **T**ime **S**tamp **D**uration
4	Edge Thread Count	ETTS	**E**dge **T**hread vs. **T**ime **S**tamp
5	Number of Edges per timestamp	TSNE	**T**ime **S**tamp vs. **N**umber of **E**dges
6	Edge Repeat	TSER	**T**ime **S**tamp vs. **E**dge **R**epeat
7	Number of Edge Memory per timestamp	TSEM	**T**ime **S**tamp vs. **E**dge **M**emory
8	Number of Edge Time per timestamp	NTSE	**T**ime **S**tamp vs. **E**dge **T**ime

9	Number of Edge Thread per timestamp	TSET	**T**ime **S**tamp vs. **E**dge **T**hread
10	Node Count	CNTS	**C**ount of **N**odes per **T**ime **S**tamp
11	Node Neighbor Count	TSNN	**T**ime **S**tamp vs. **N**ode **N**eighbor
12	Number of Nodes per timestamp	TSNC	**T**ime **S**tamp vs. **N**ode **C**ount
13	Node Repeat	TSNR	**T**ime **S**tamp vs. **N**ode **R**epeat

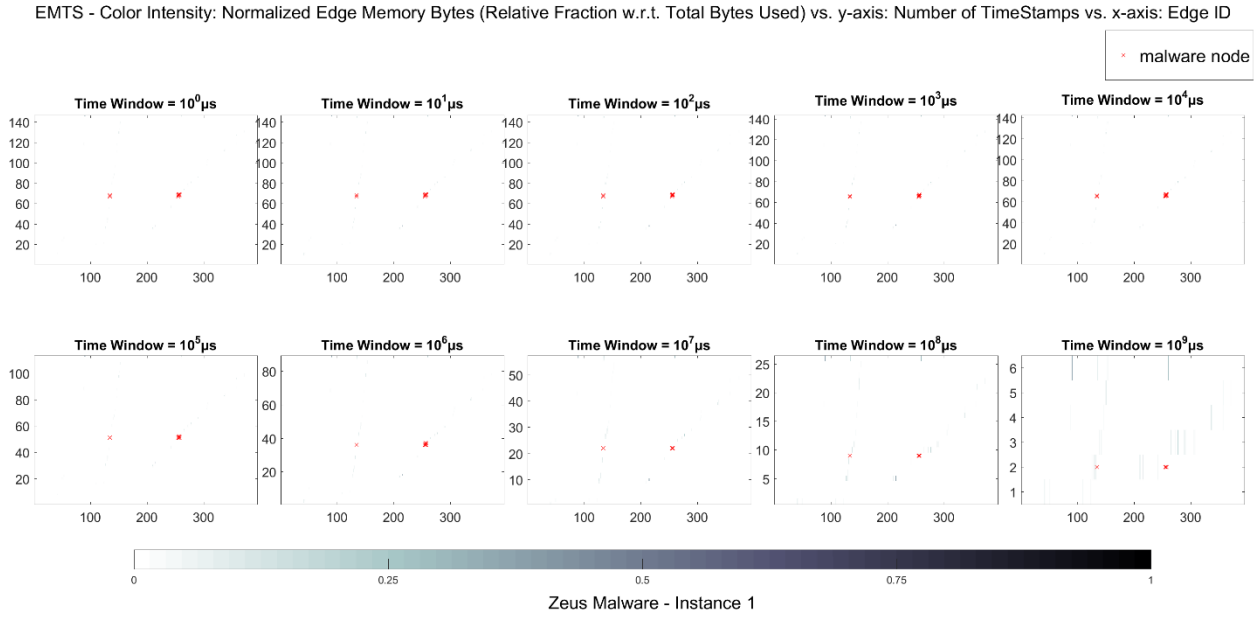
7.1.1 Zeus Malware – Instance 1

Time Graph Edge Based Features

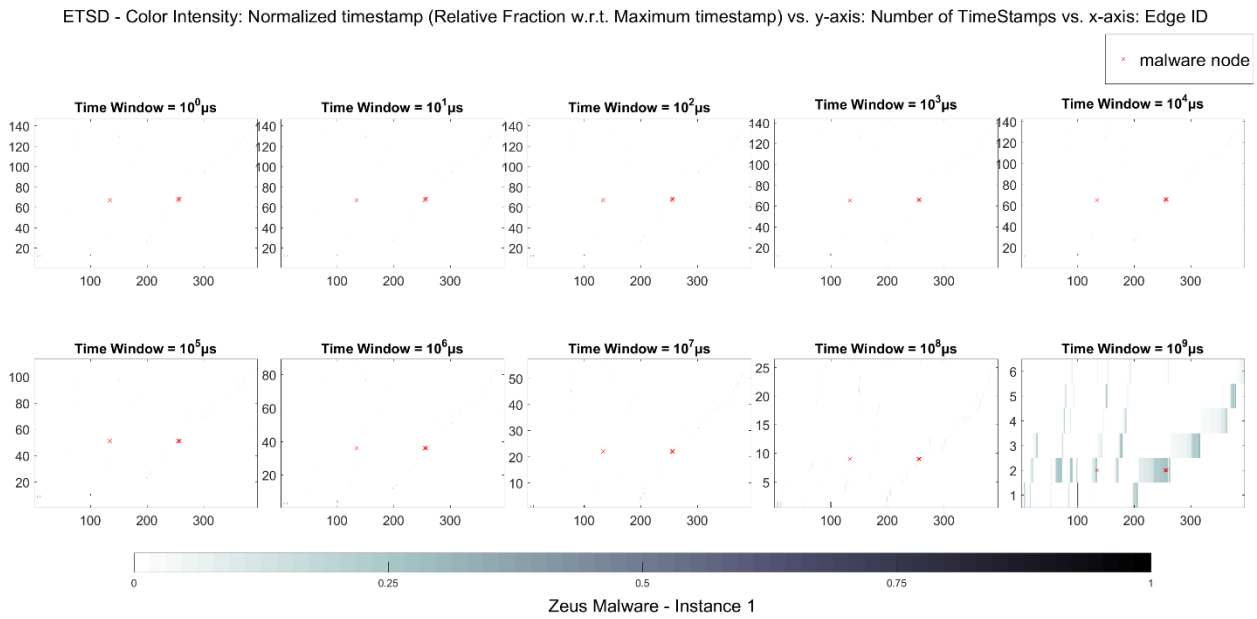
1) ECTS



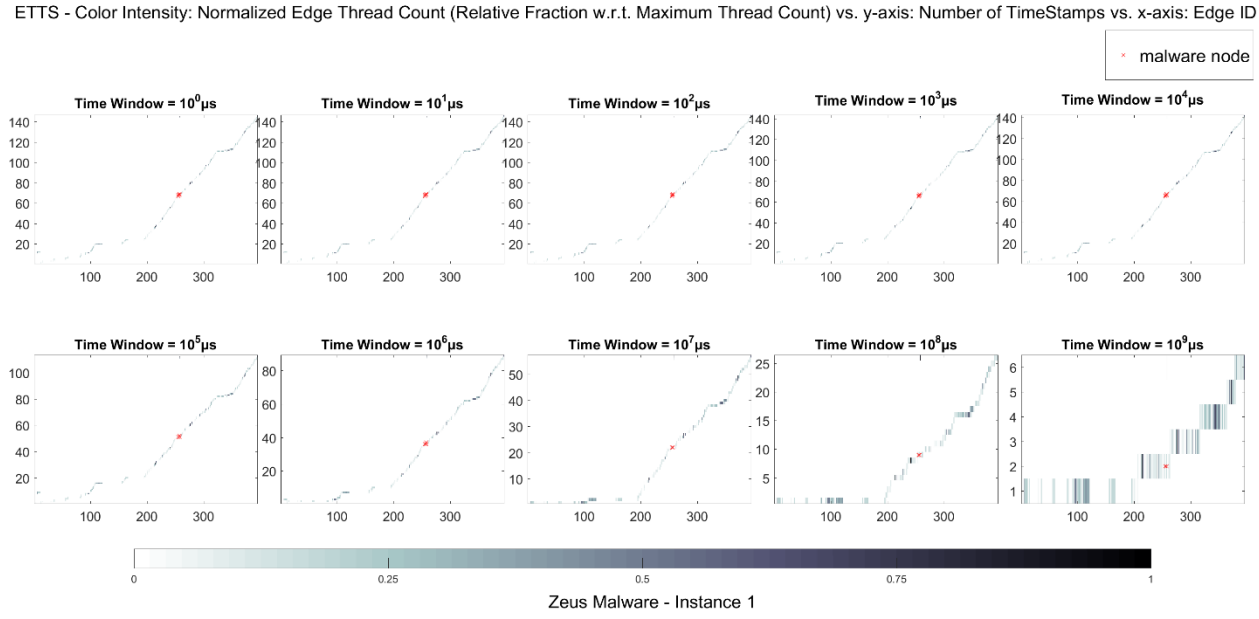
2) EMTS



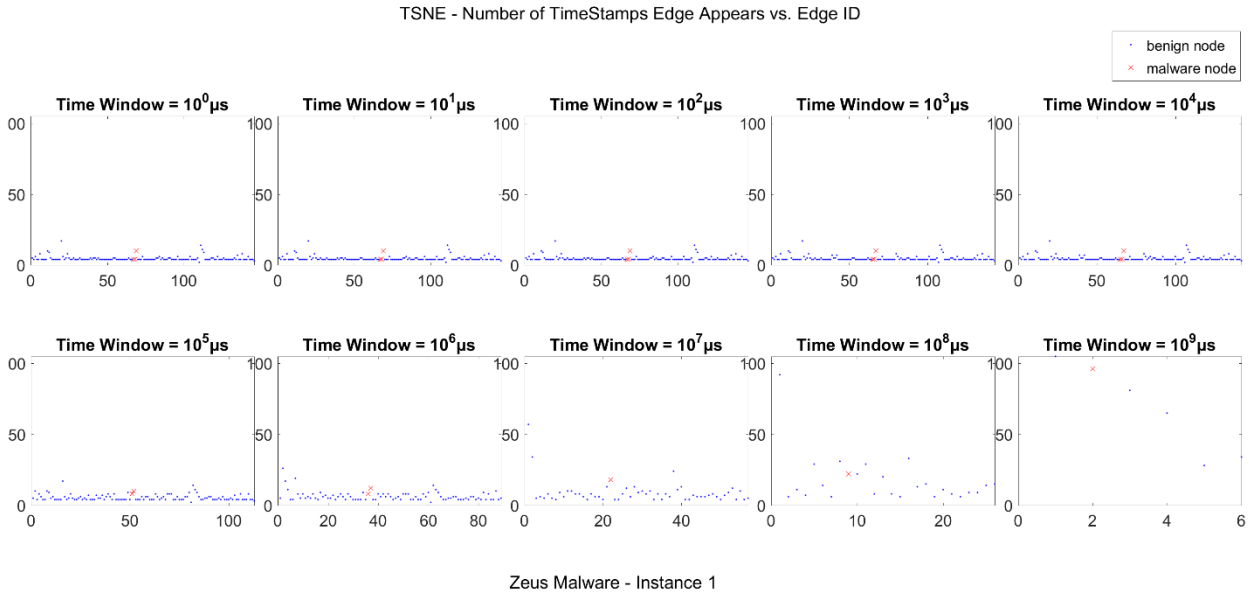
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Zeus Malware - Instance 1

4) ETTS

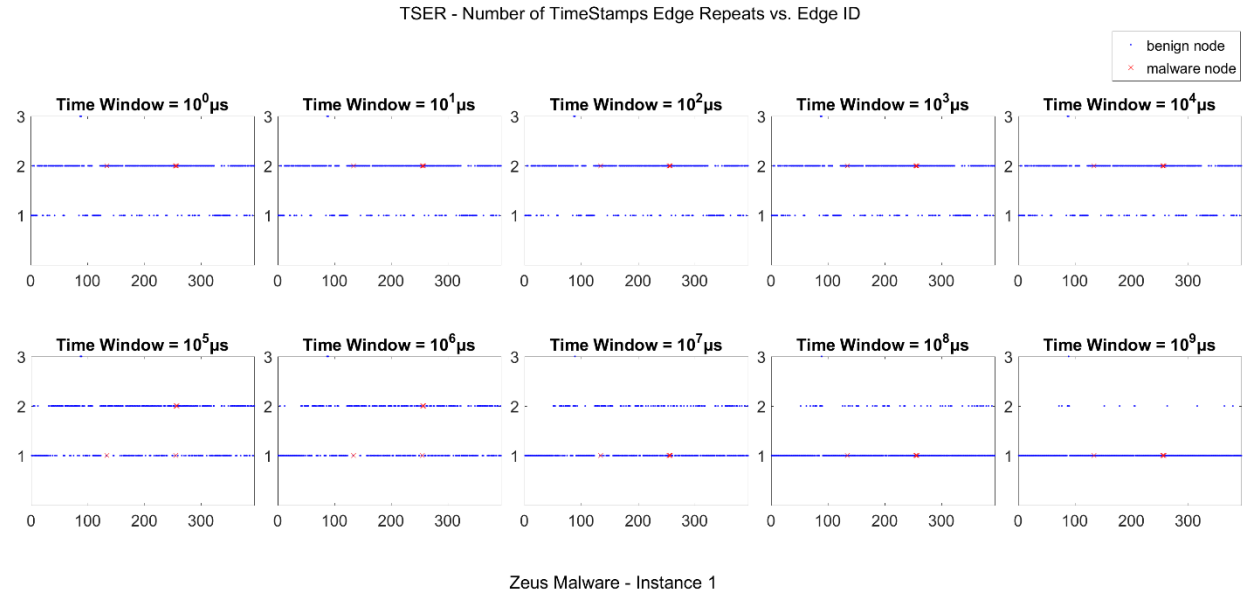

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Zeus Malware - Instance 1

5) TSNE



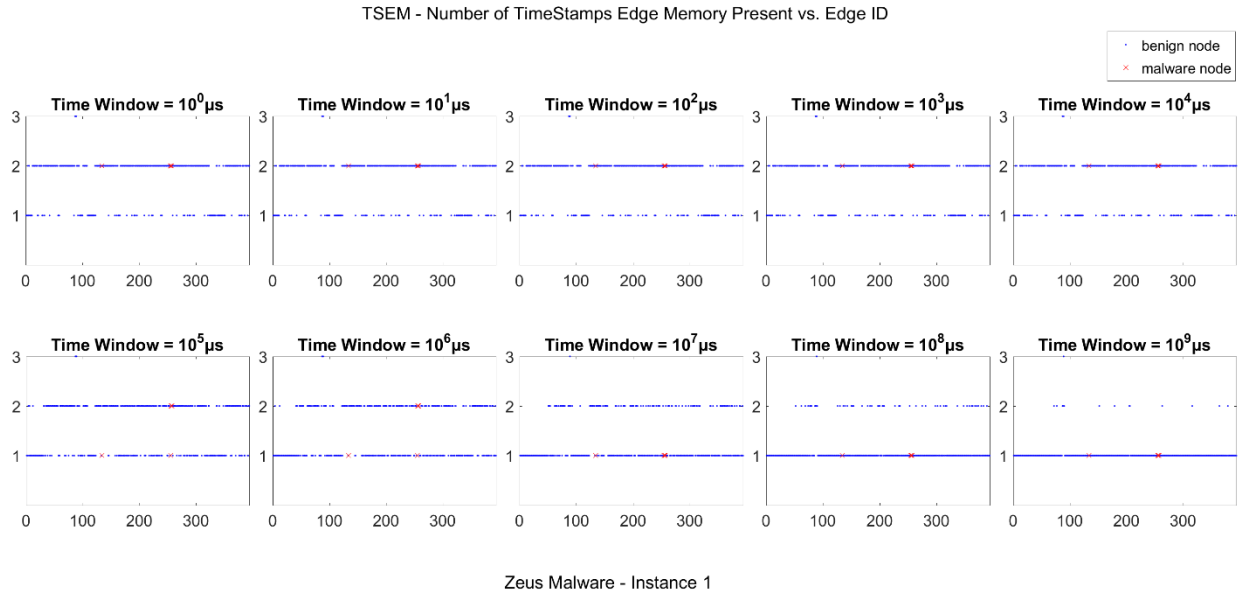
Zeus Malware - Instance 1

6) TSER

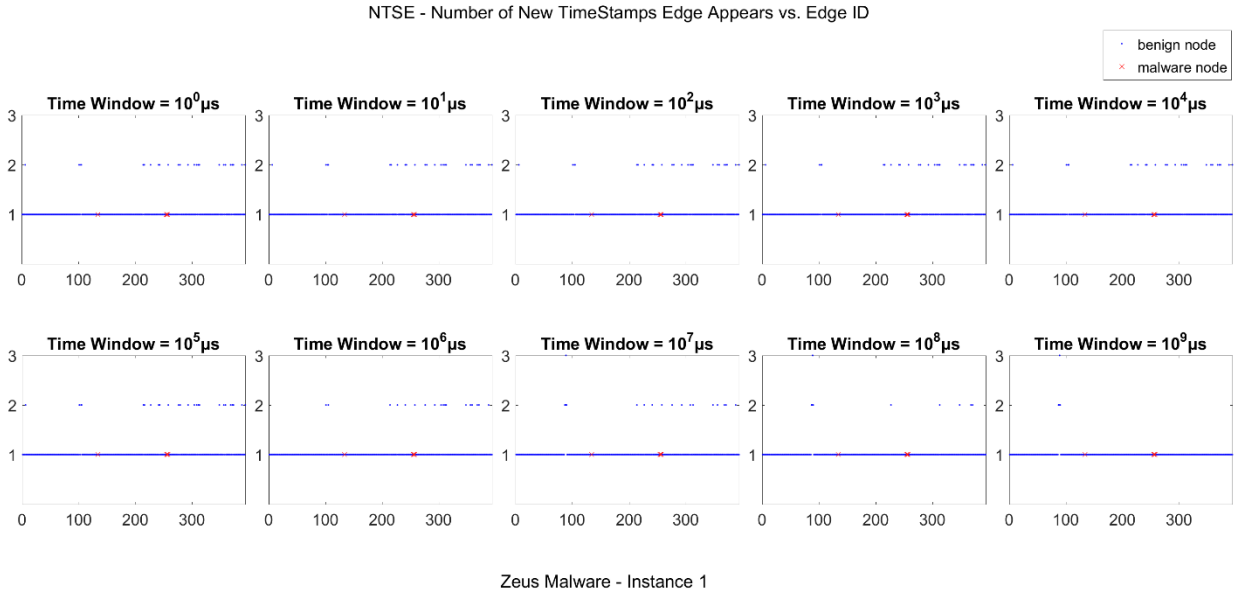


Zeus Malware - Instance 1

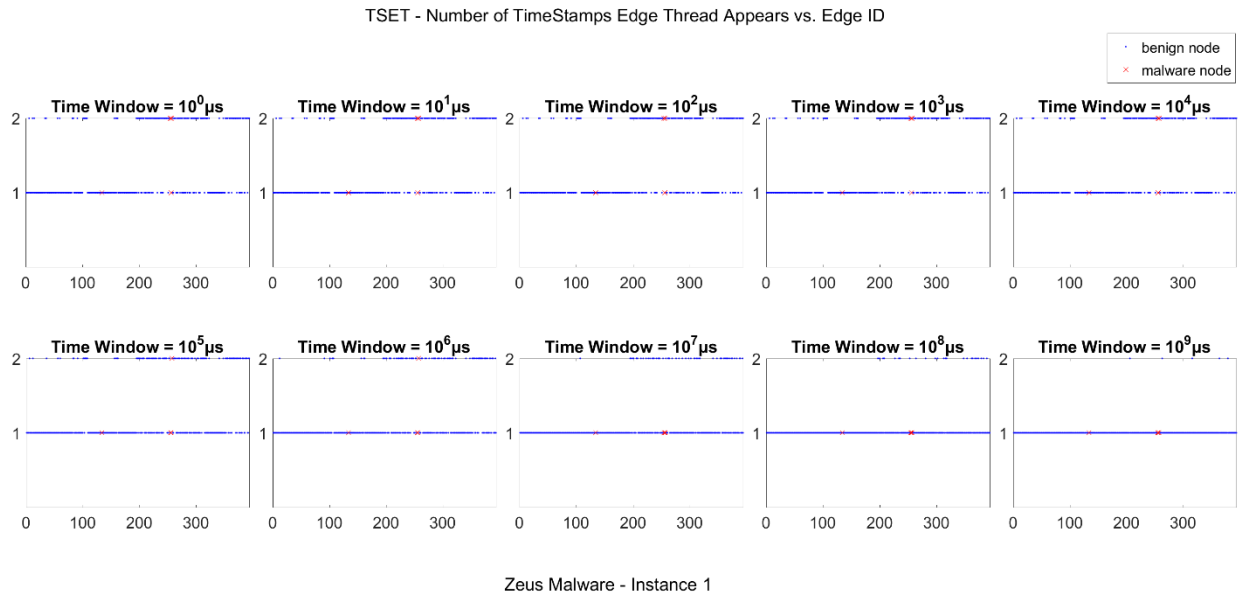
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Zeus Malware - Instance 1

8) NTSE

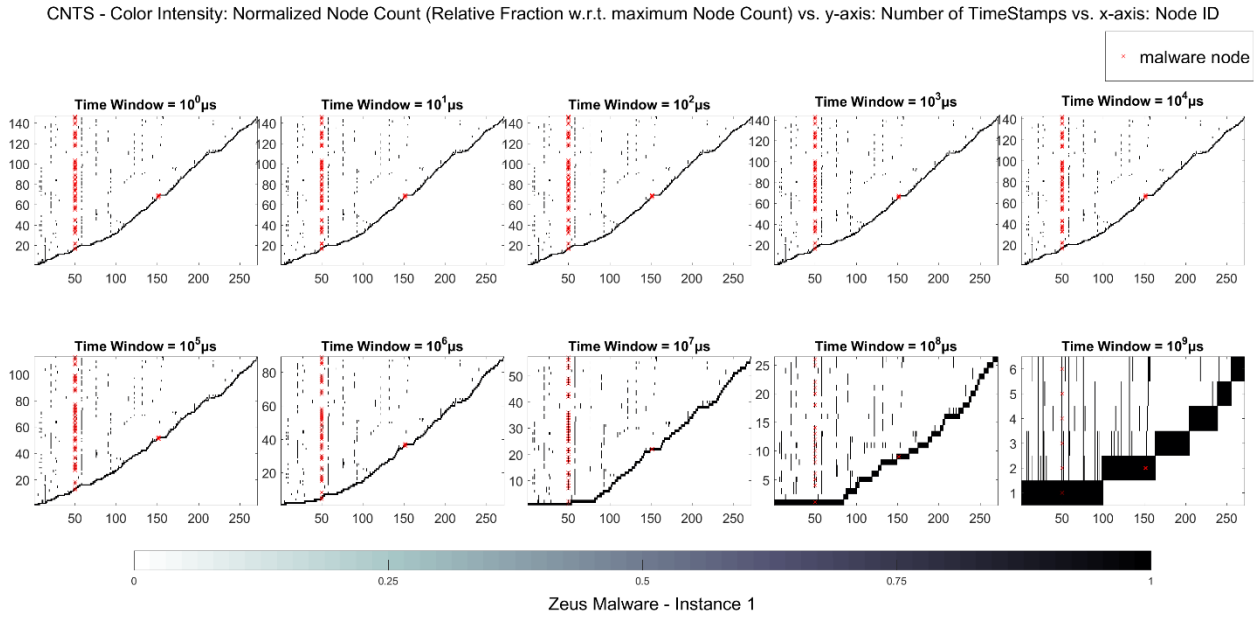

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Zeus Malware - Instance 1

9) TSET

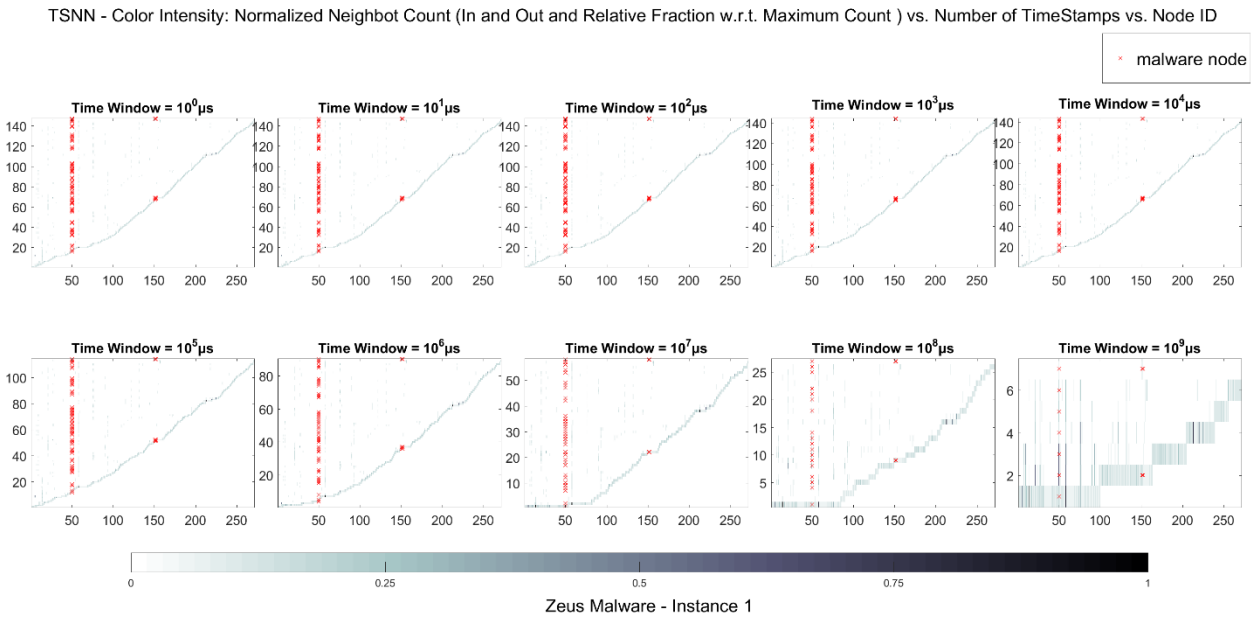


Time Graph Node Based Features

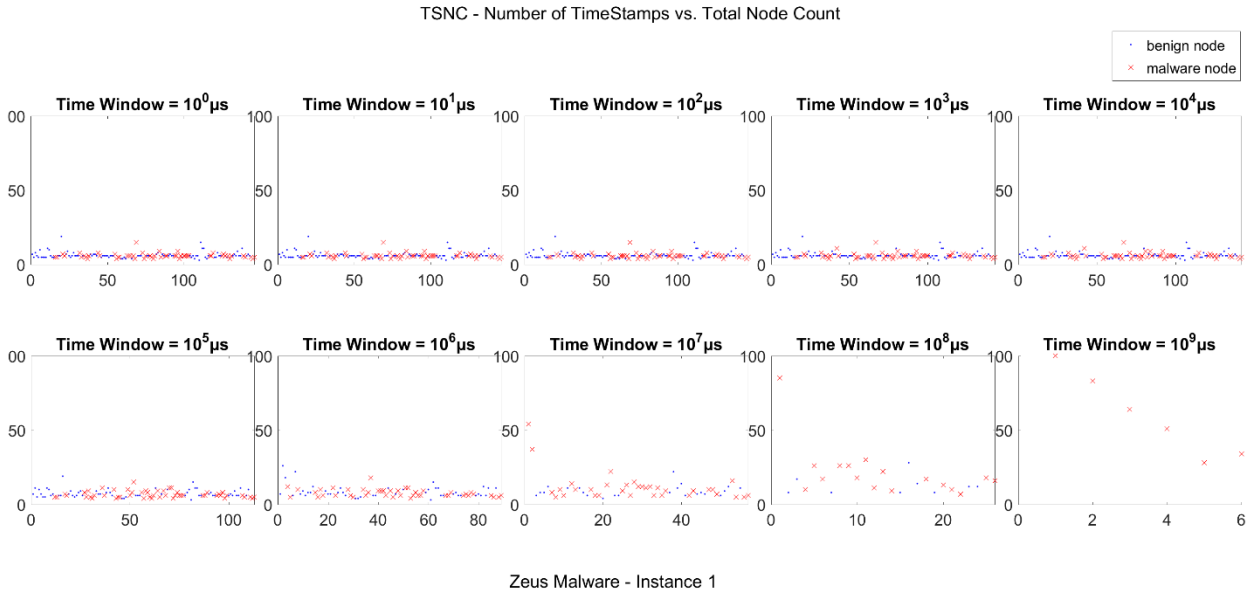
10) CNTS



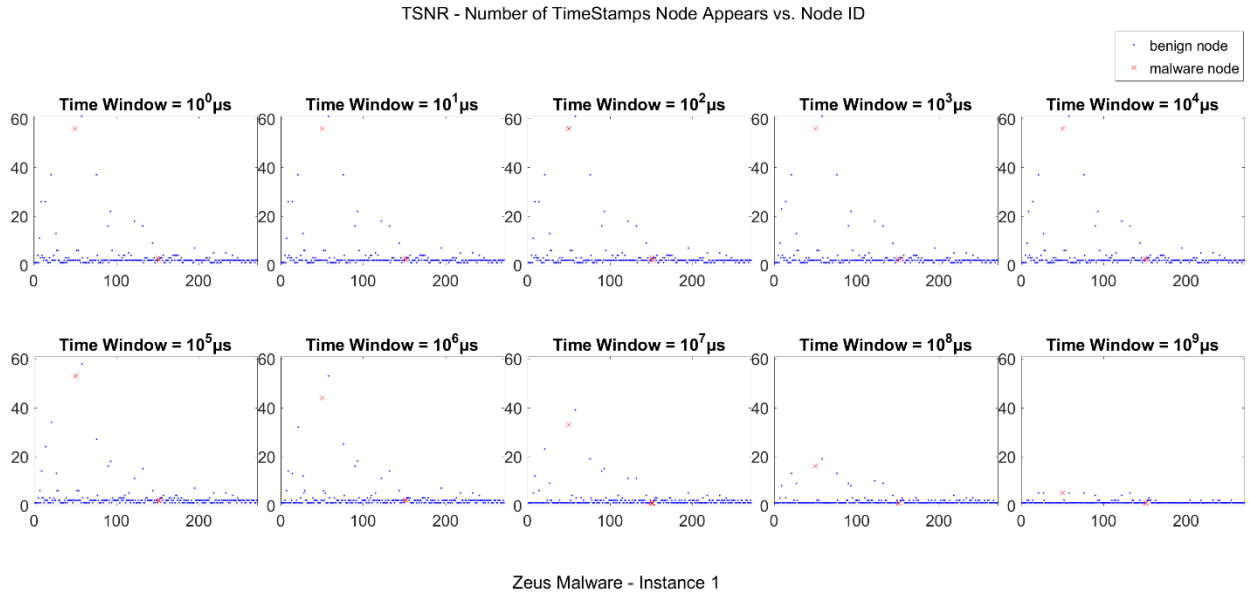
11) TSNN



12) TSNC



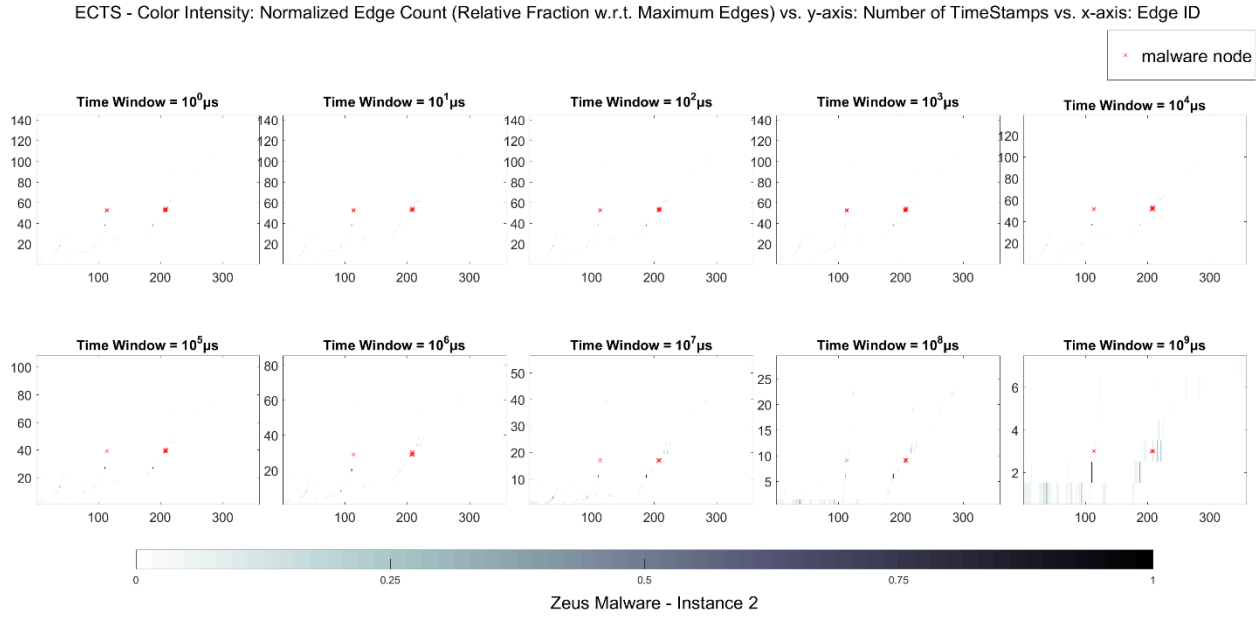
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Zeus Malware - Instance 1

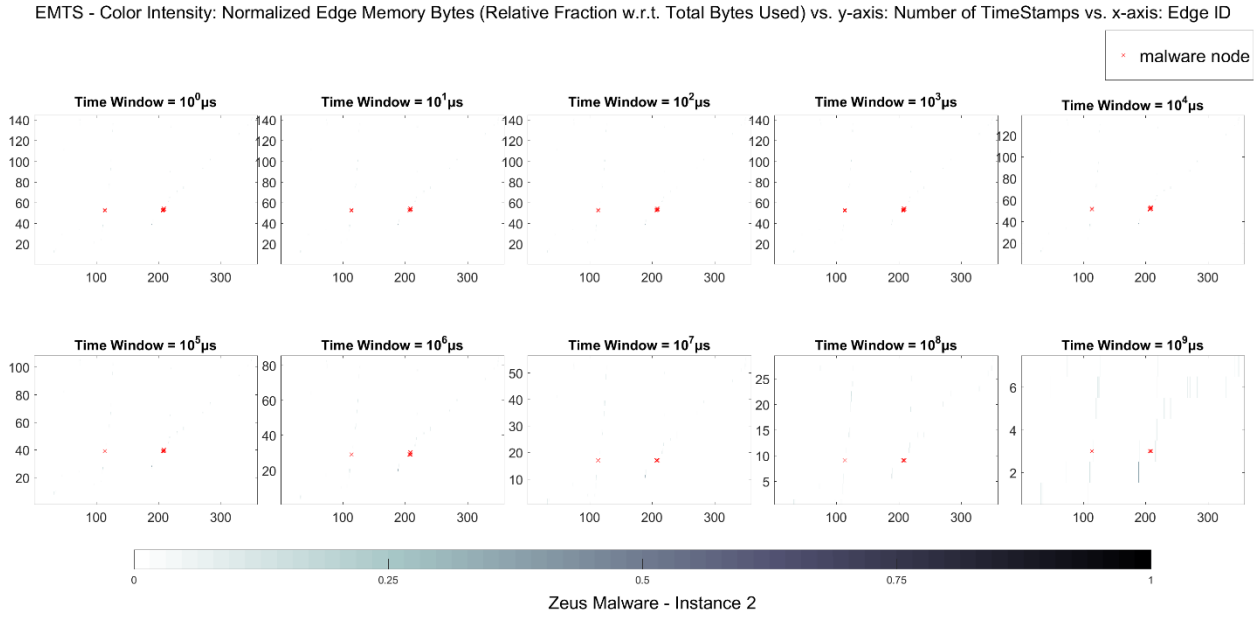
7.1.2 Zeus Malware – Instance 2

Time Graph Edge Based Features

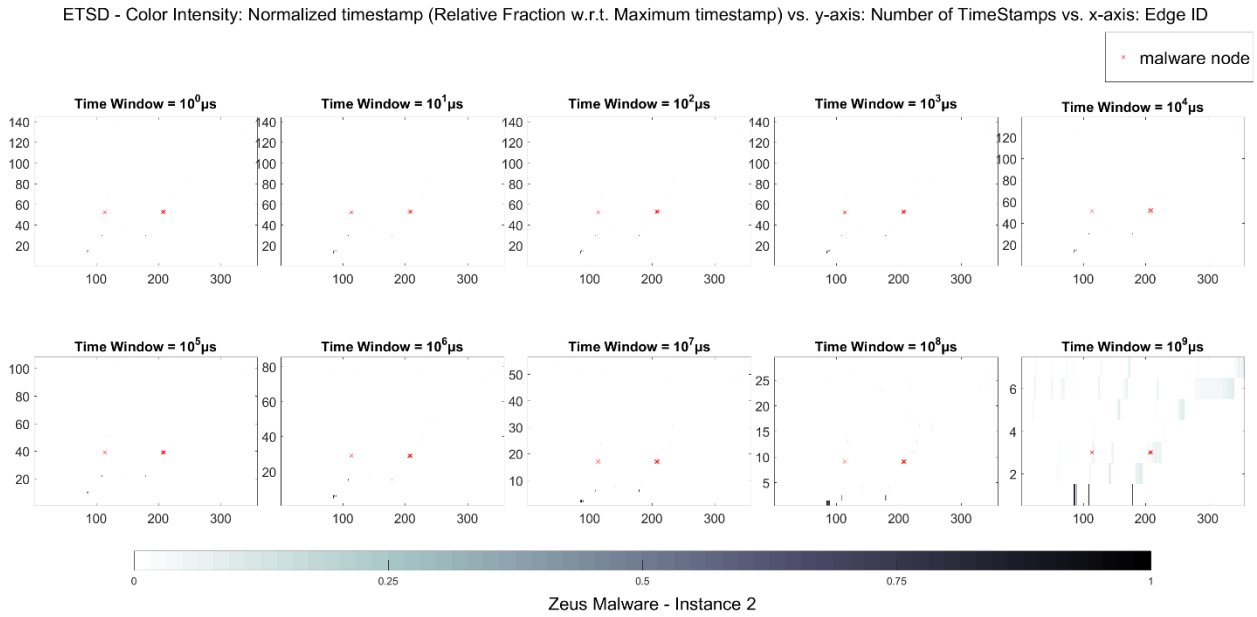
1) ECTS



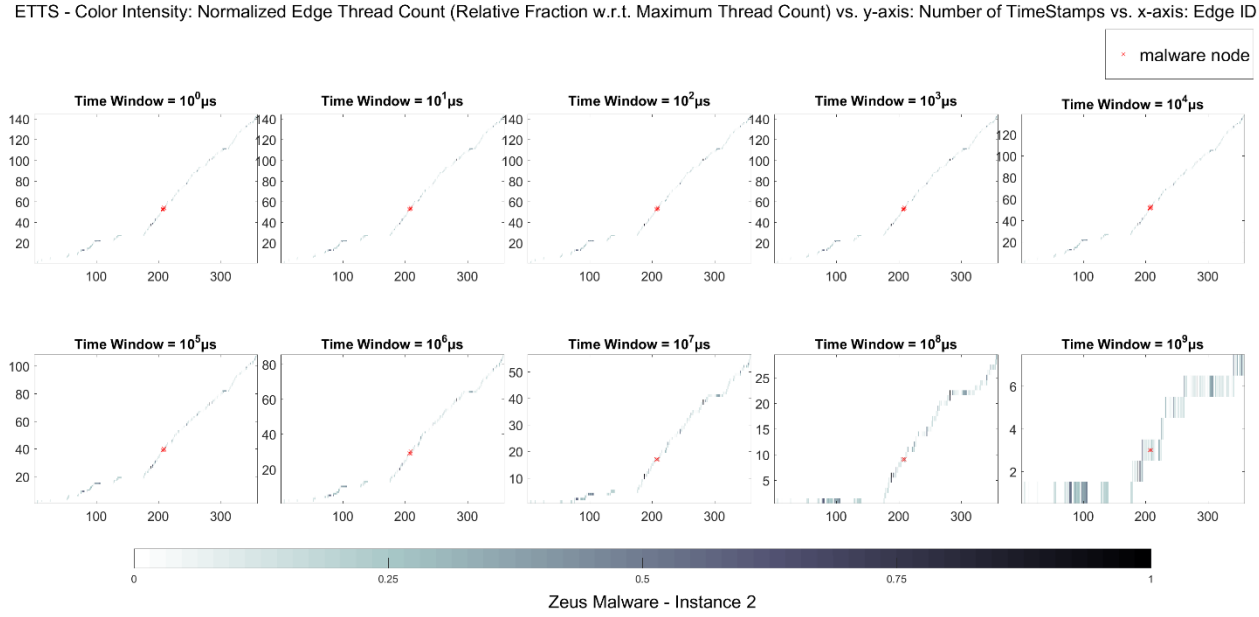
2) EMTS



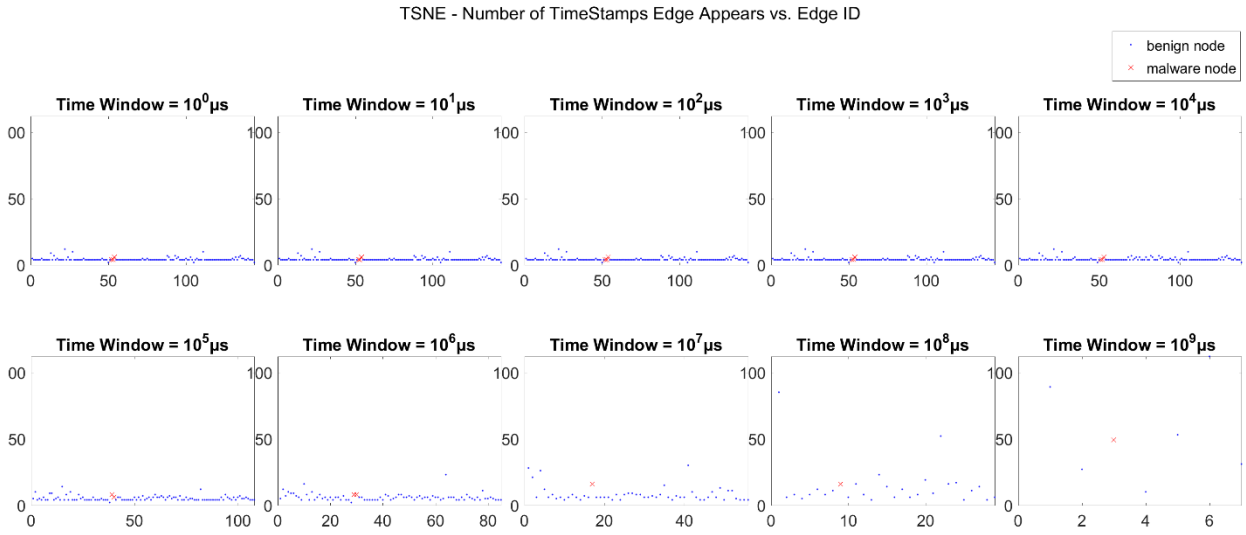
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Zeus Malware - Instance 2

4) ETTS

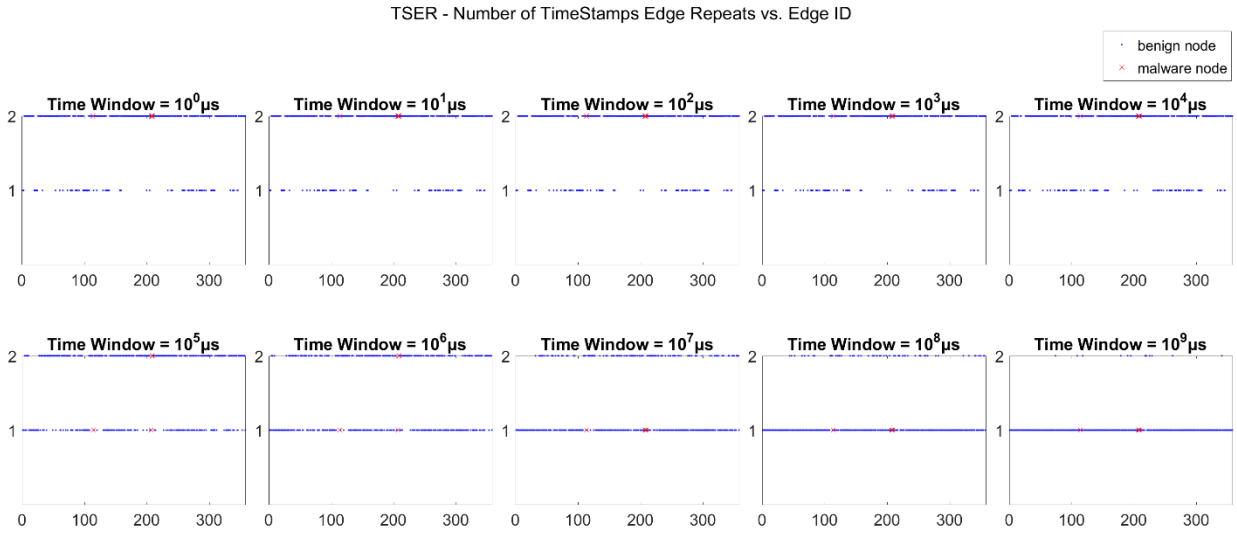

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Zeus Malware - Instance 2

5) TSNE



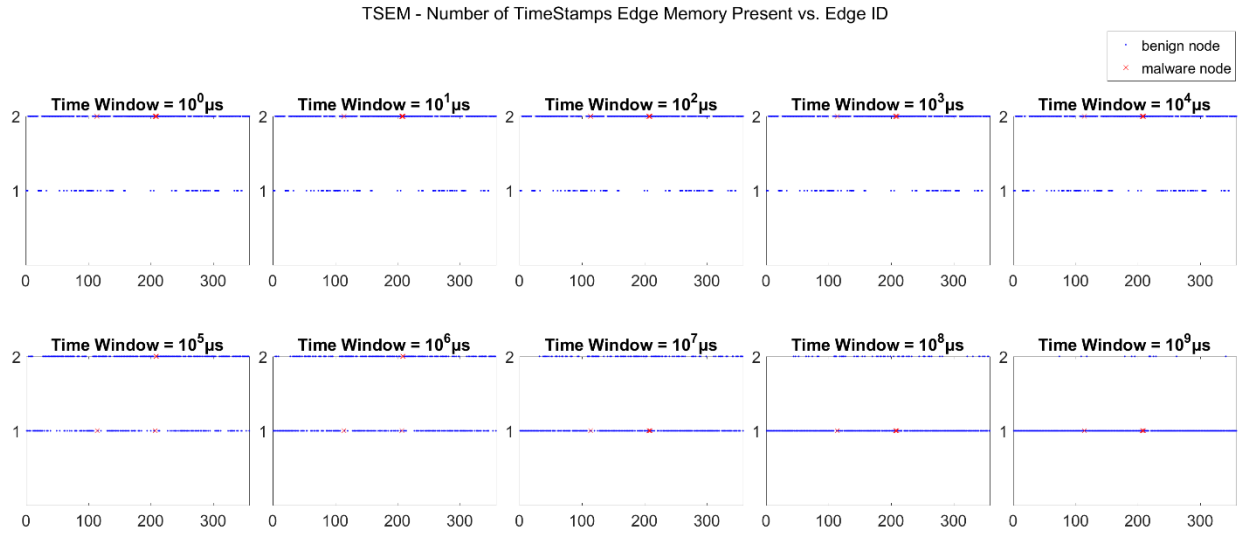
Zeus Malware - Instance 2

6) TSER



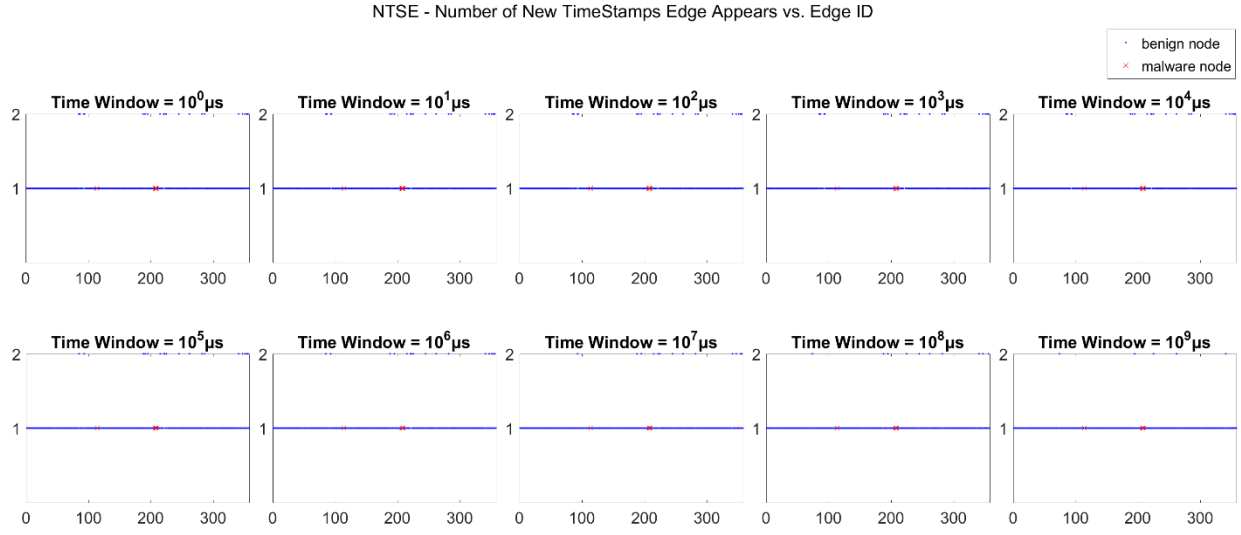
Zeus Malware - Instance 2

7) TSEM



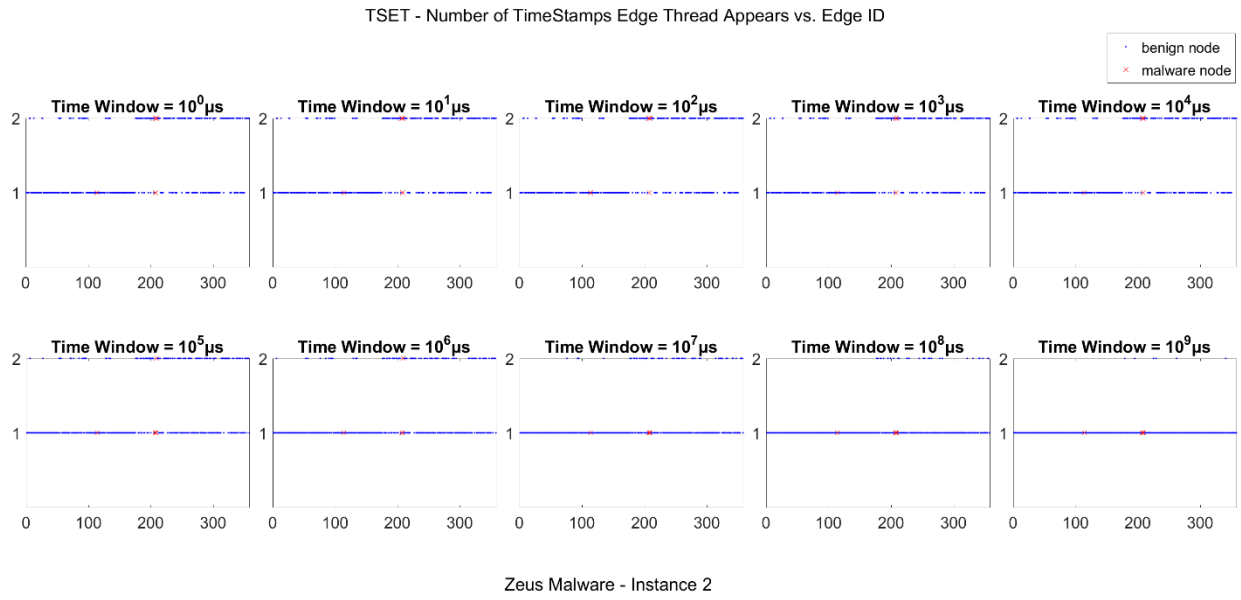
Zeus Malware - Instance 2

8) NTSE



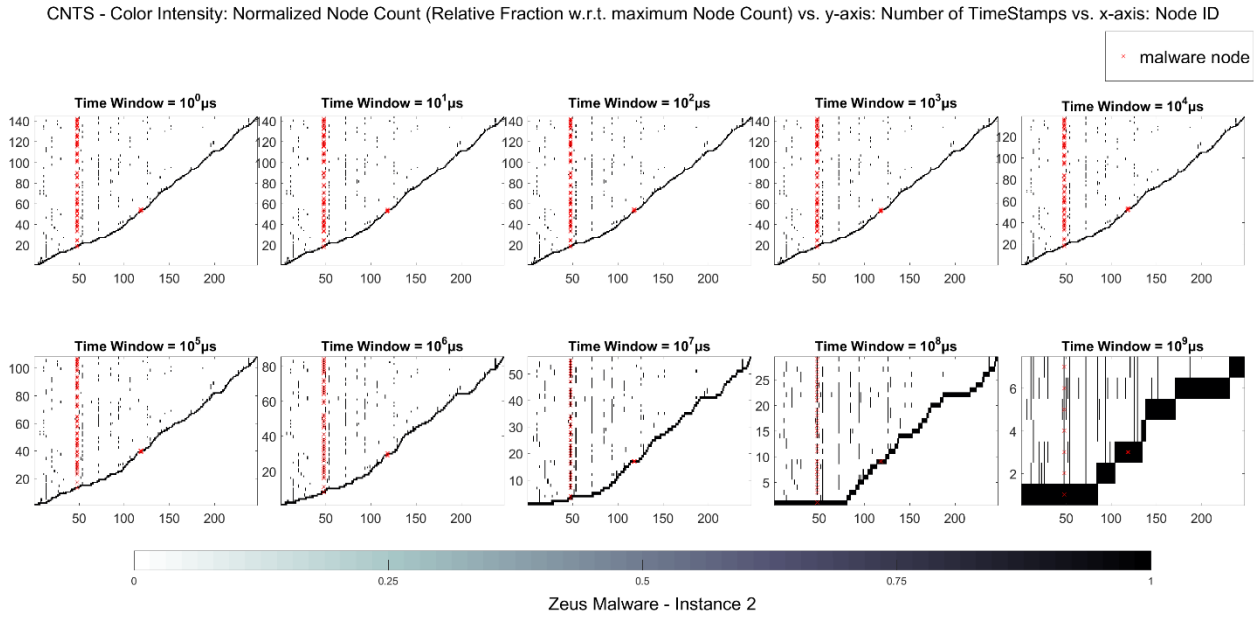
Zeus Malware - Instance 2

9) TSET

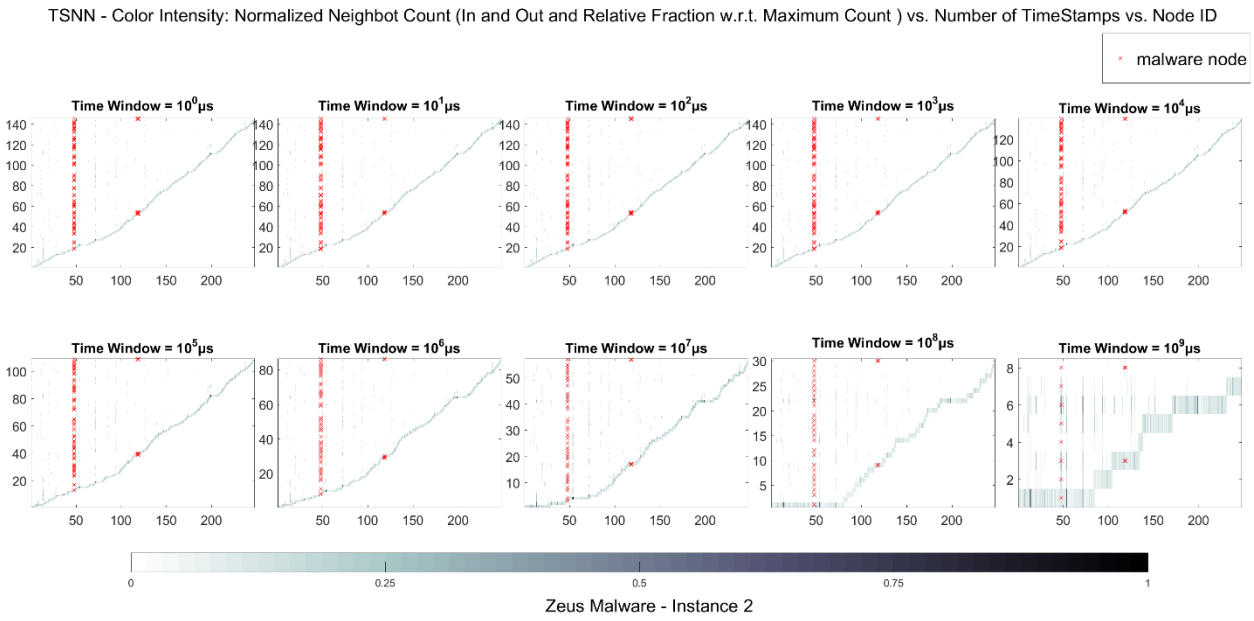


Time Graph Node Based Features

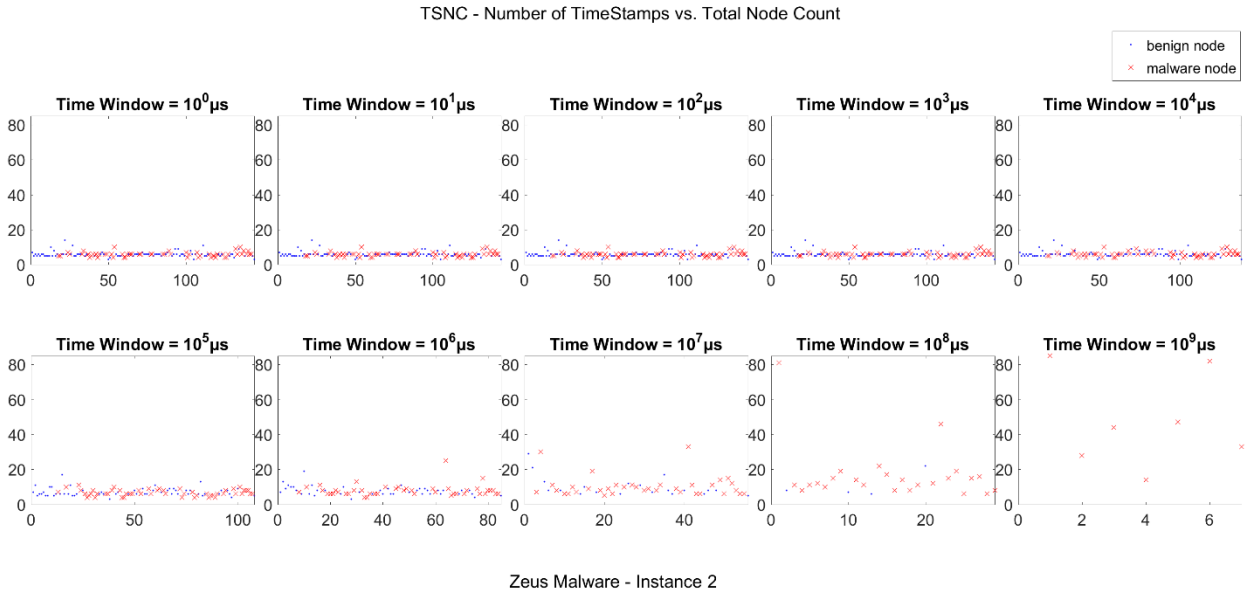
10) CNTS



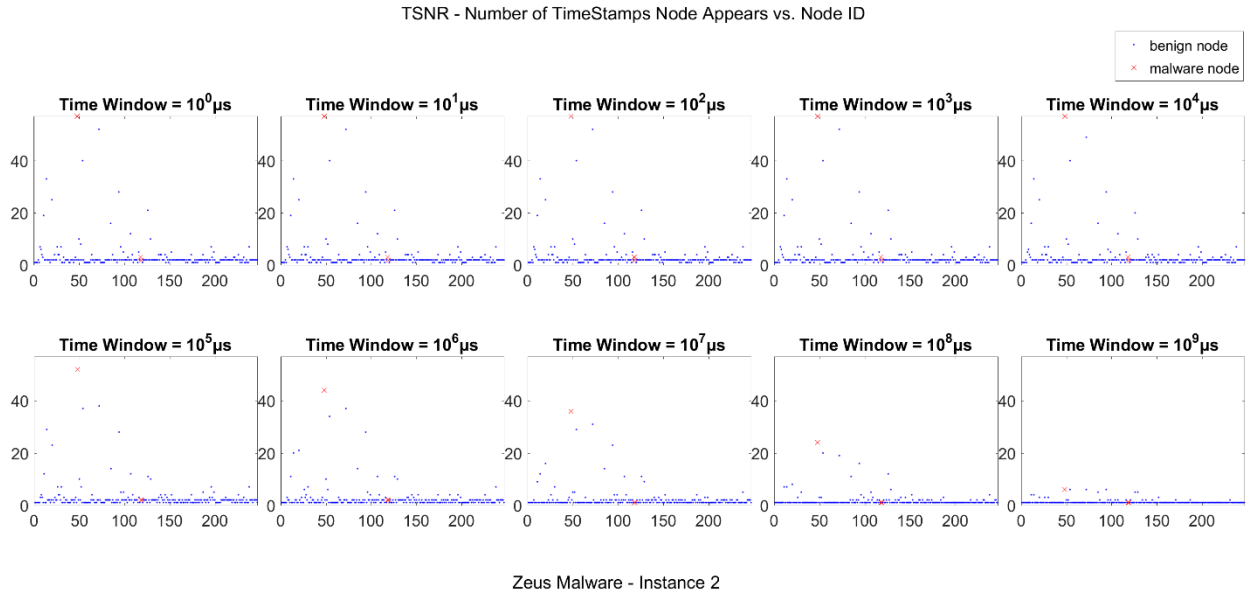
11) TSNN



12) TSNC



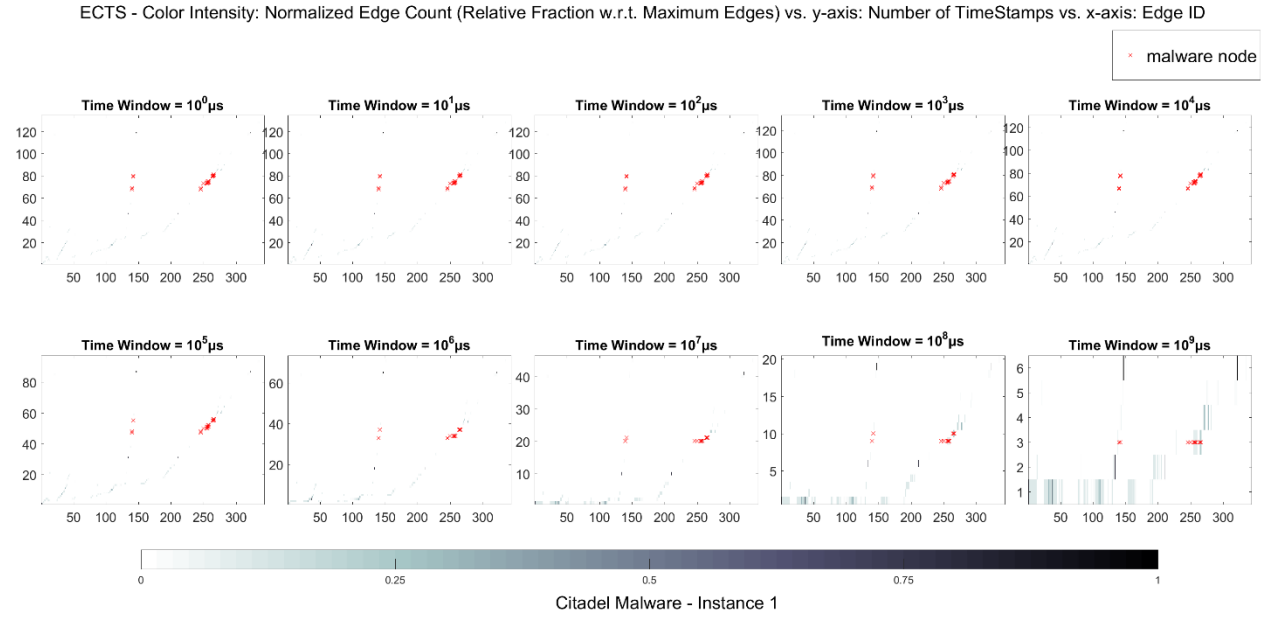
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
20
40
0
50
100
150
200
Zeus Malware - Instance 2

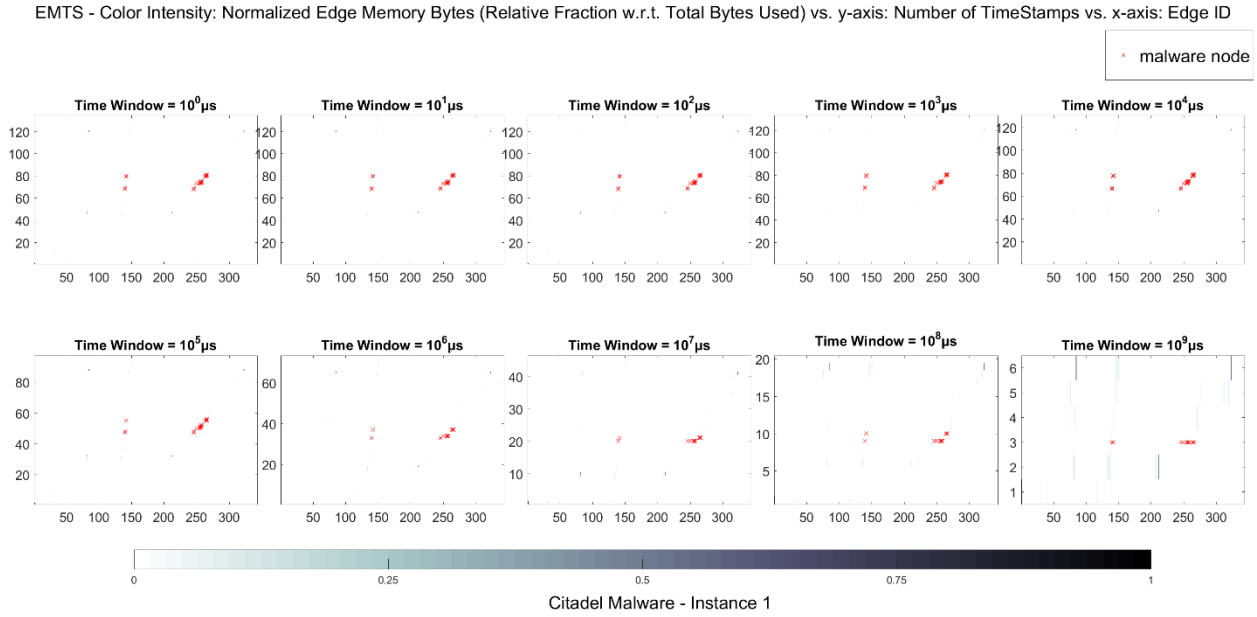
7.1.3 Citadel Malware – Instance 1

Time Graph Edge Based Features

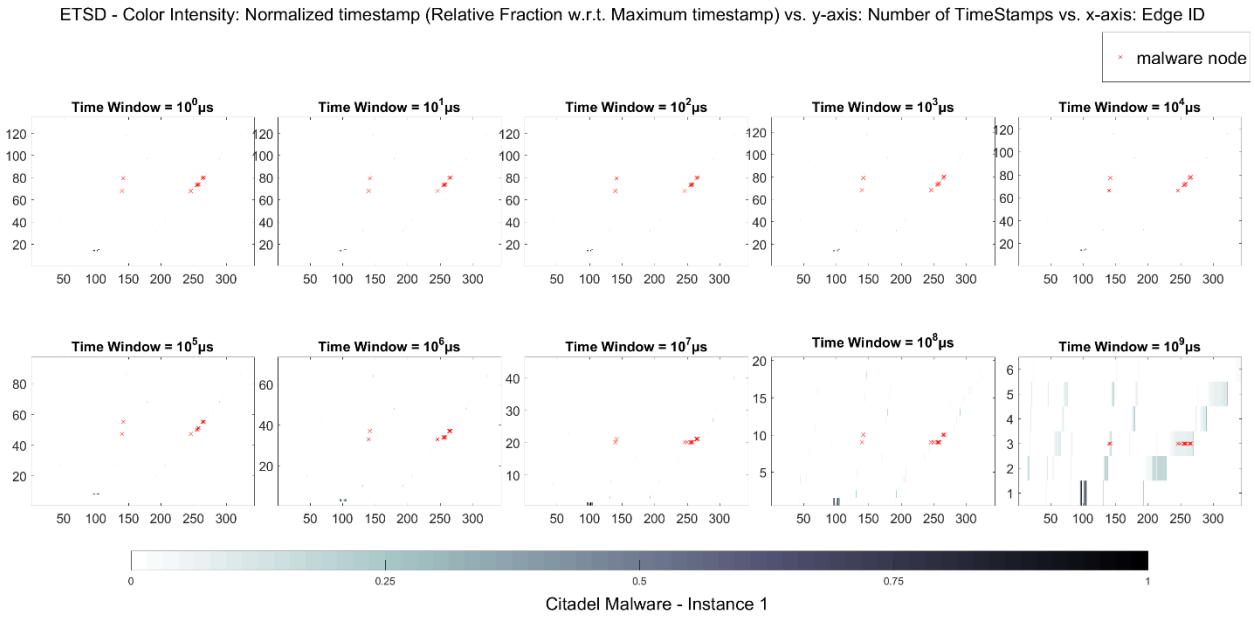
1) ECTS



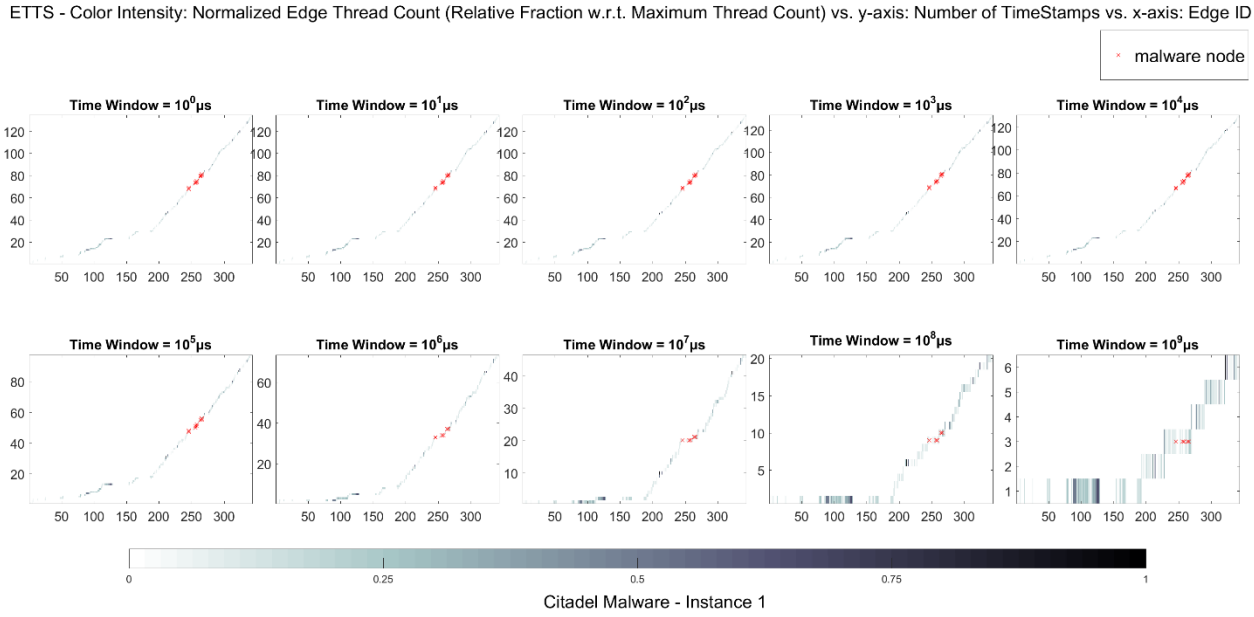
2) EMTS



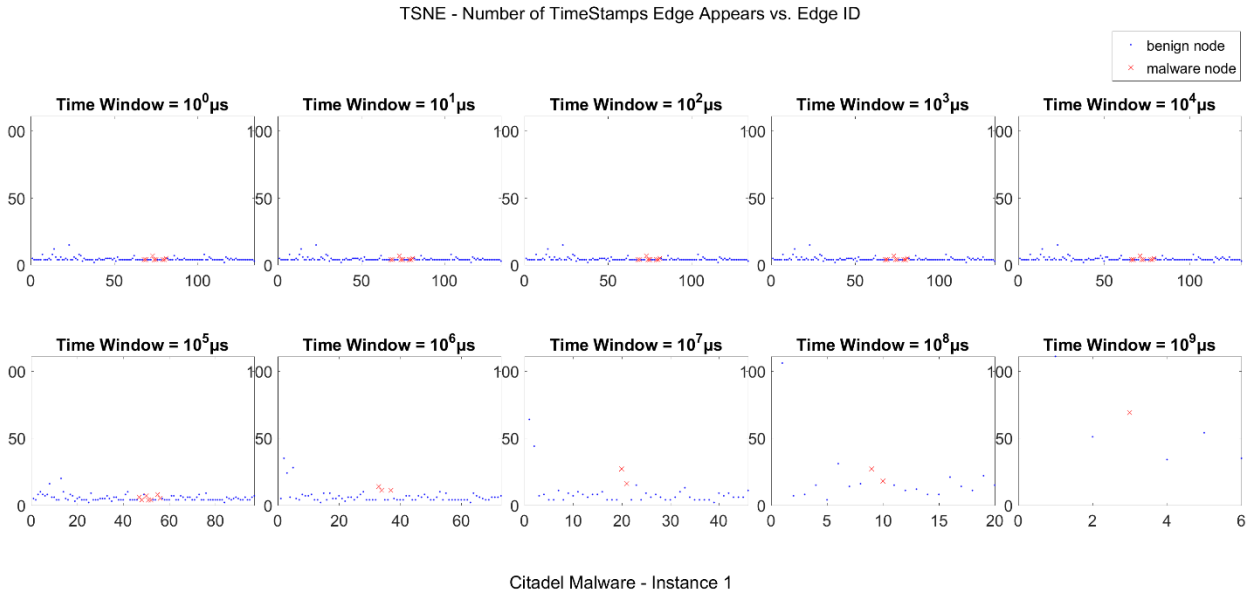
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Citadel Malware - Instance 1

4) ETTS

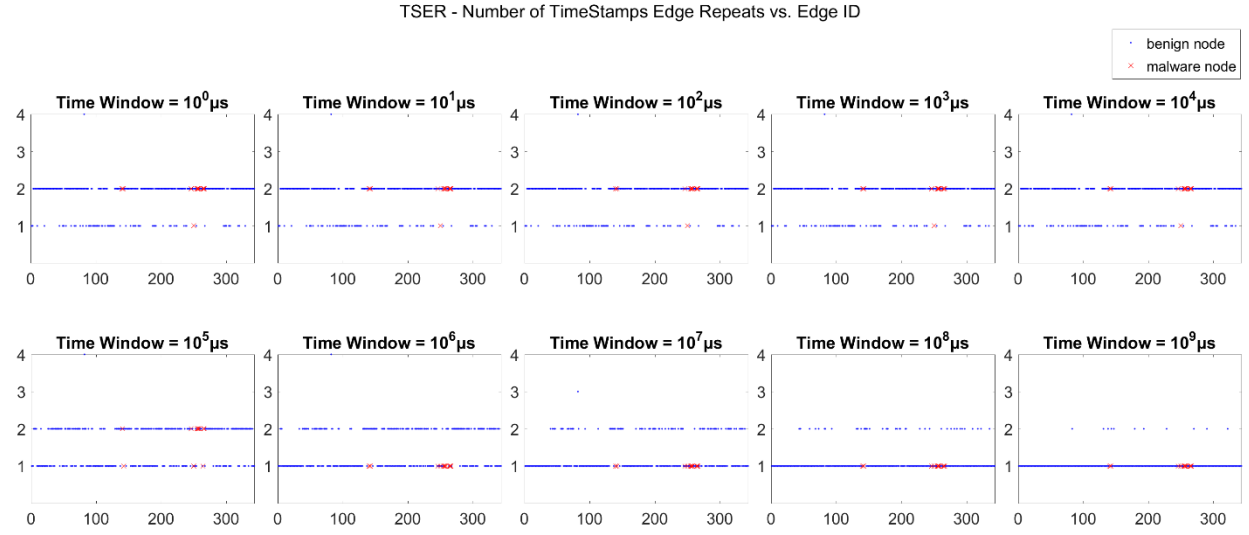

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Citadel Malware - Instance 1

5) TSNE



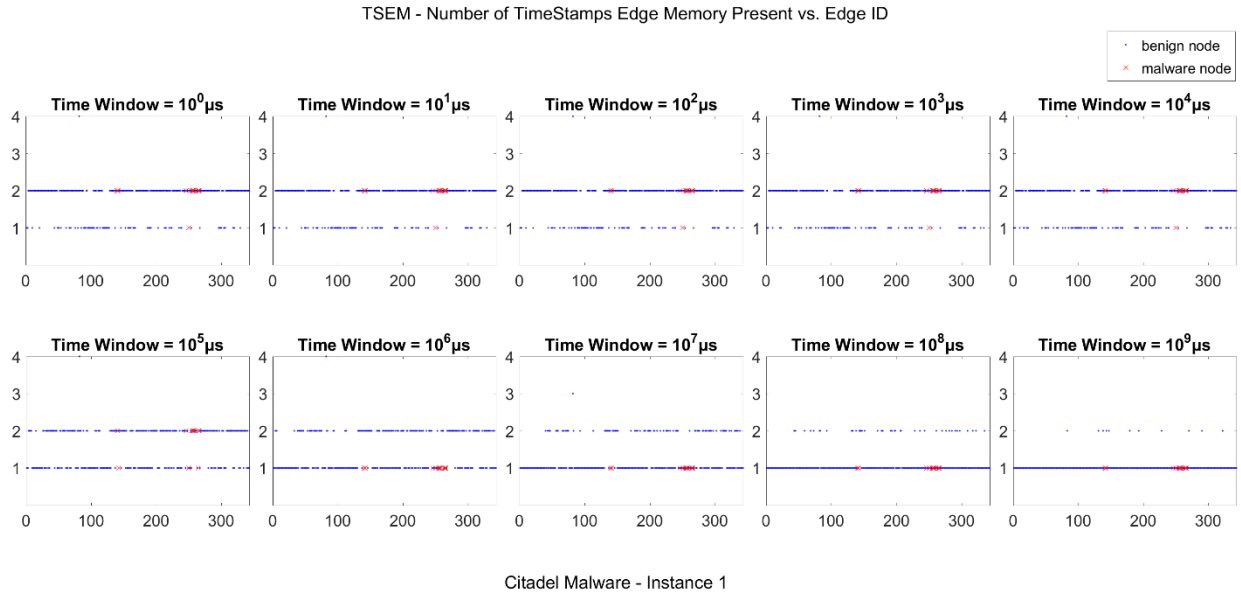
Citadel Malware - Instance 1

6) TSER

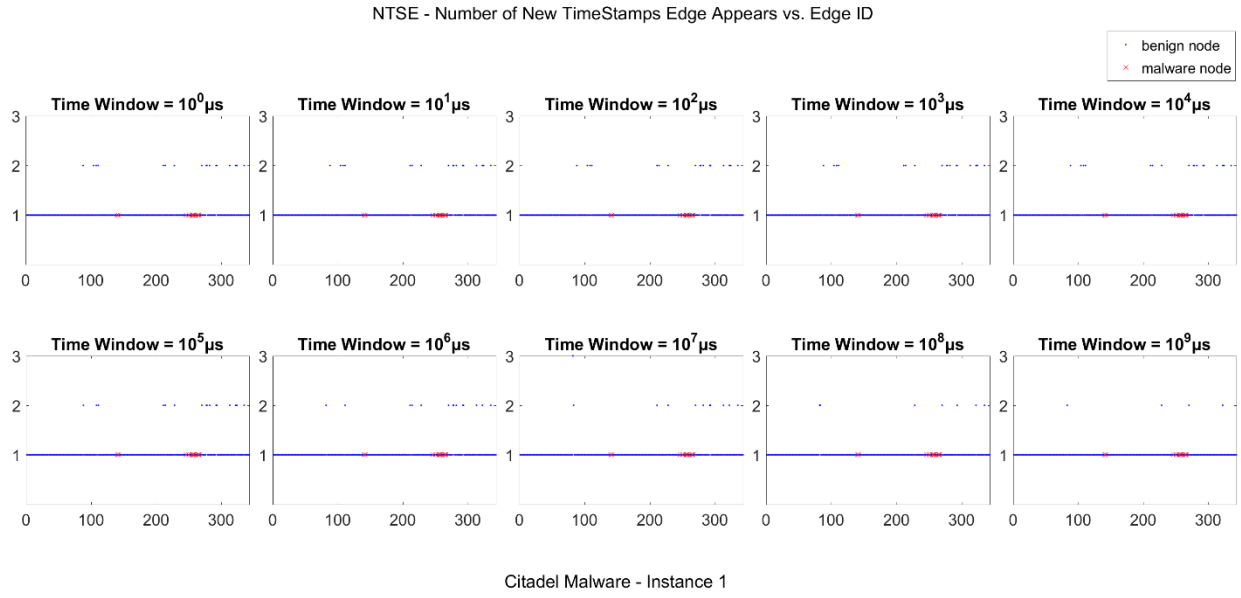


Citadel Malware - Instance 1

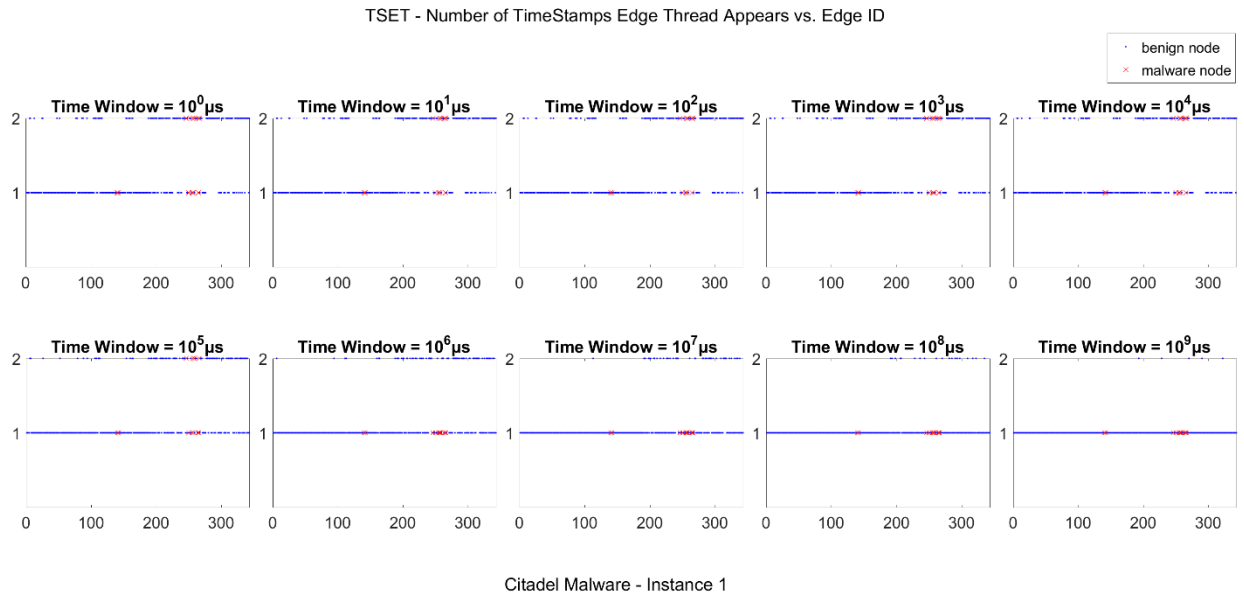
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Citadel Malware - Instance 1

8) NTSE

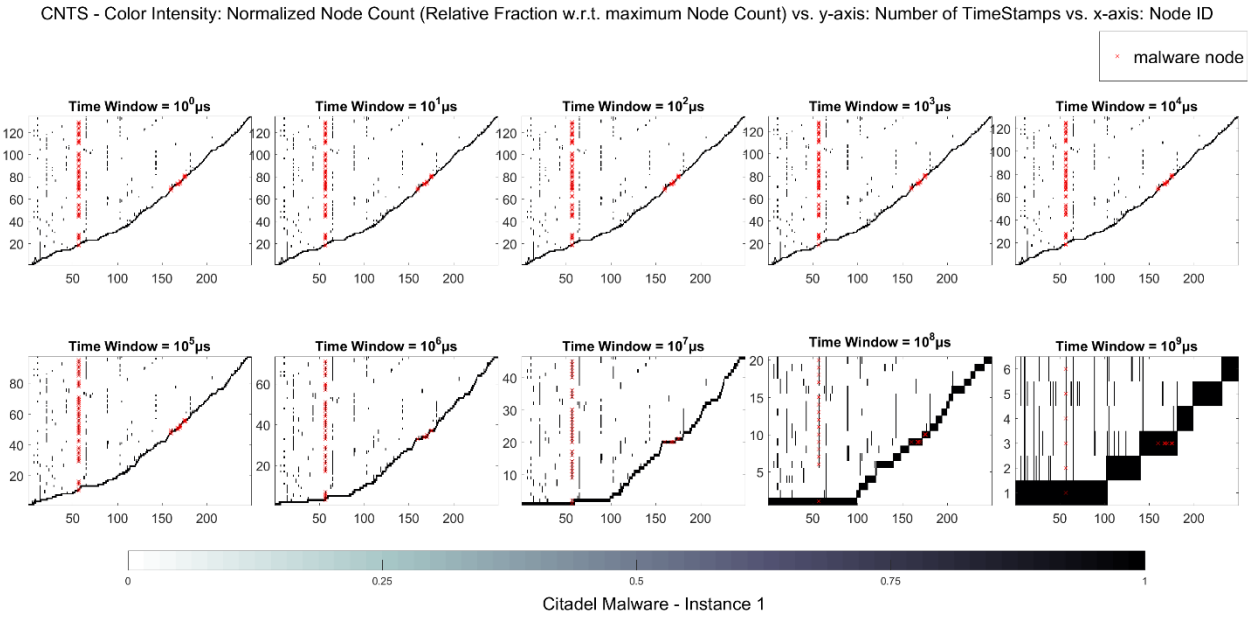

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Citadel Malware - Instance 1

9) TSET

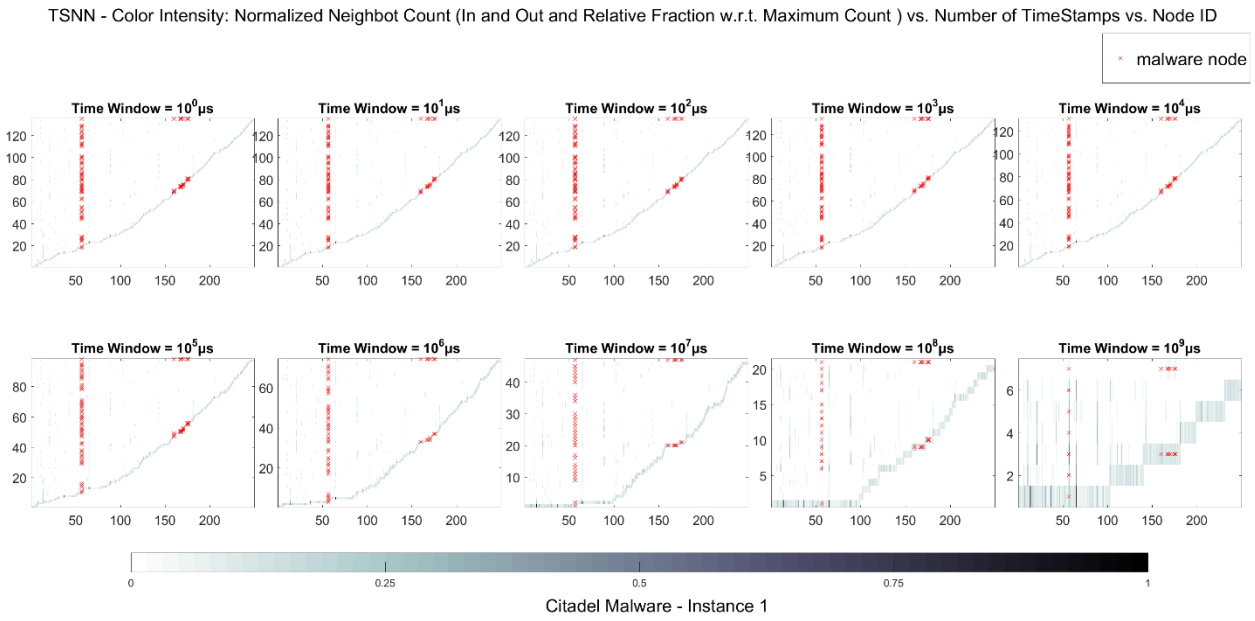


Time Graph Node Based Features

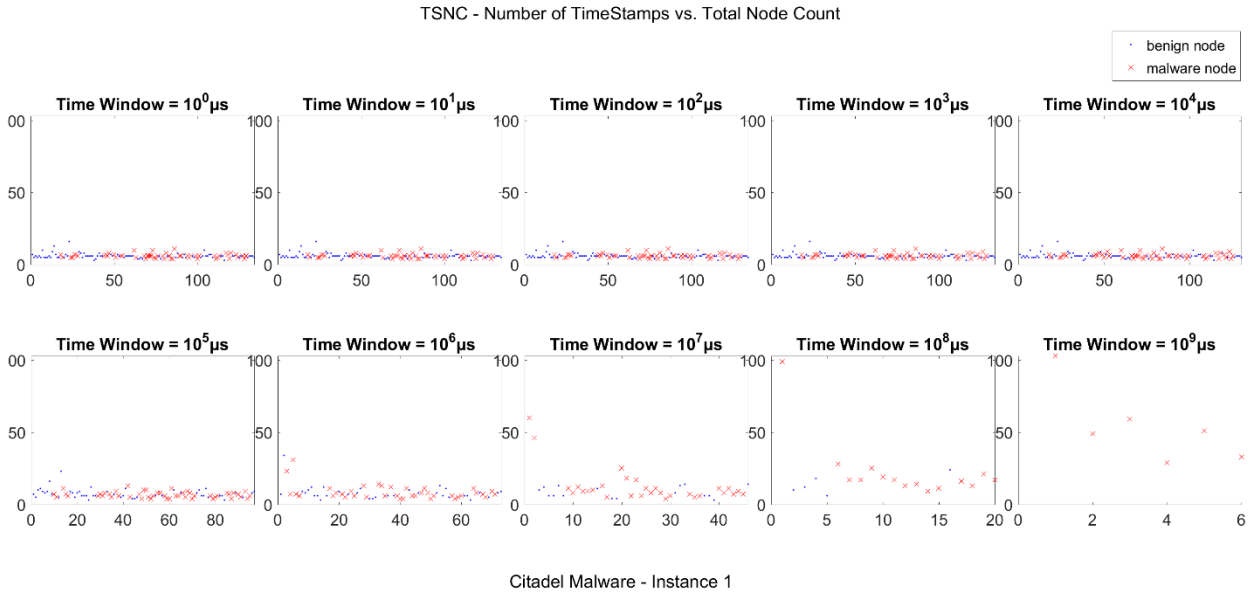
10) CNTS



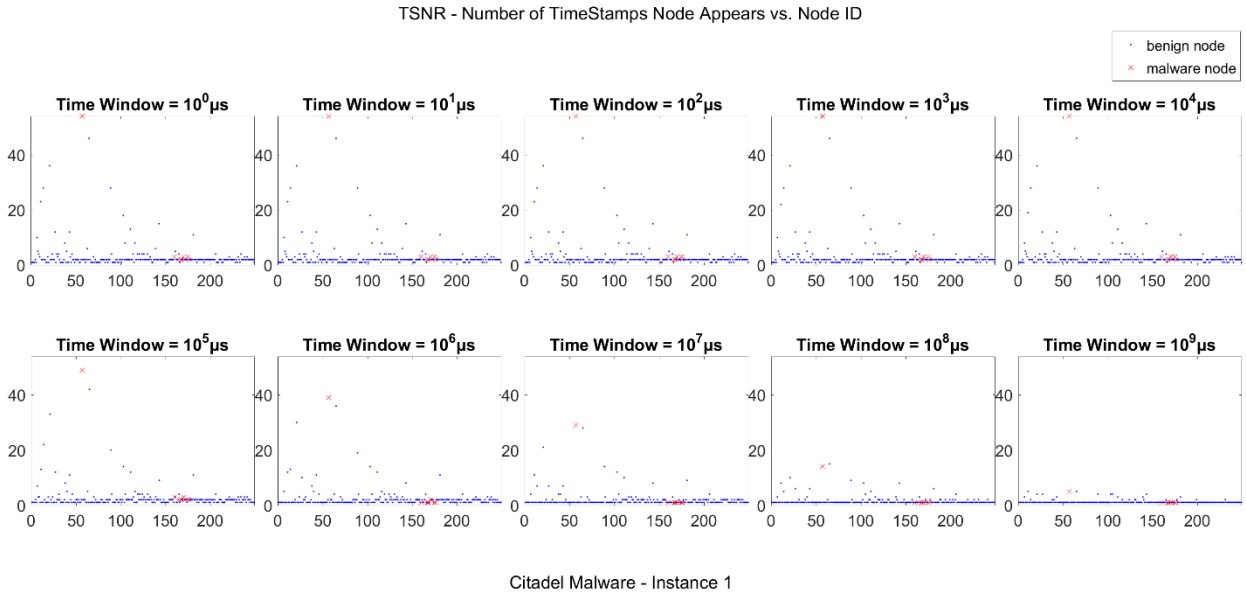
11) TSNN



12) TSNC



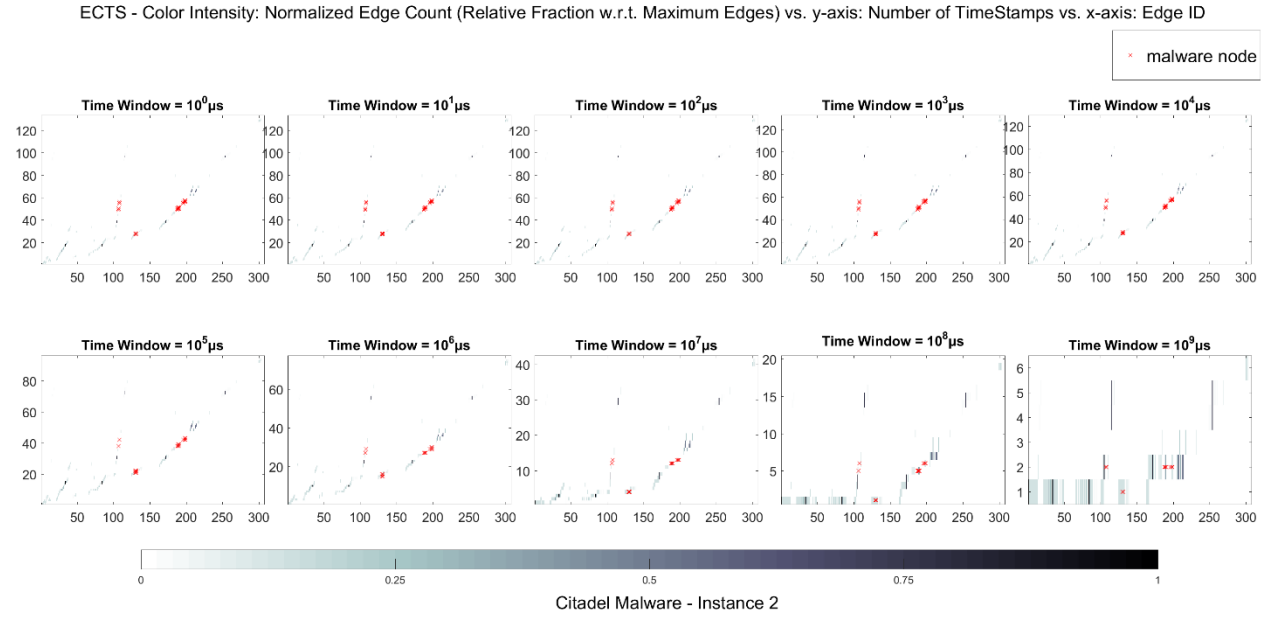
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Citadel Malware - Instance 1

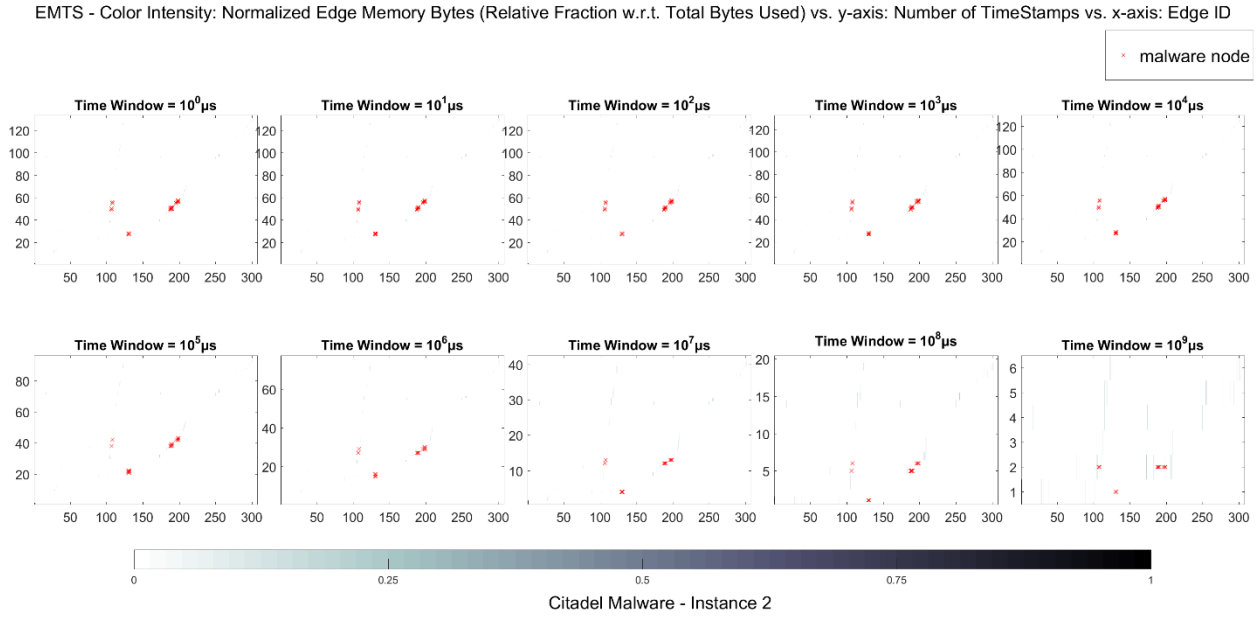
7.1.4 Citadel Malware – Instance 2

Time Graph Edge Based Features

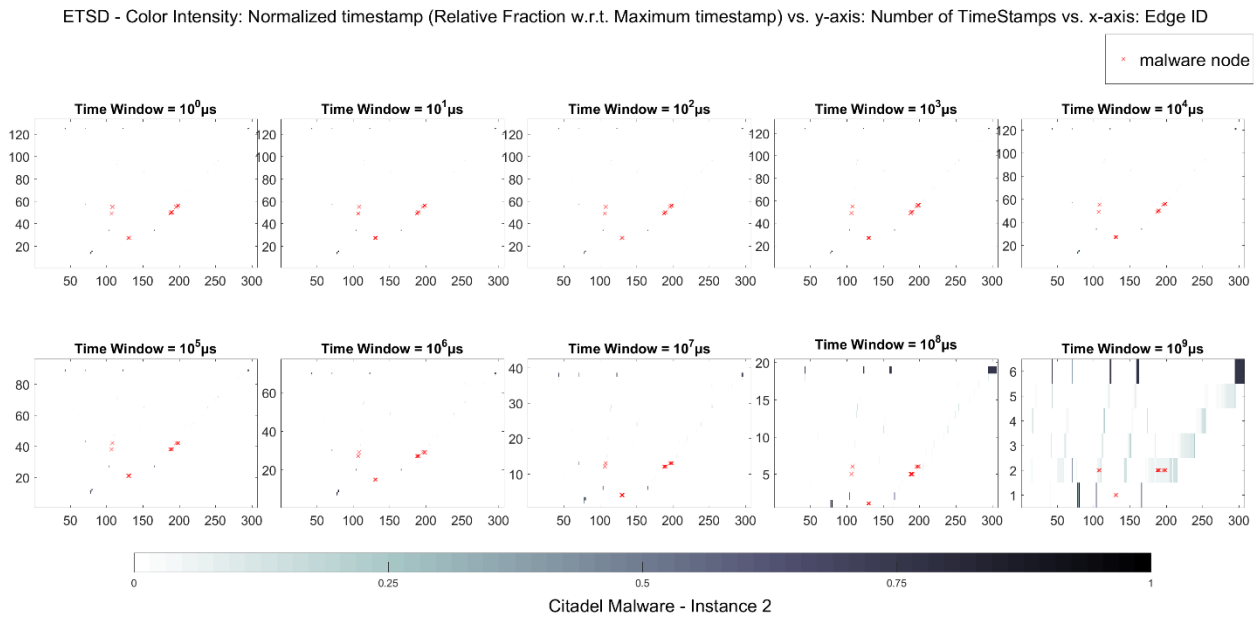
1) ECTS



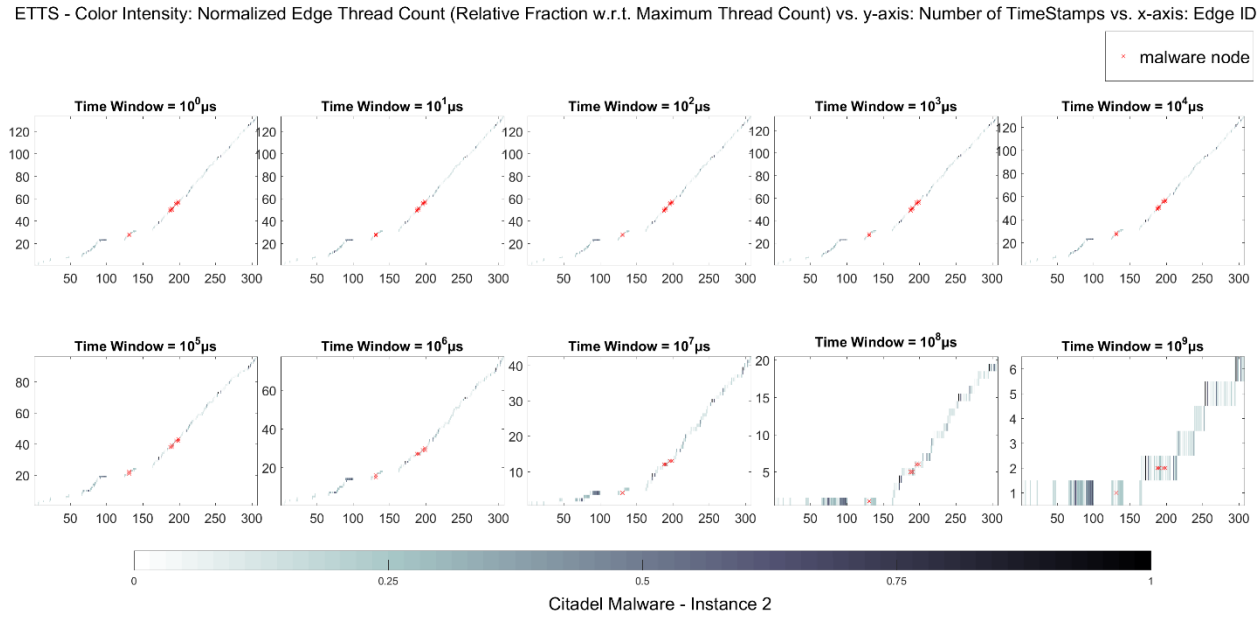
2) EMTS



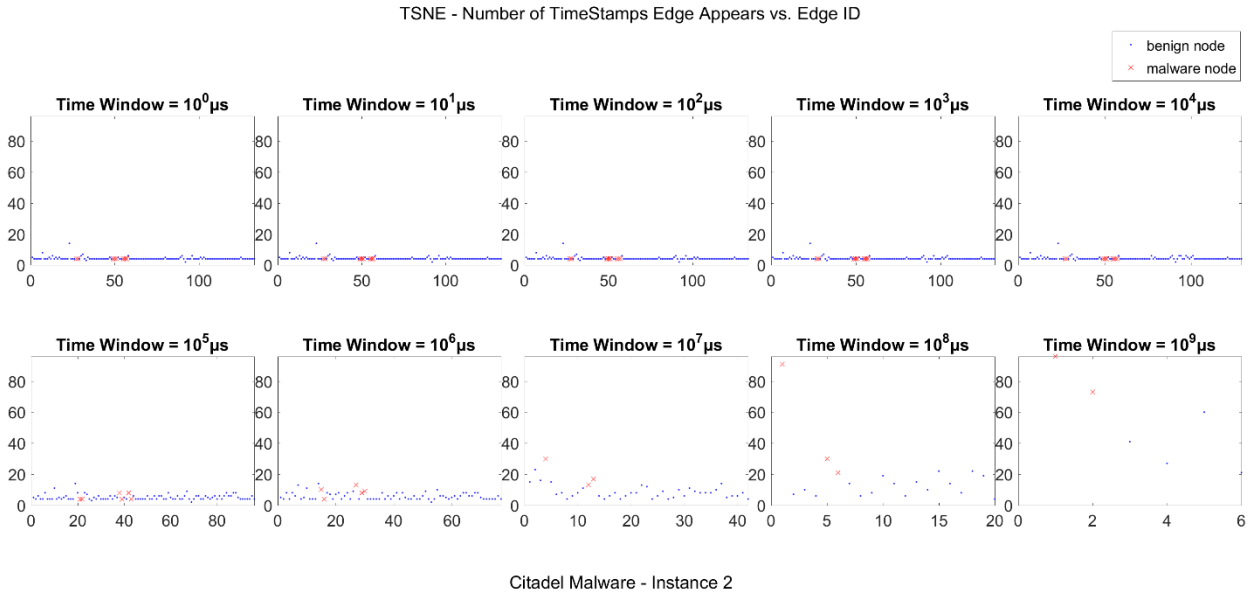
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Citadel Malware - Instance 2

4) ETTS

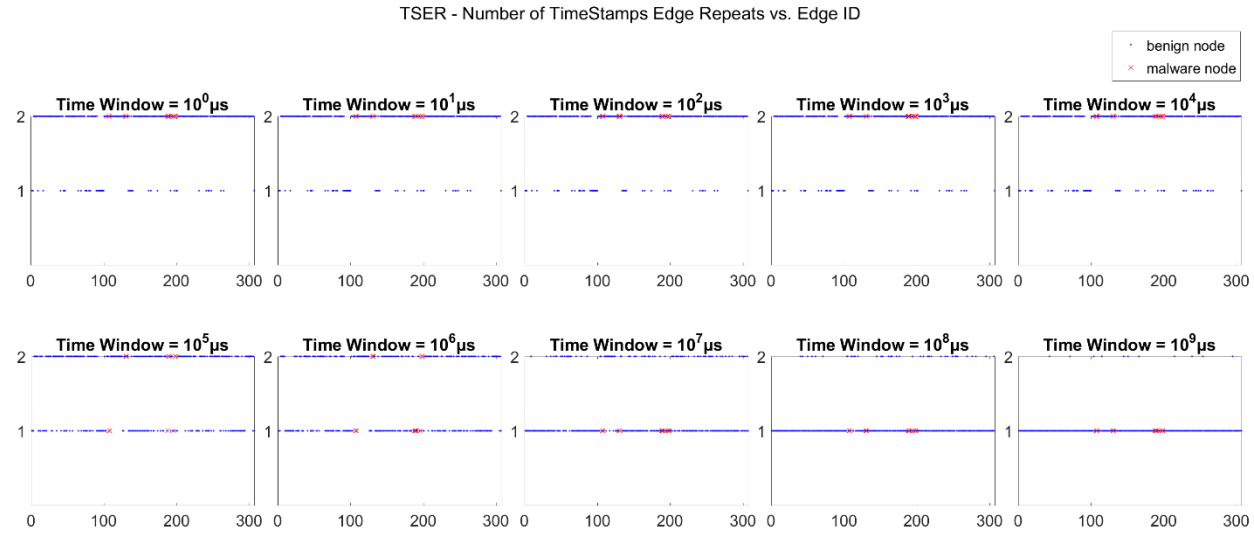

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Citadel Malware - Instance 2

5) TSNE



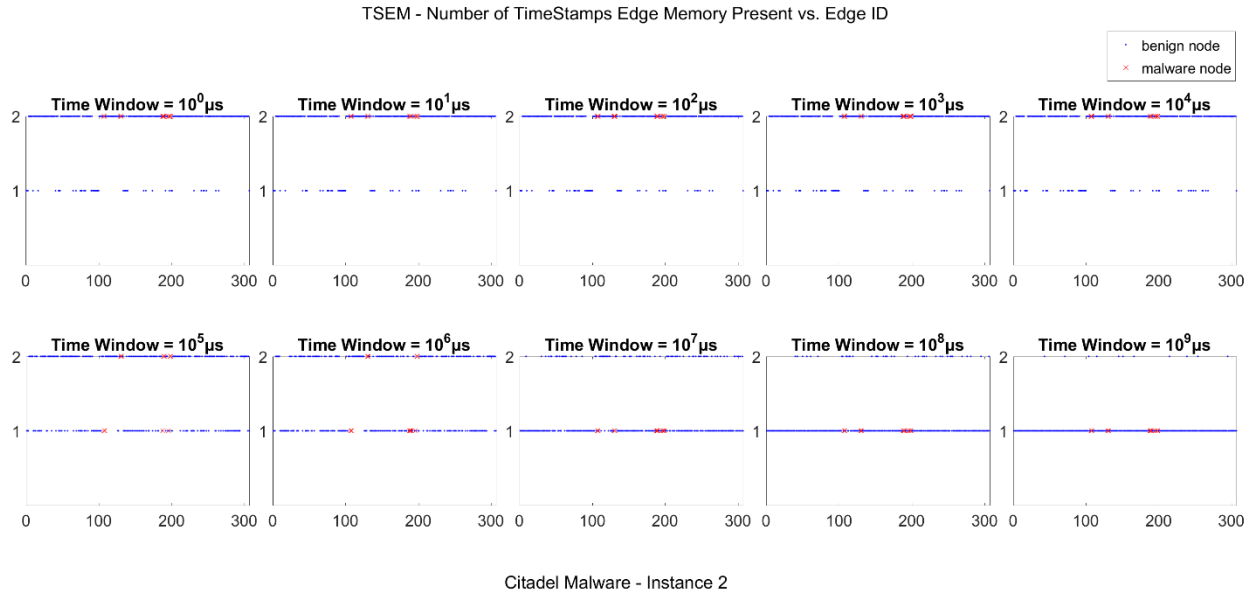
Citadel Malware - Instance 2

6) TSER

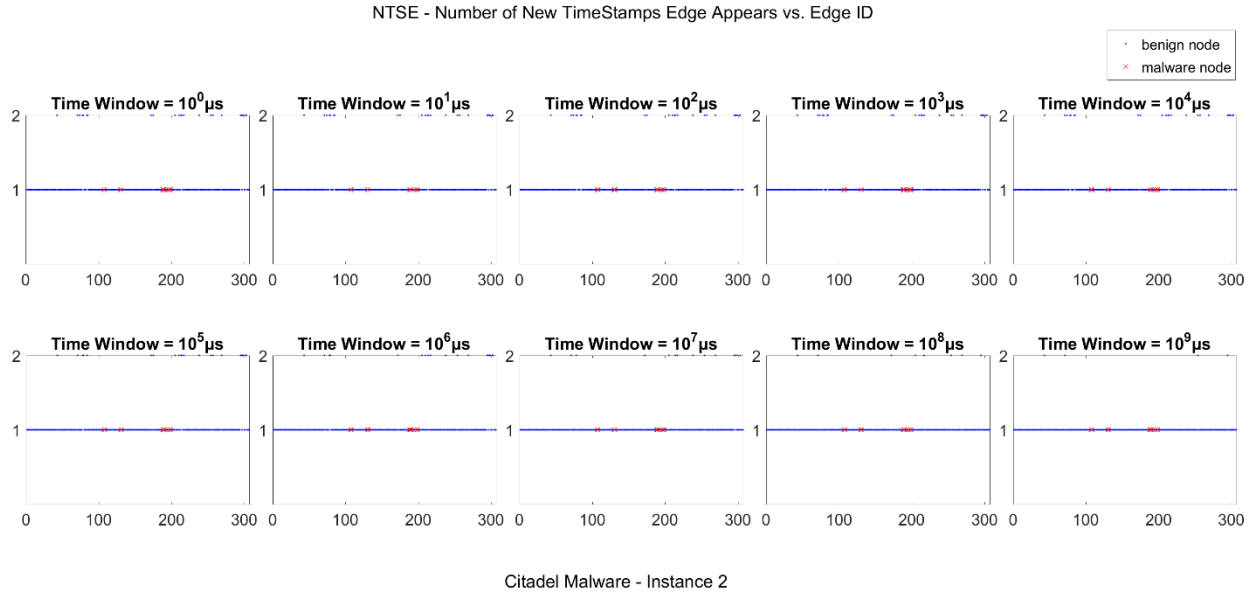


Citadel Malware - Instance 2

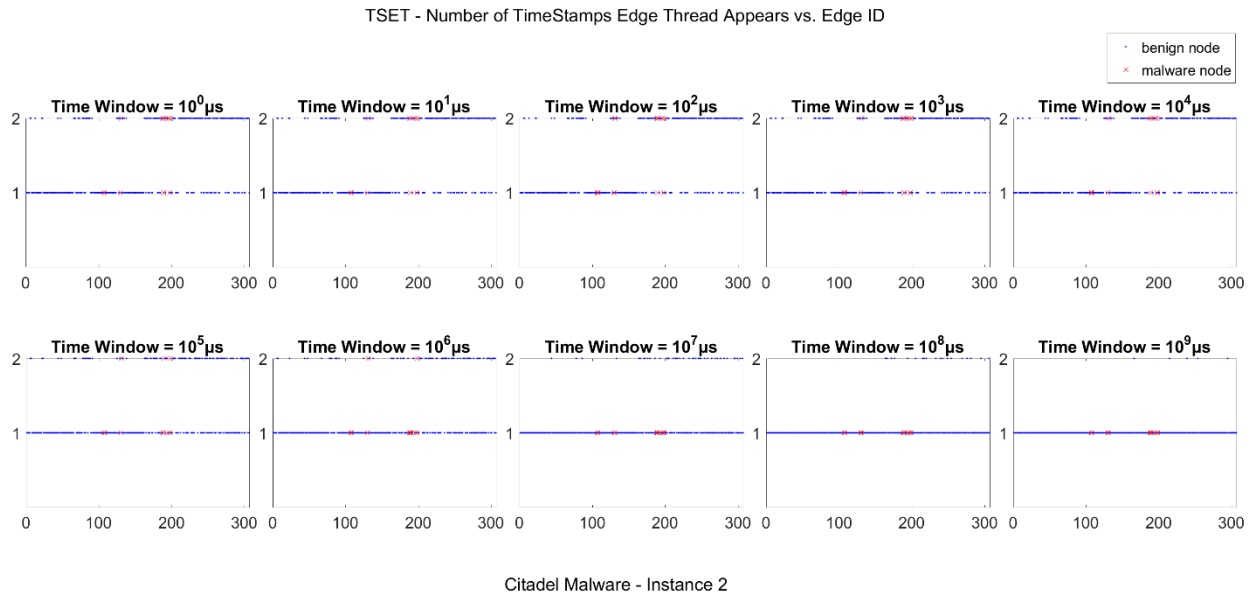
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Citadel Malware - Instance 2

8) NTSE

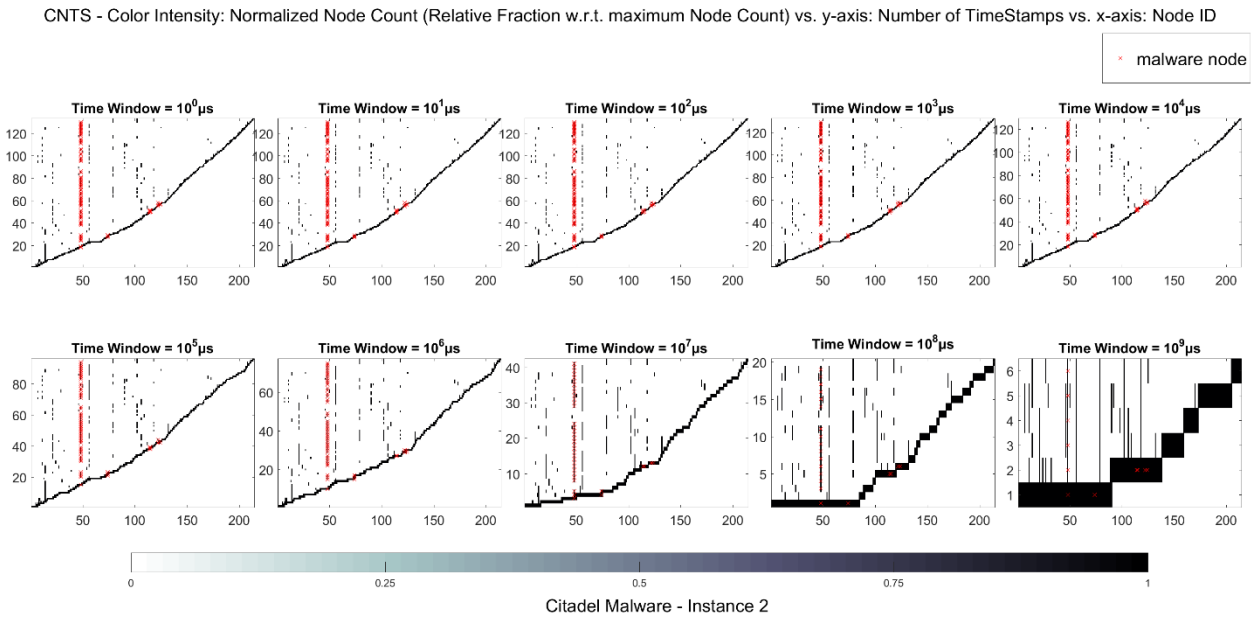

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Citadel Malware - Instance 2

9) TSET

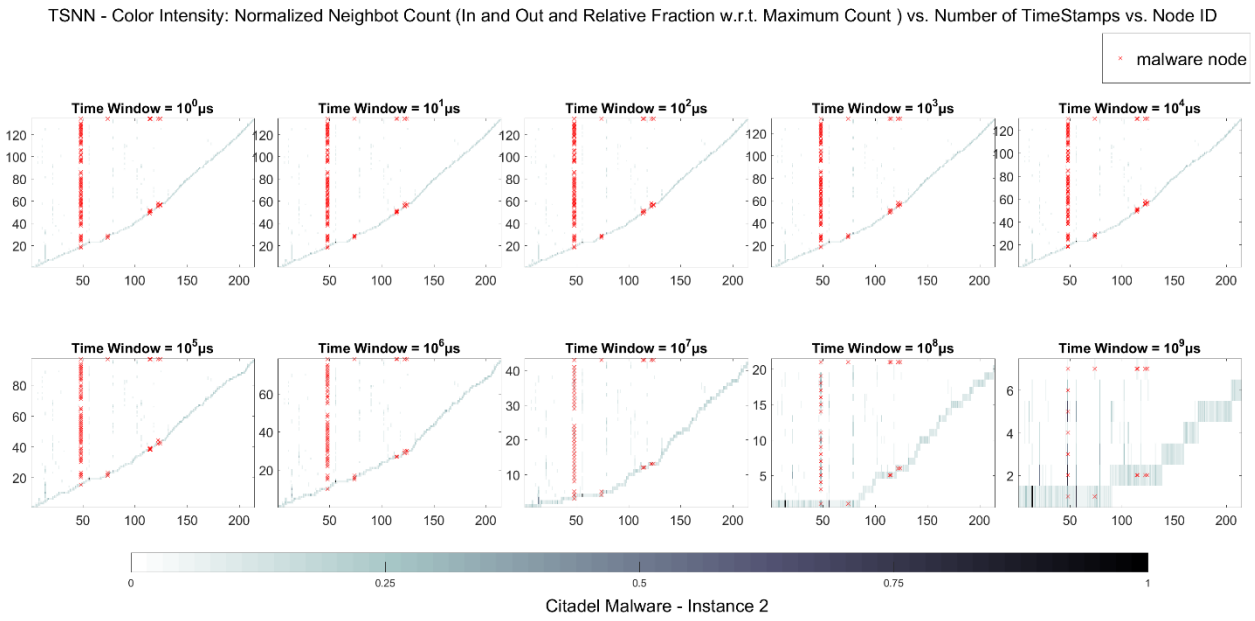


Time Graph Node Based Features

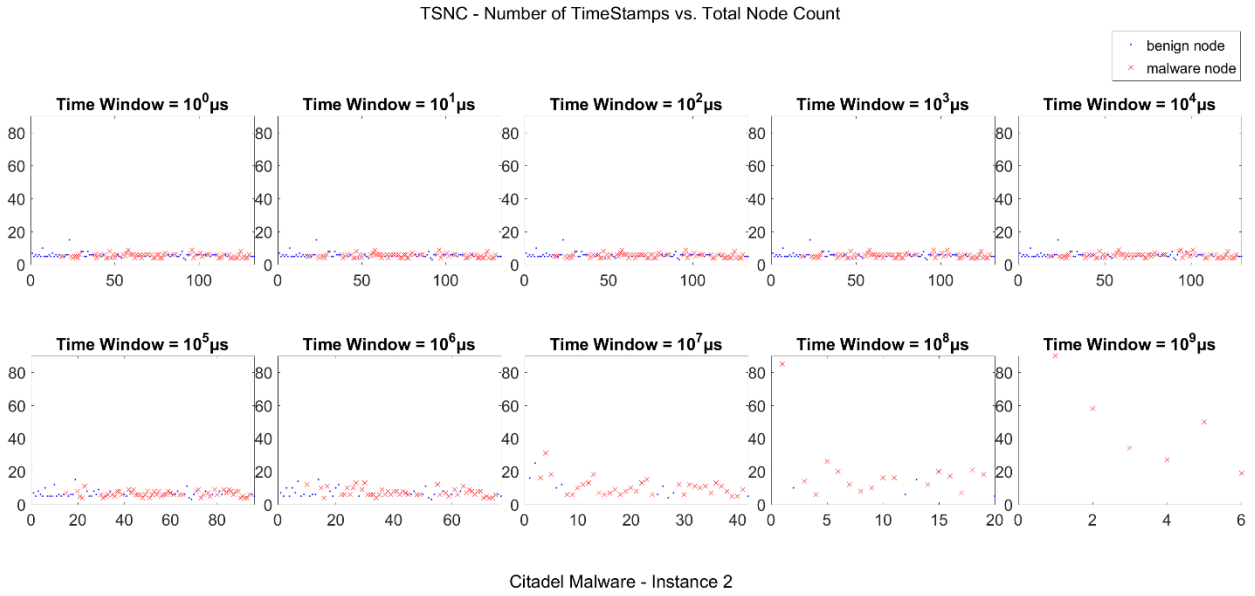
10) CNTS



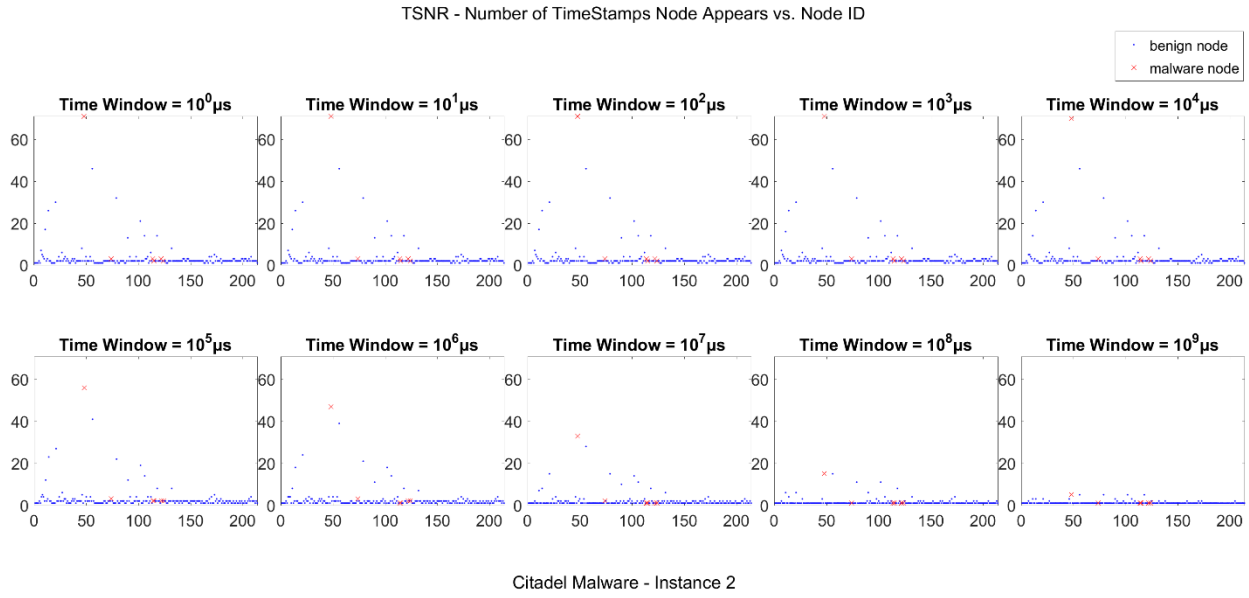
11) TSNN



12) TSNC



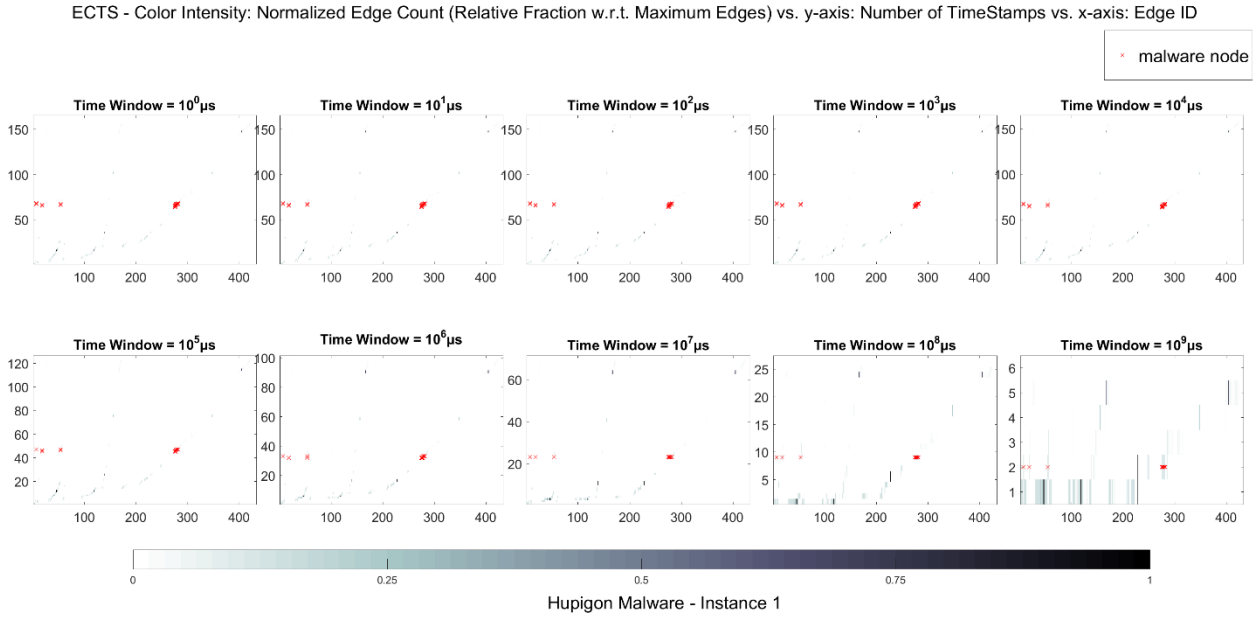
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
20
40
60
0
50
100
150
200
Citadel Malware - Instance 2

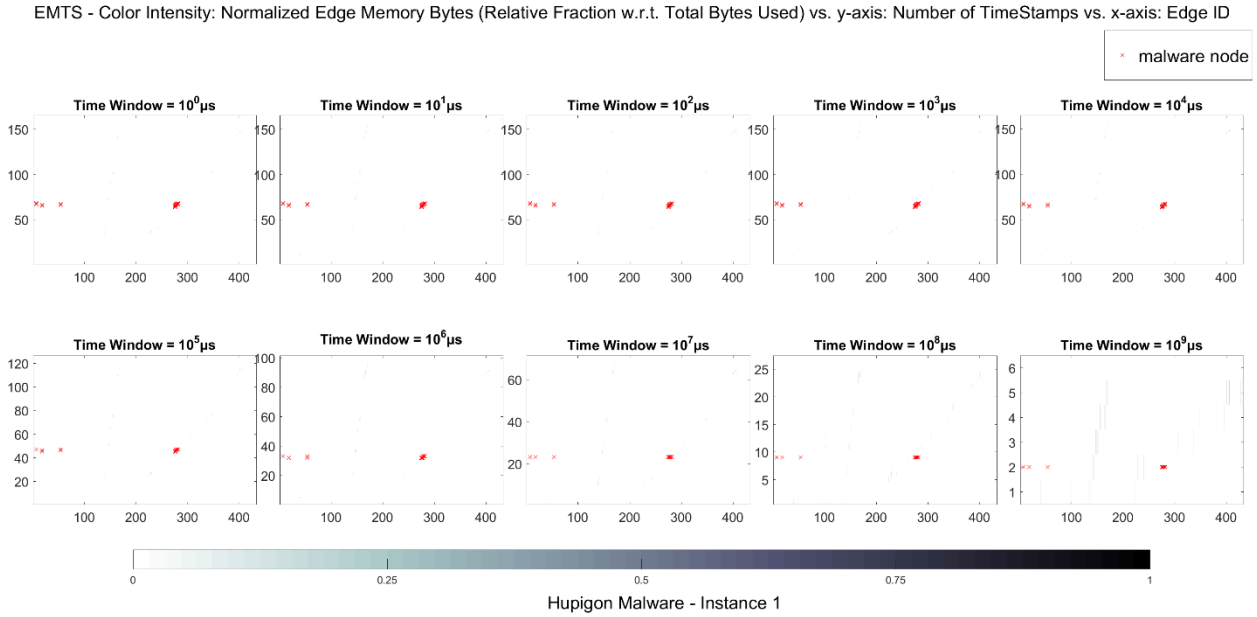
7.1.5 Hupigon Malware – Instance 1

Time Graph Edge Based Features

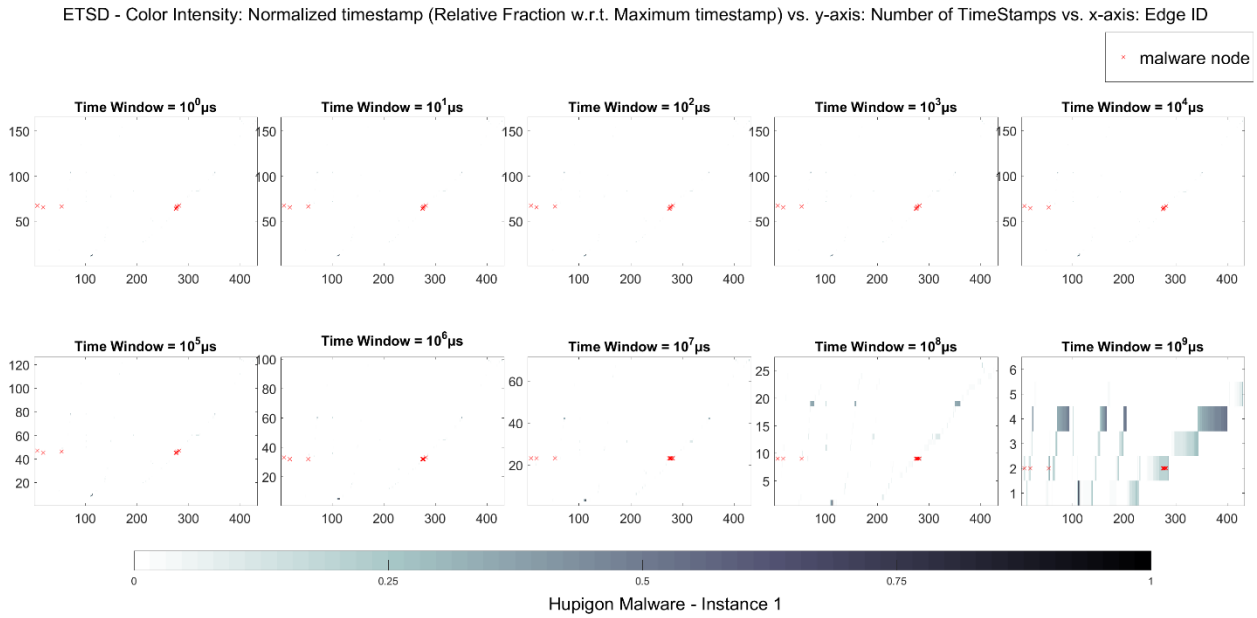
1) ECTS



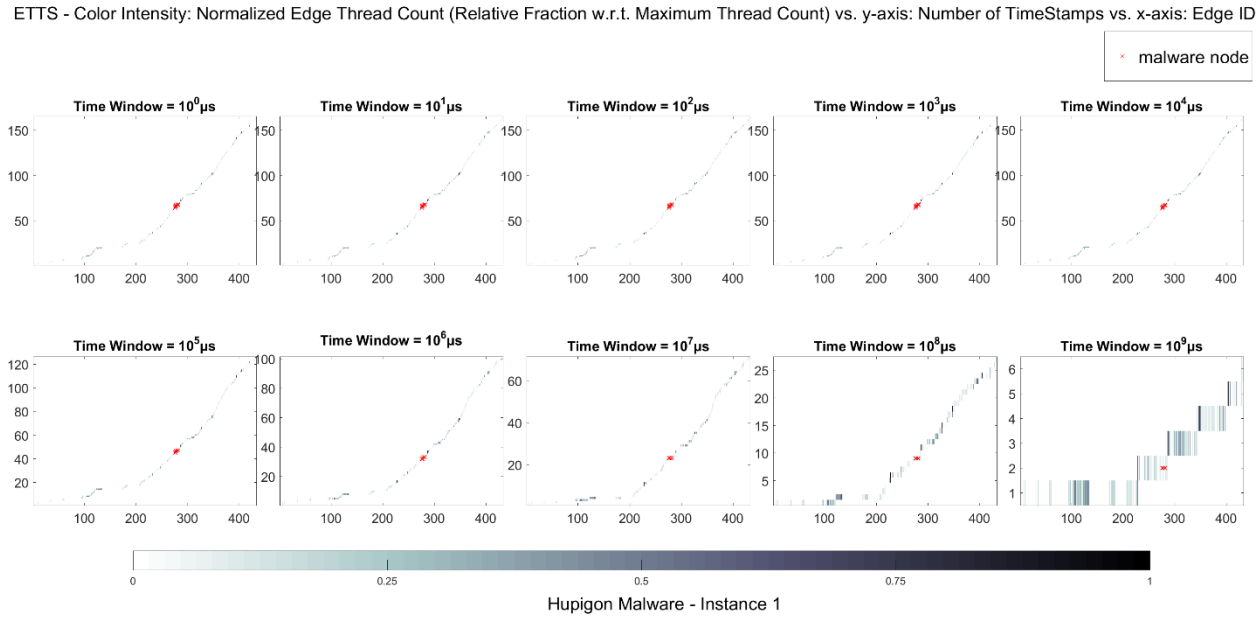
2) EMTS



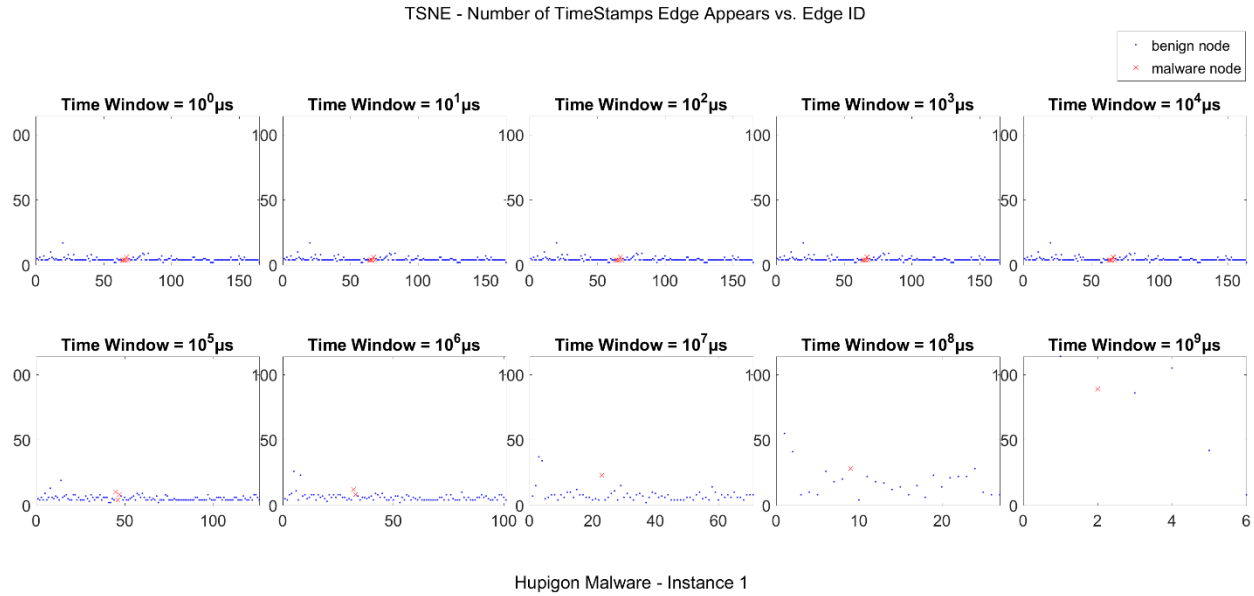
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Hupigon Malware - Instance 1

4) ETTS

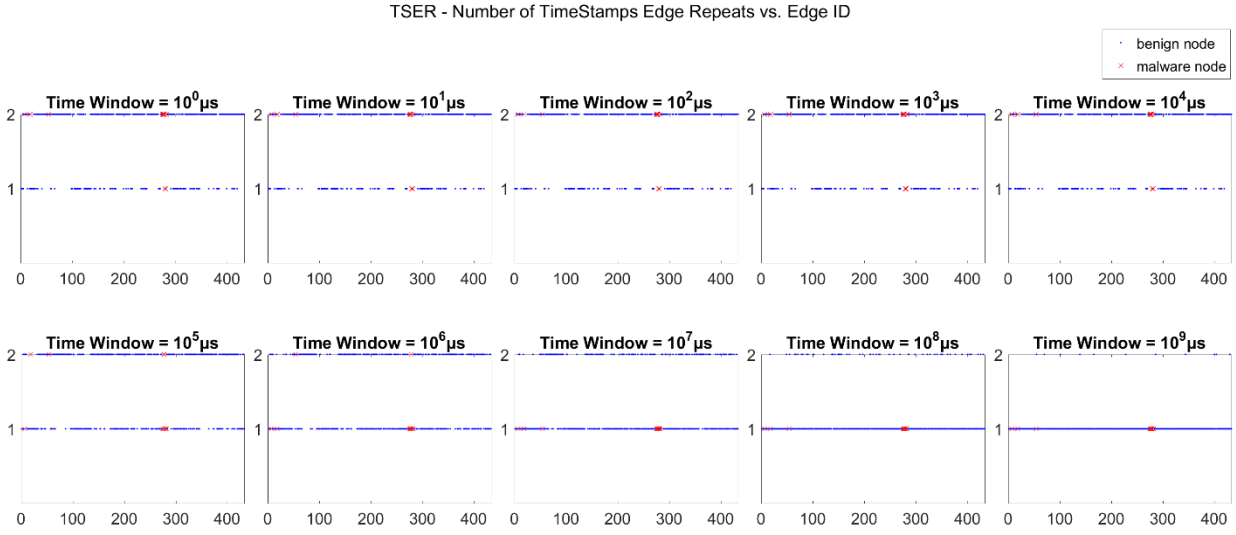

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Hupigon Malware - Instance 1

5) TSNE



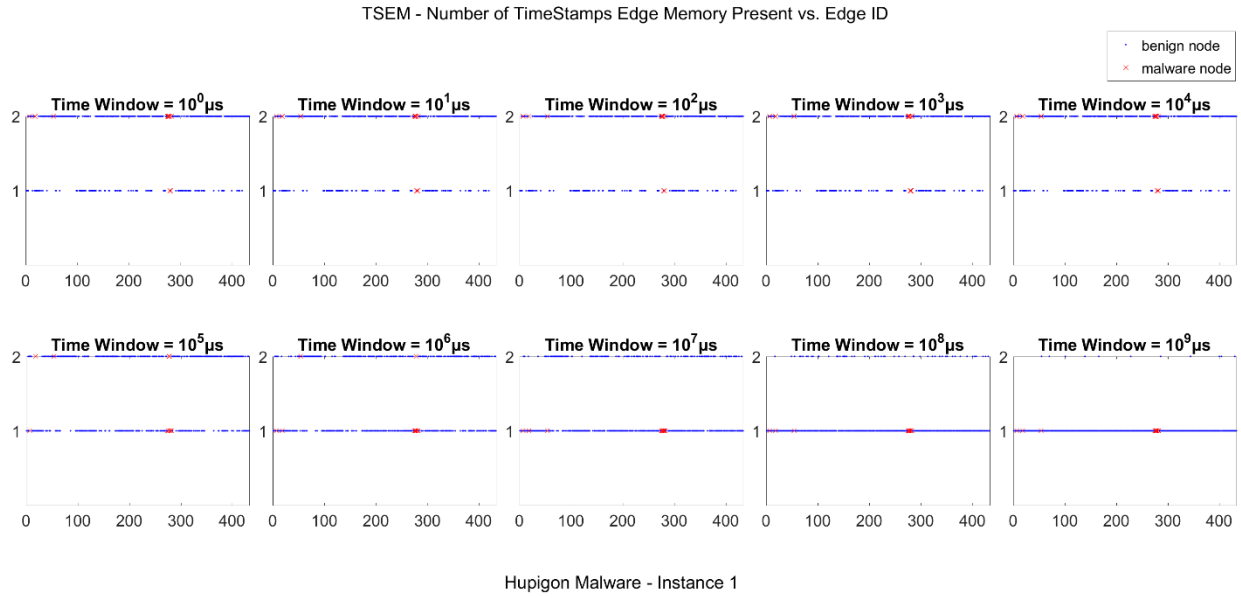
Hupigon Malware - Instance 1

6) TSER

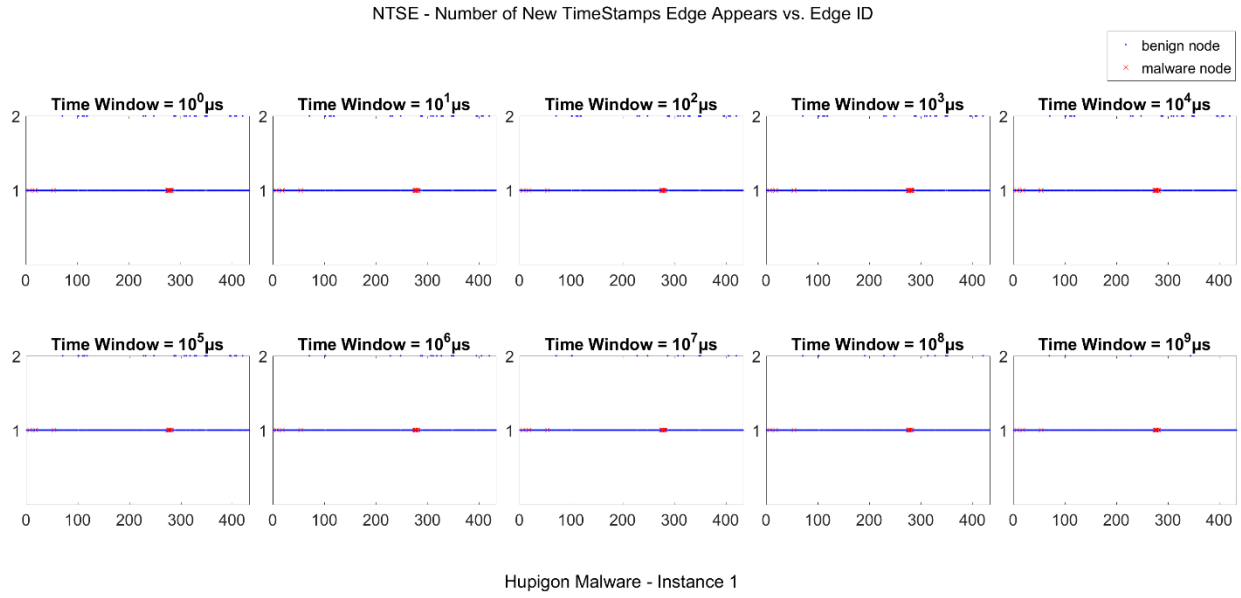


Hupigon Malware - Instance 1

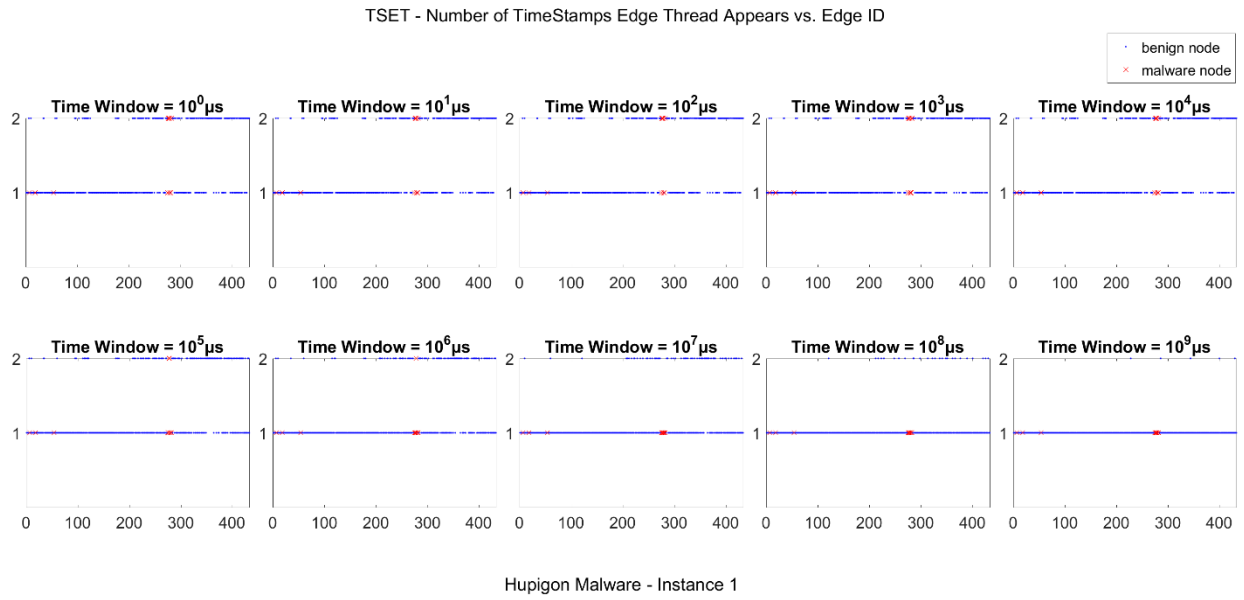
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Hupigon Malware - Instance 1

8) NTSE

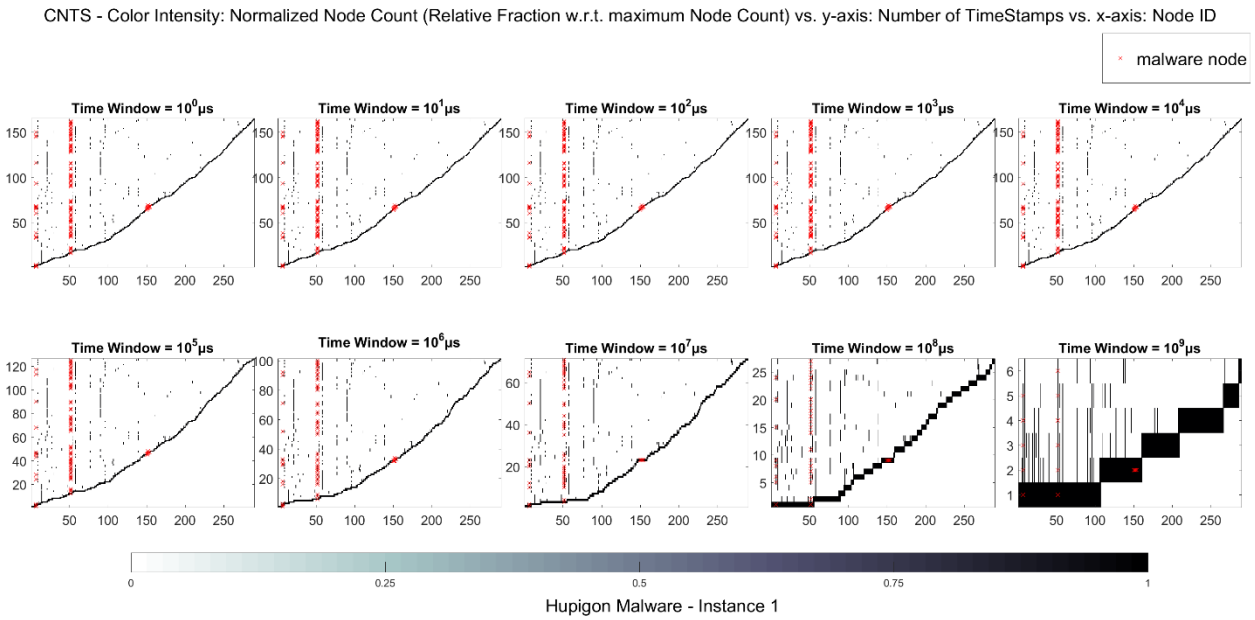

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Hupigon Malware - Instance 1

9) TSET

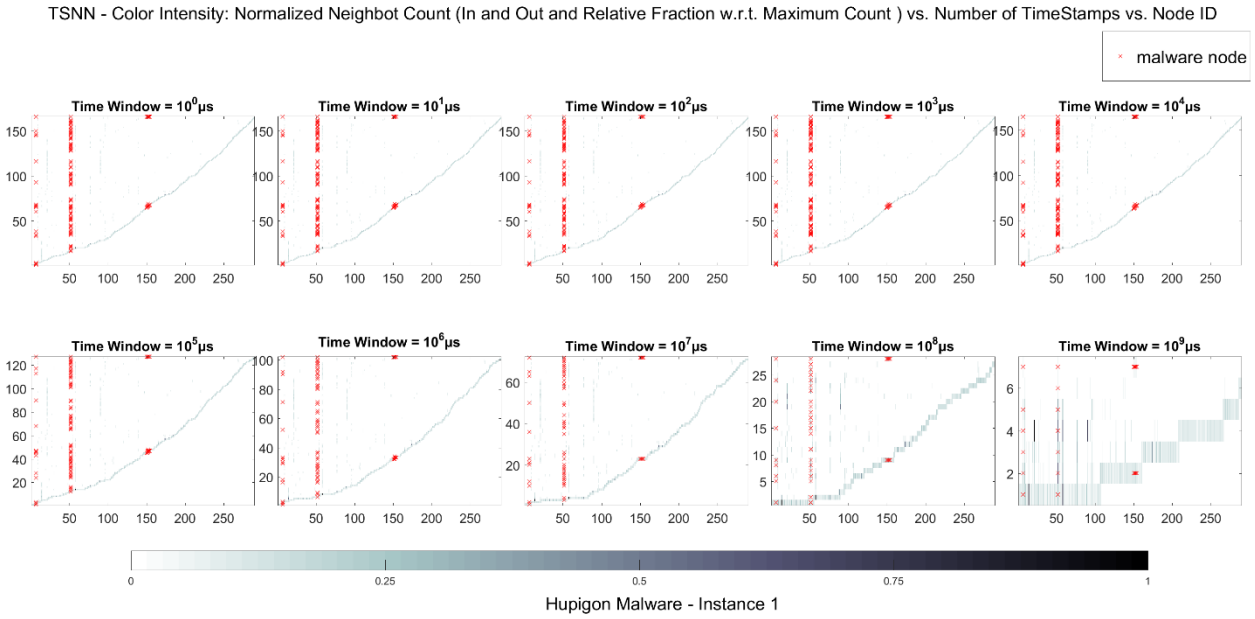


Time Graph Node Based Features

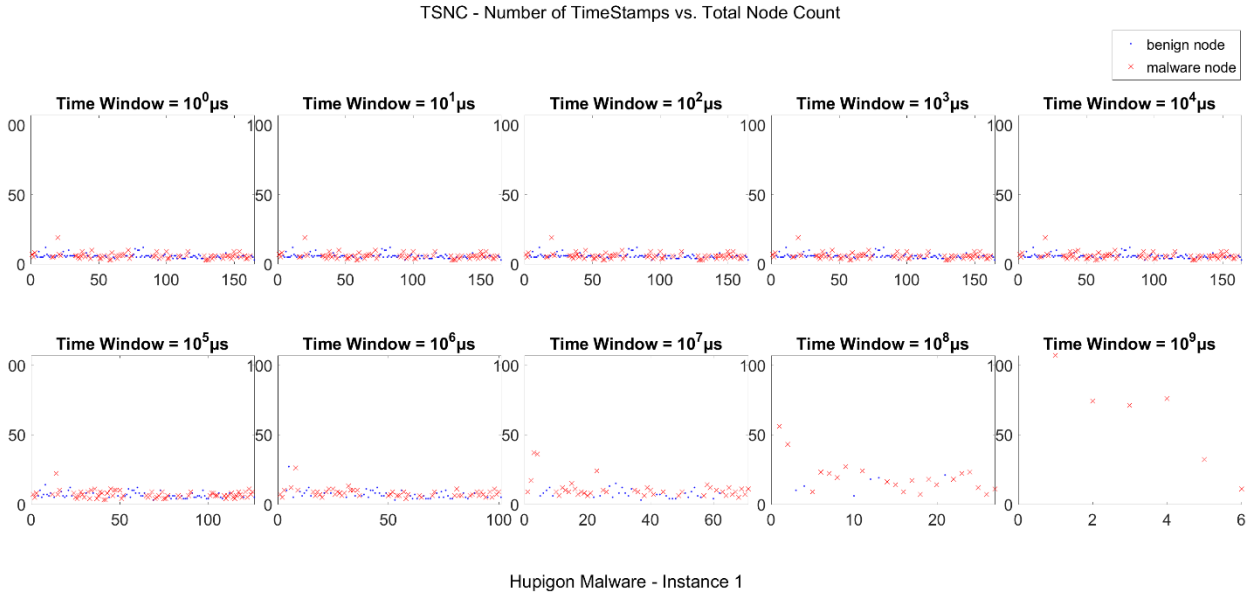
10) CNTS



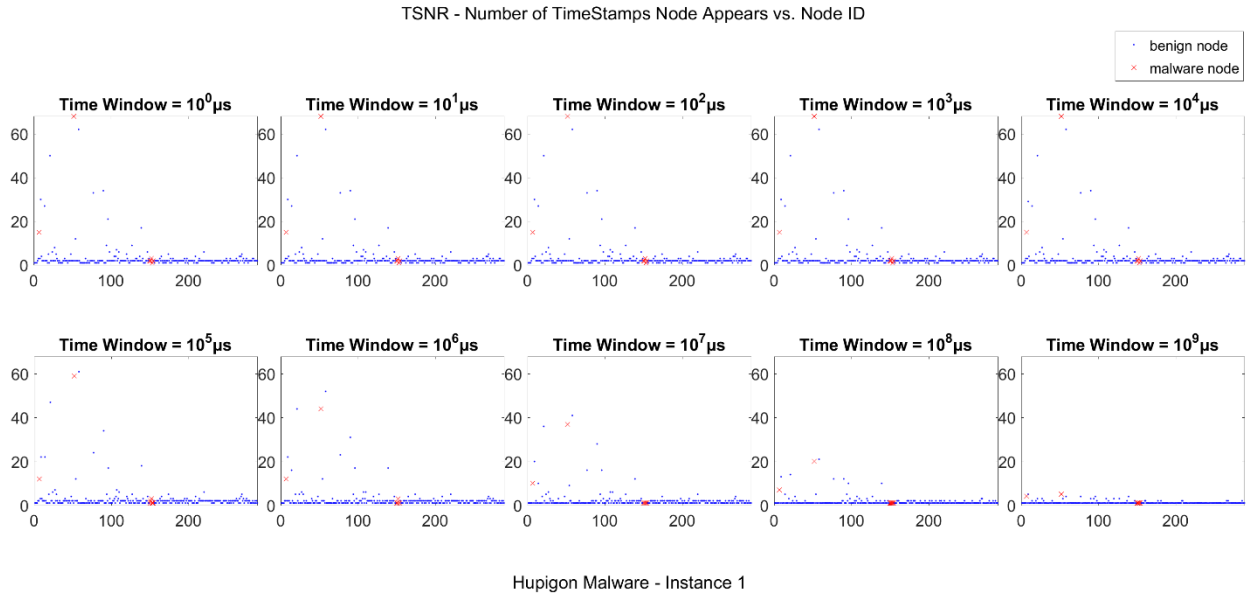
11) TSNN



12) TSNC



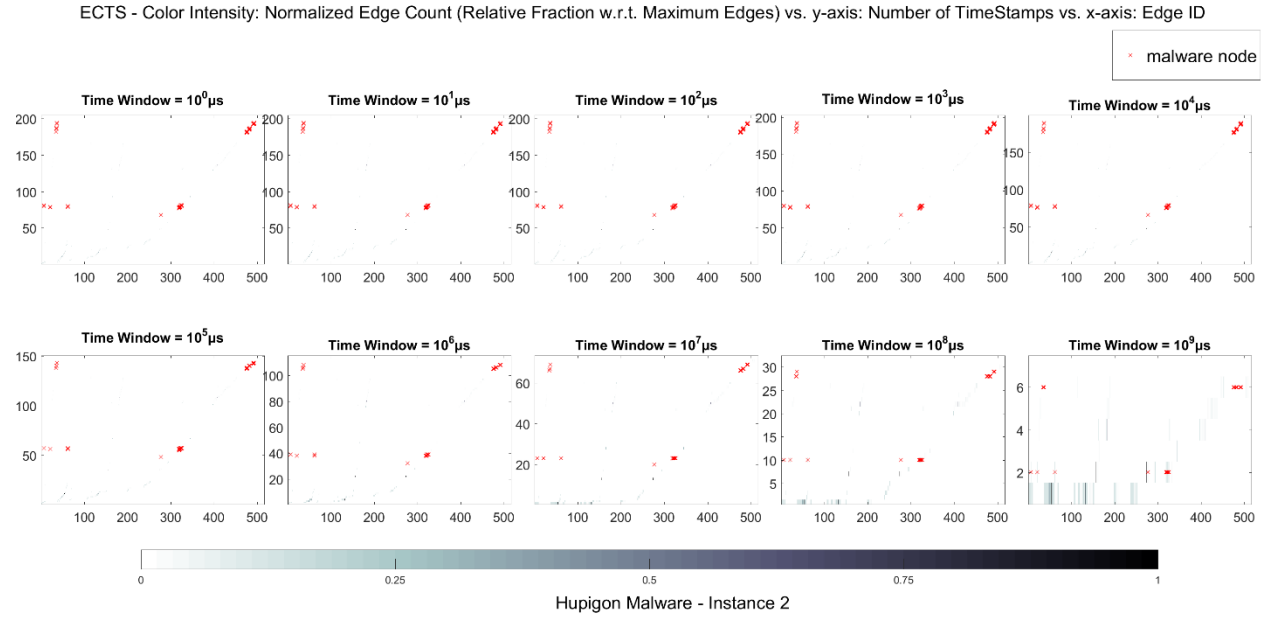
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
20
40
60
0
100
200
Hupigon Malware - Instance 1

7.1.6 Hupigon Malware – Instance 2

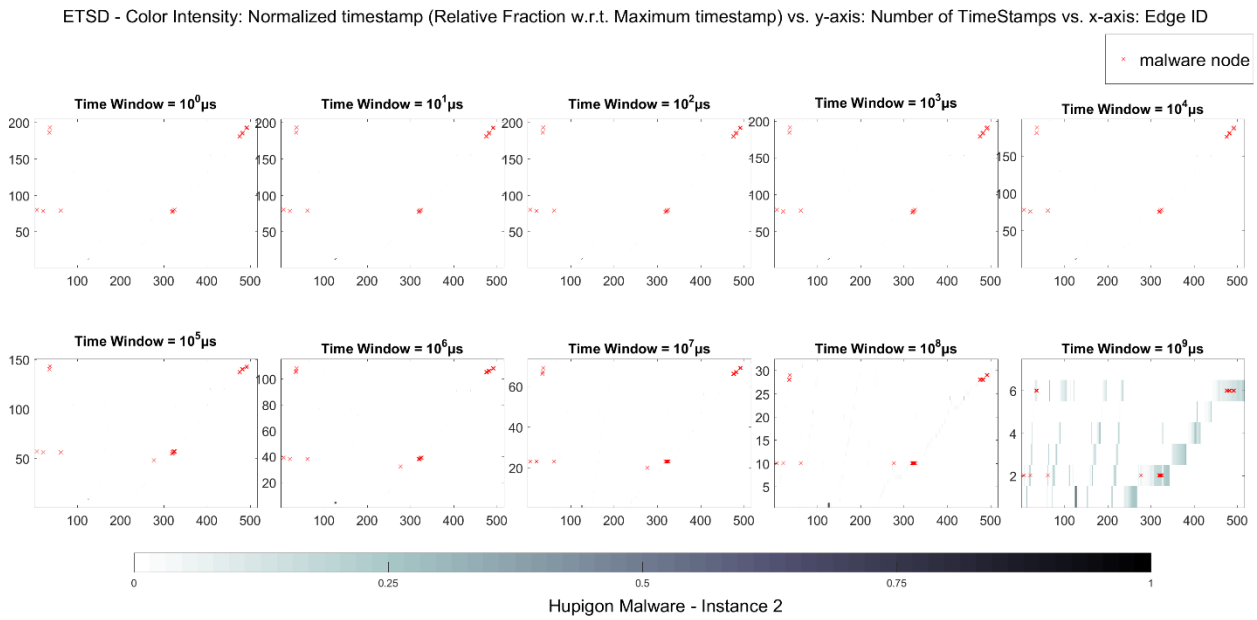
Time Graph Edge Based Features

1) ECTS

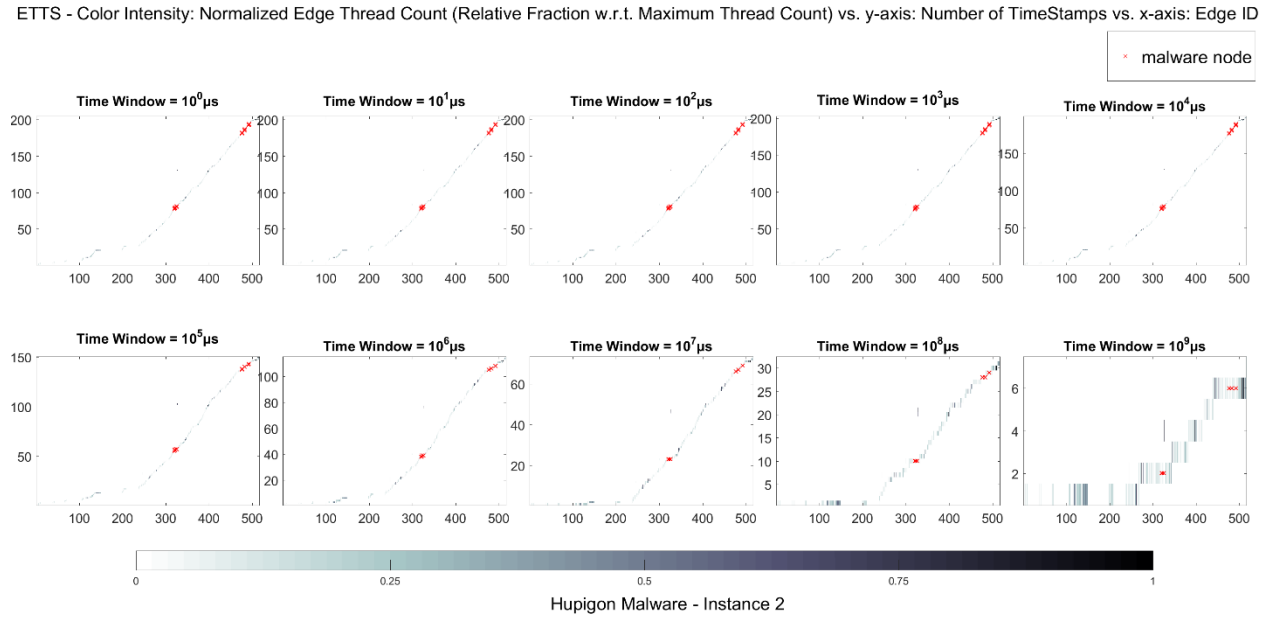


2) EMTS

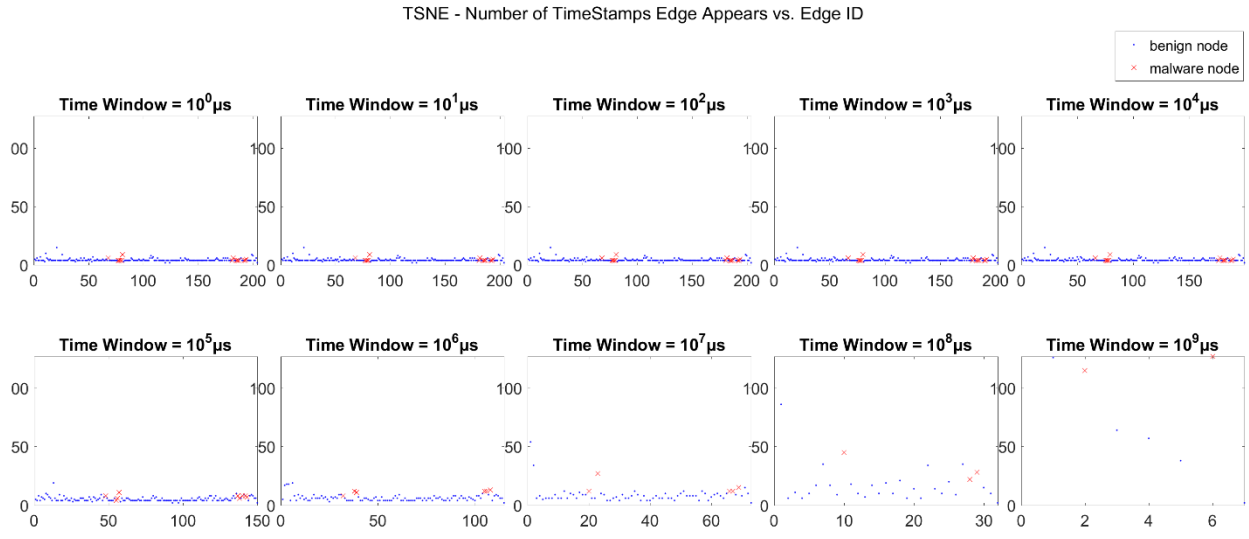
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Hupigon Malware - Instance 2

4) ETTS

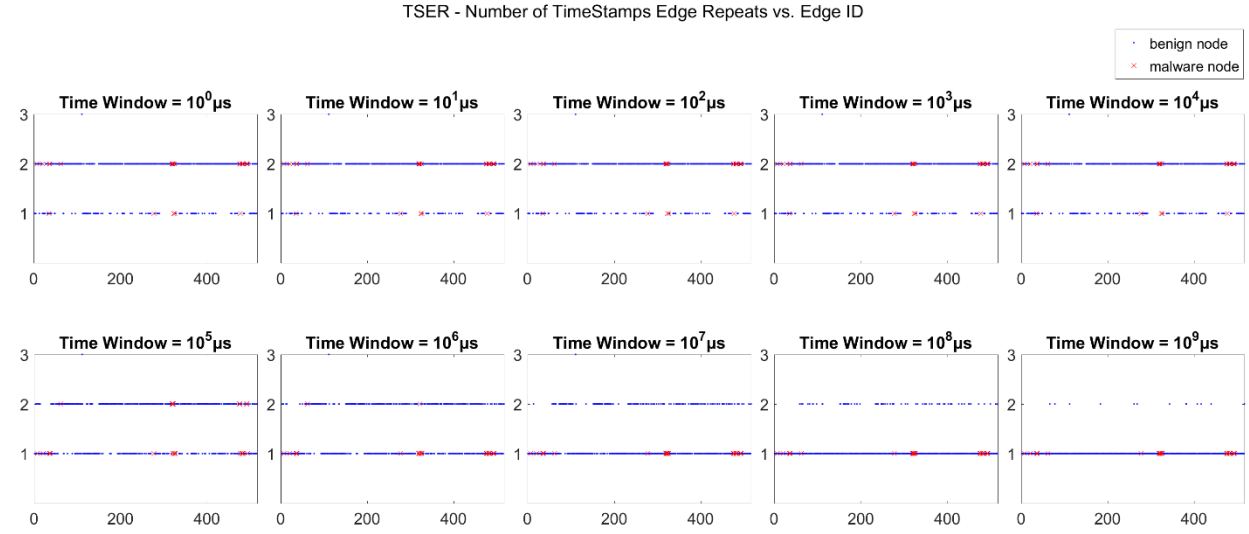

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Hupigon Malware - Instance 2

5) TSNE



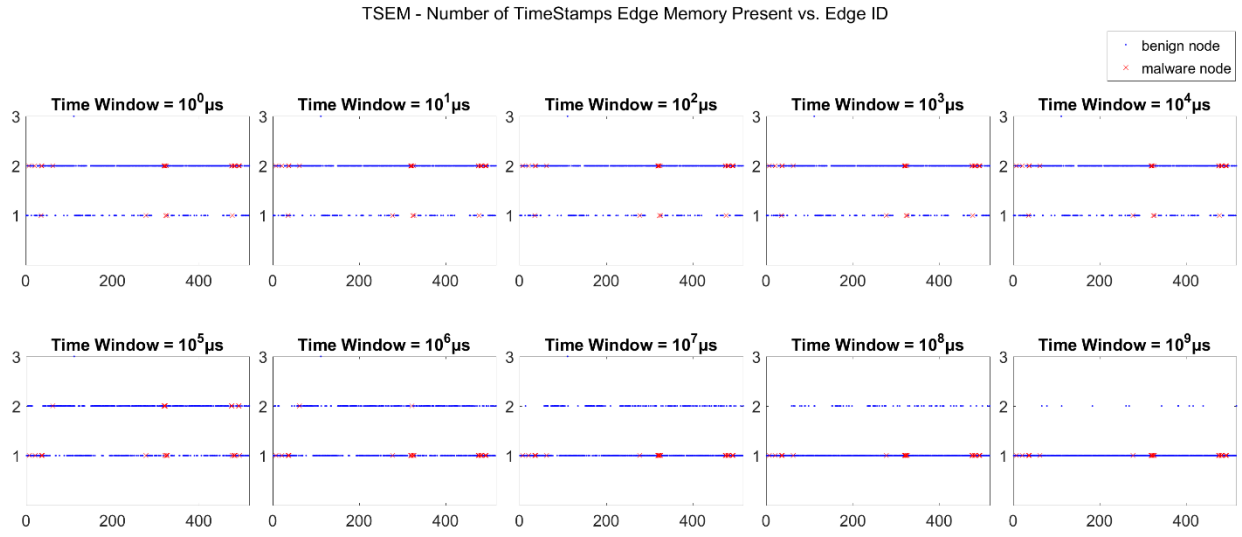
Hupigon Malware - Instance 2

6) TSER



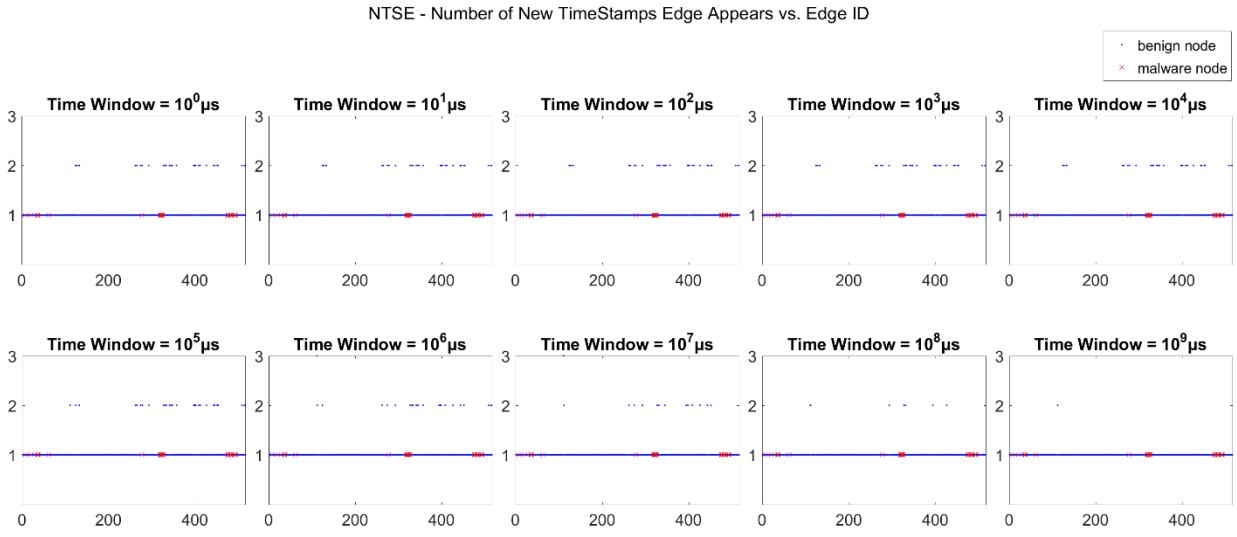
Hupigon Malware - Instance 2

7) TSEM



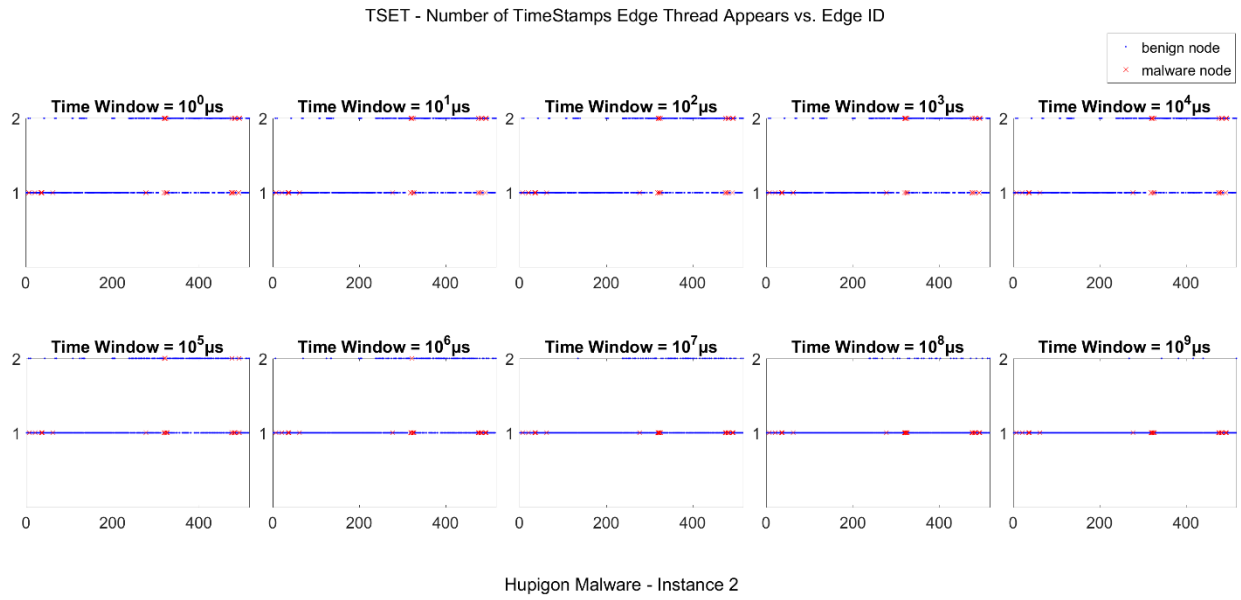
Hupigon Malware - Instance 2

8) NTSE



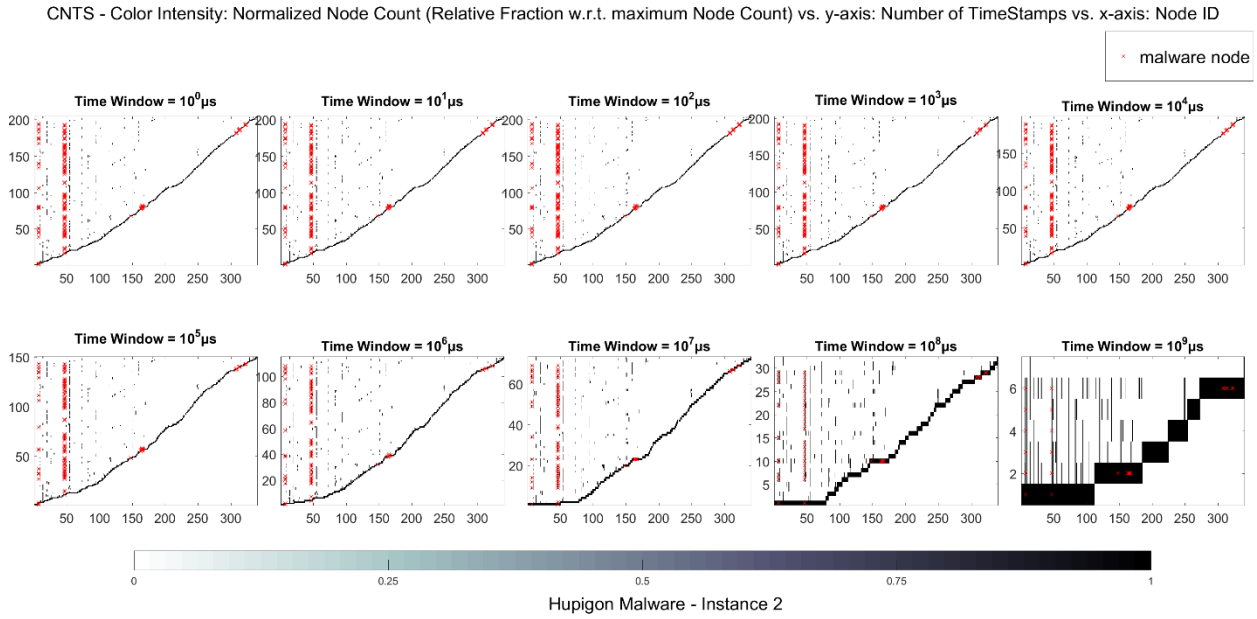
Hupigon Malware - Instance 2

9) TSET

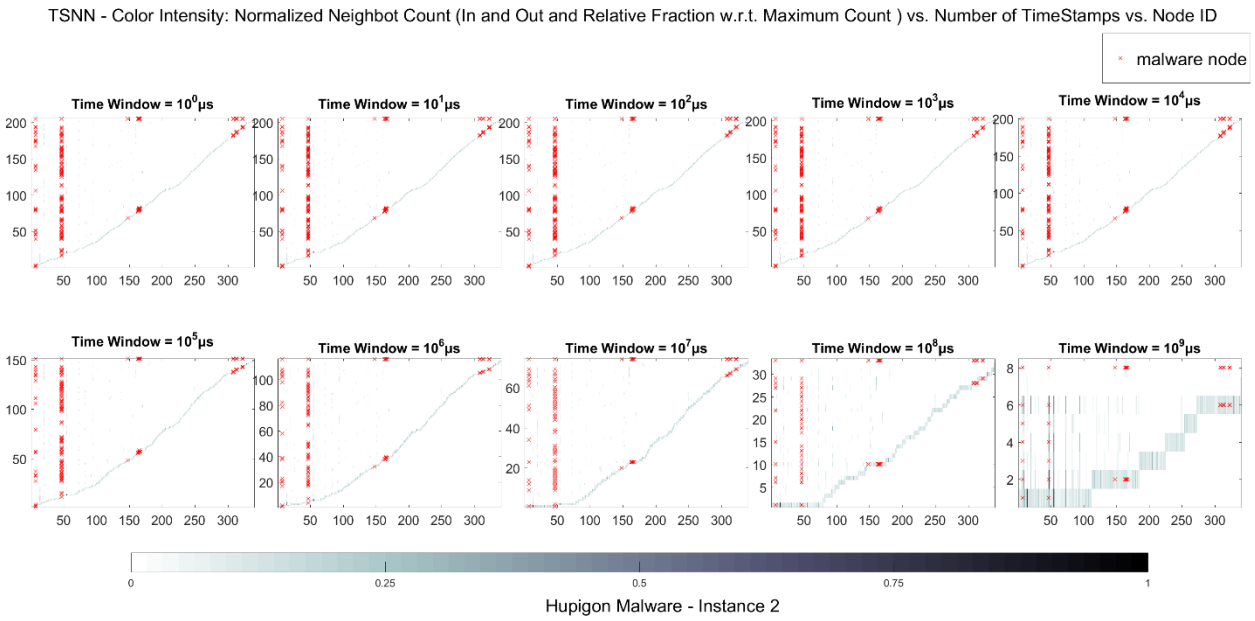


Time Graph Node Based Features

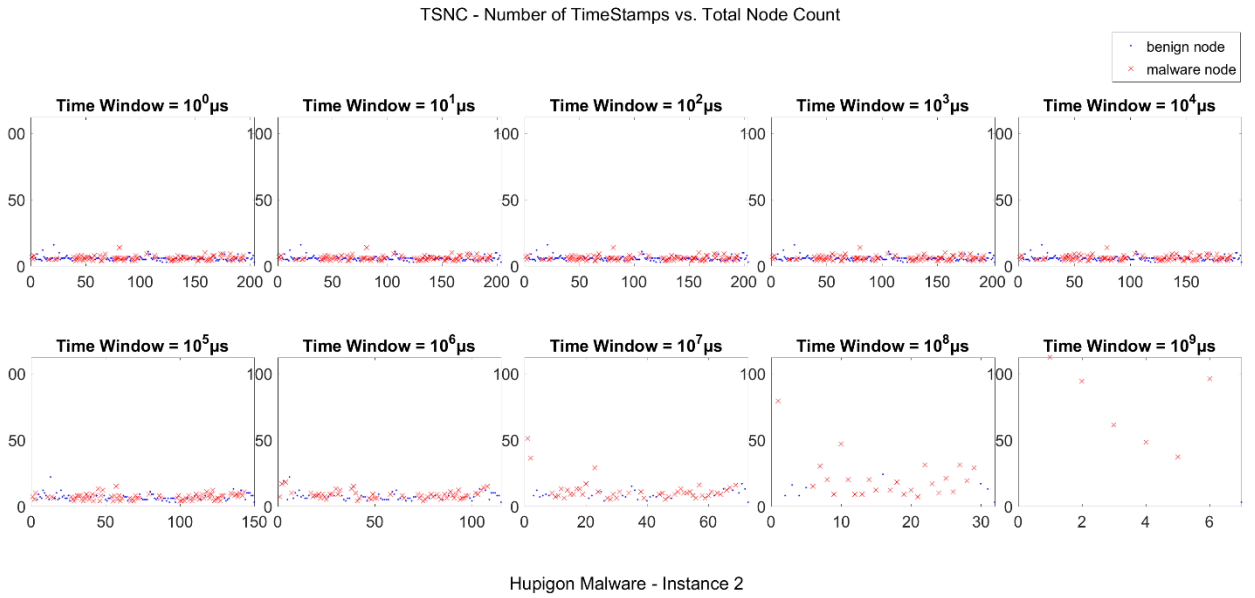
10) CNTS



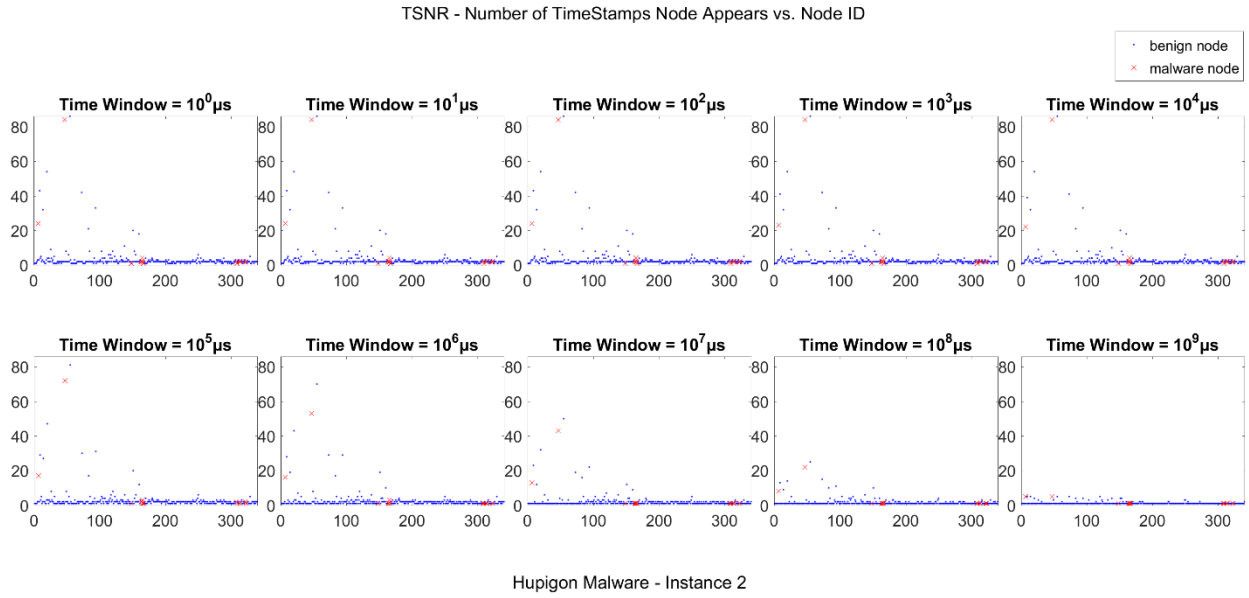
11) TSNN



12) TSNC



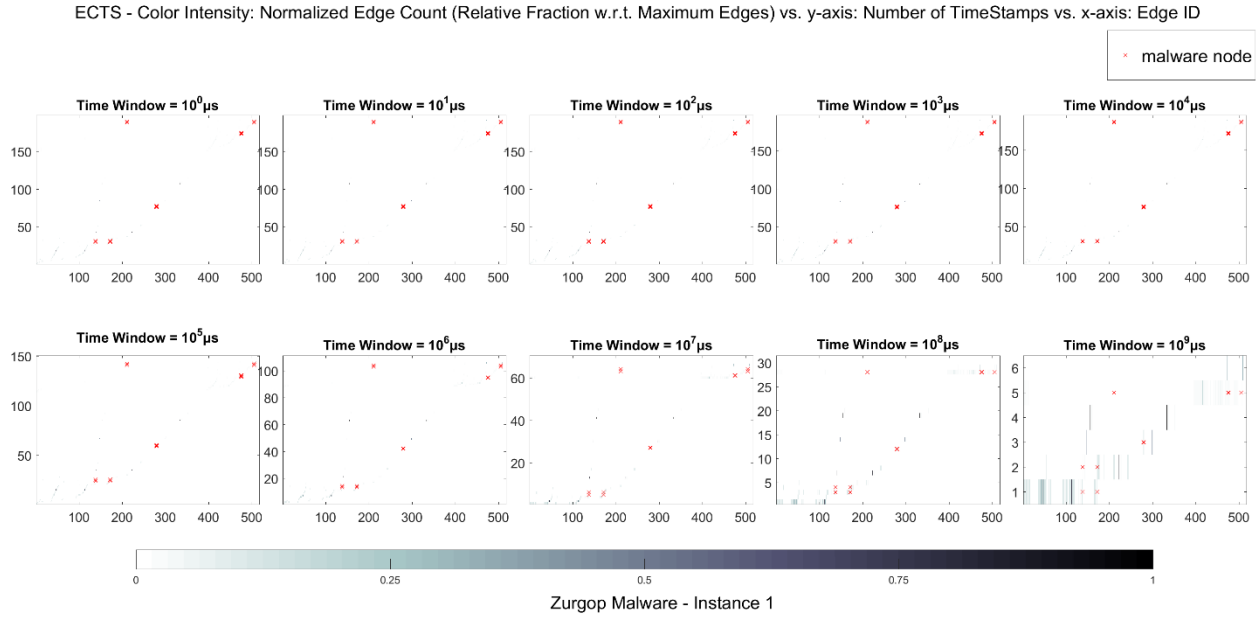
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Hupigon Malware - Instance 2

7.1.7 Zurgop Malware – Instance 1

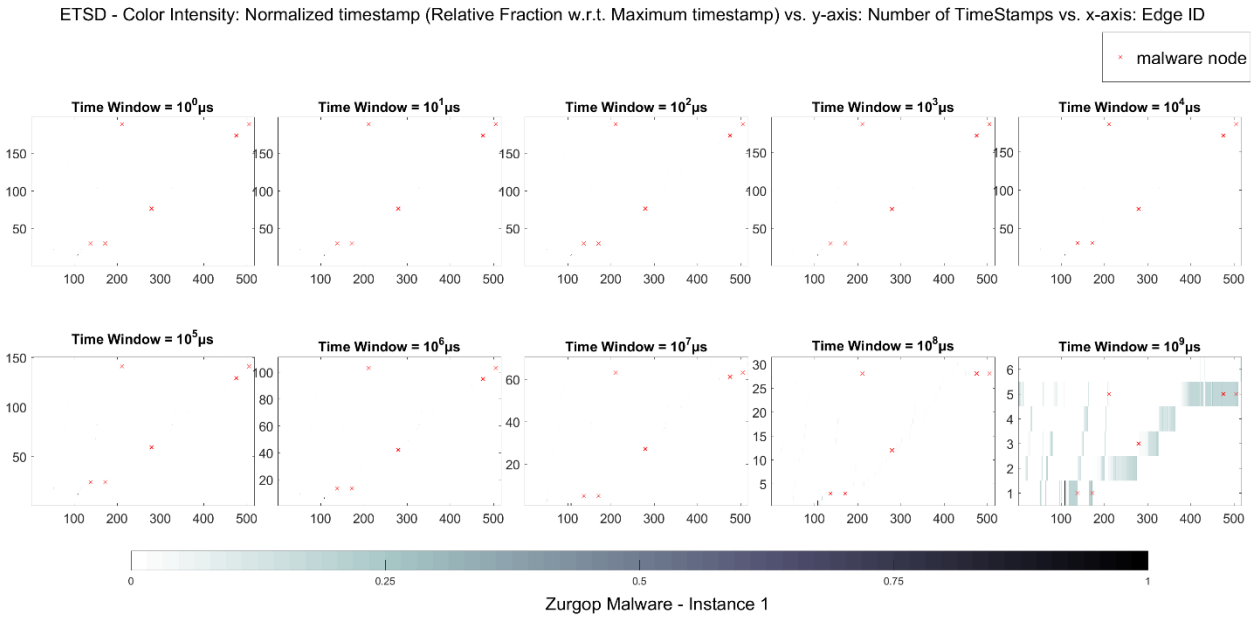
Time Graph Edge Based Features

1) ECTS

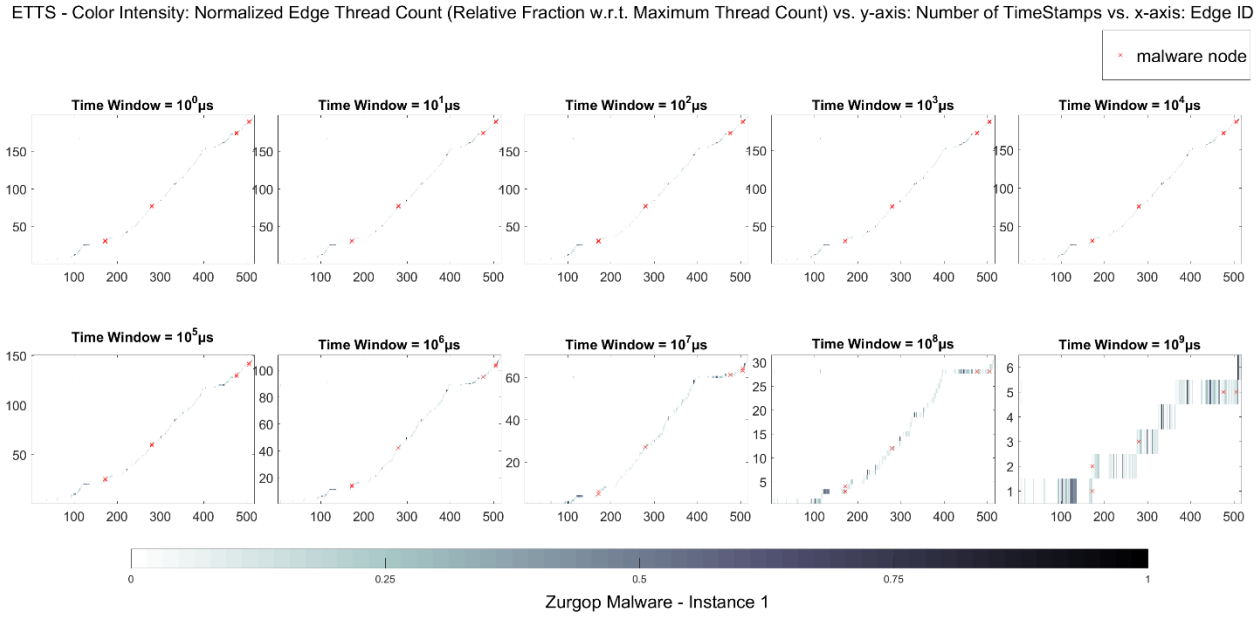


2) EMTS

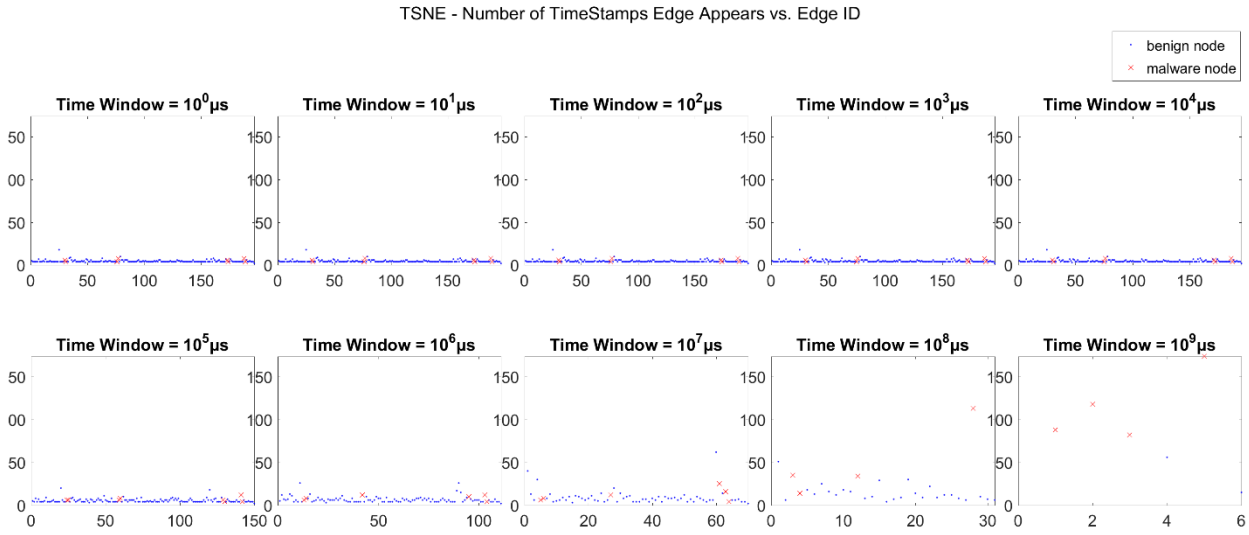
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Zurgop Malware - Instance 1

4) ETTS

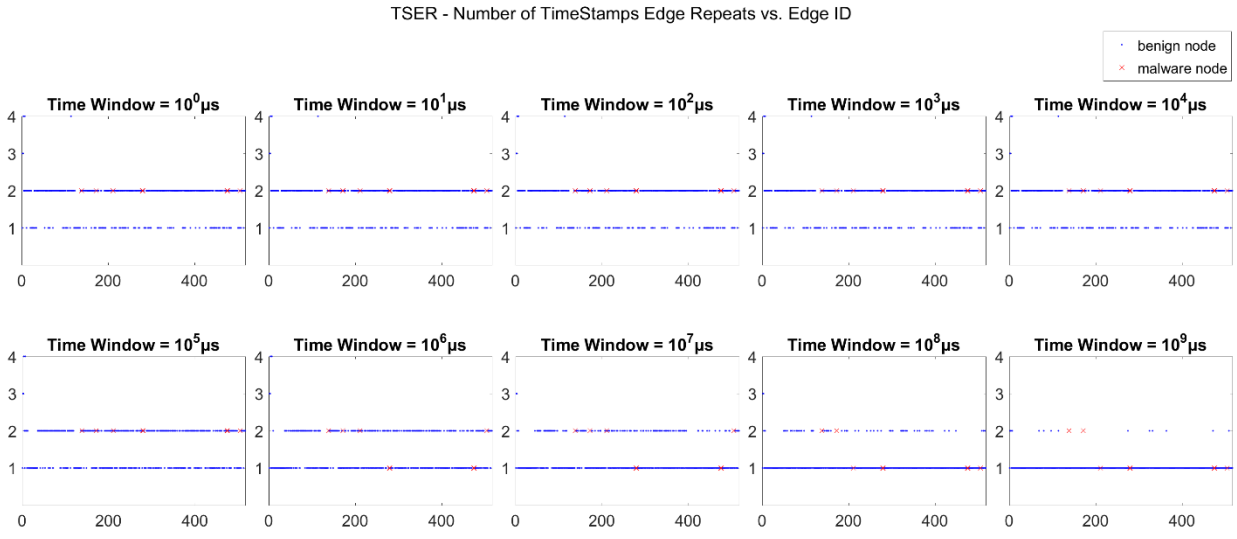

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Zurgop Malware - Instance 1

5) TSNE



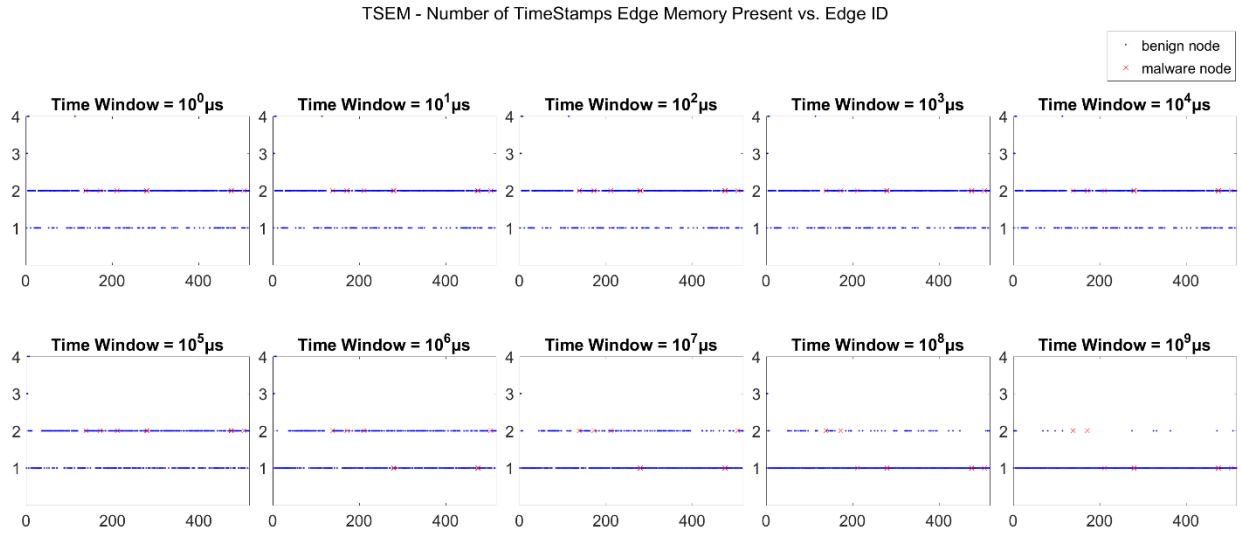
Zurgop Malware - Instance 1

6) TSER

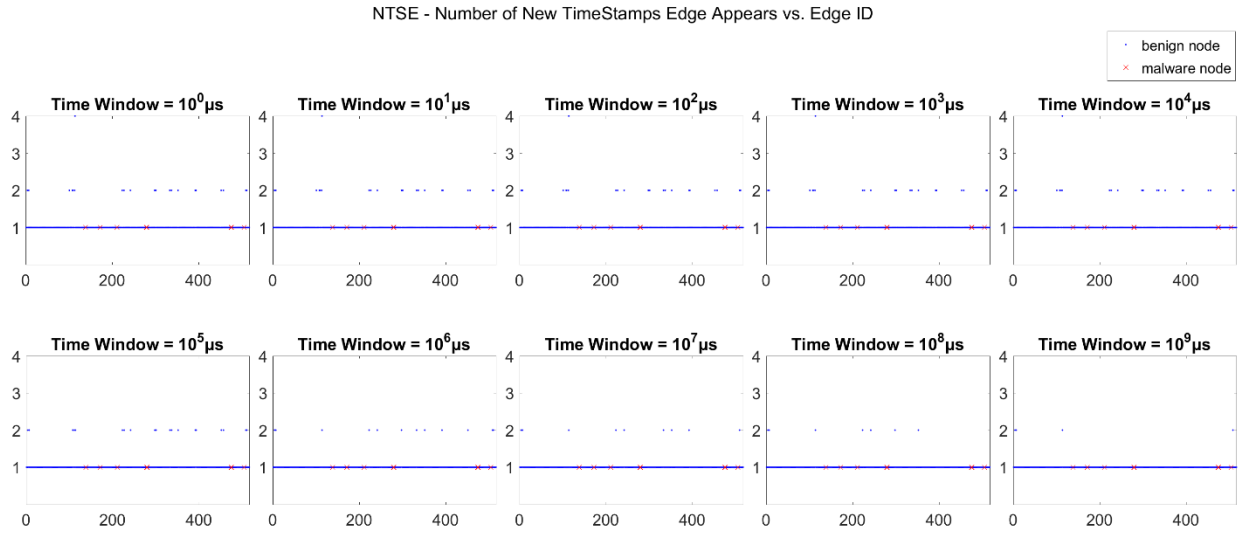


Zurgop Malware - Instance 1

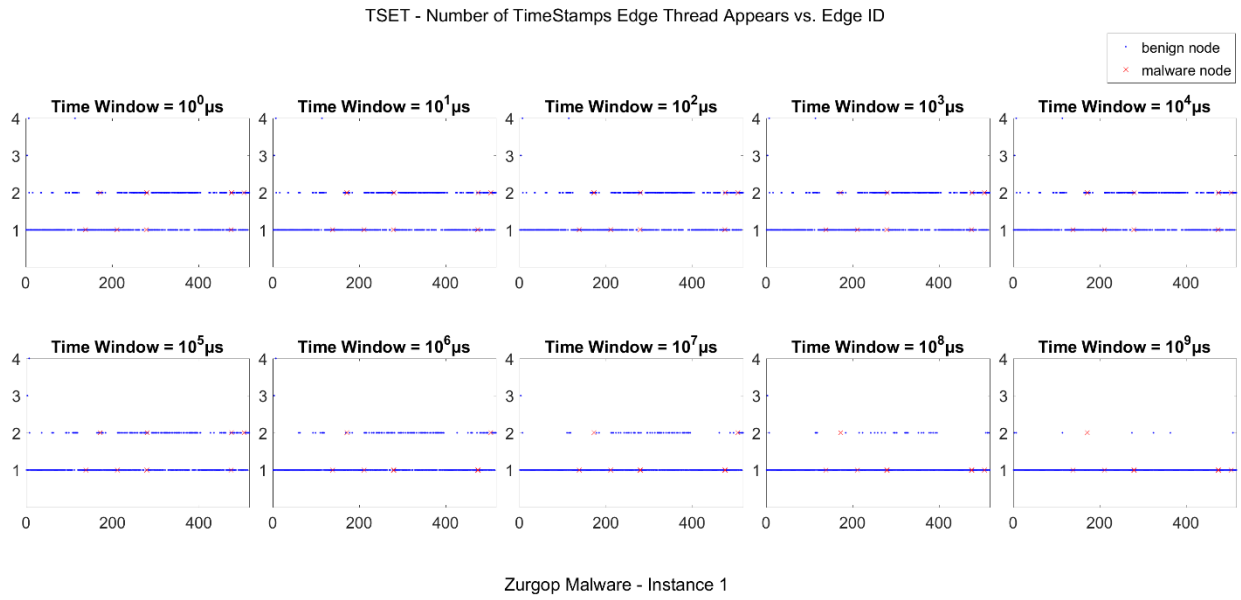
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Zurgop Malware - Instance 1

8) NTSE

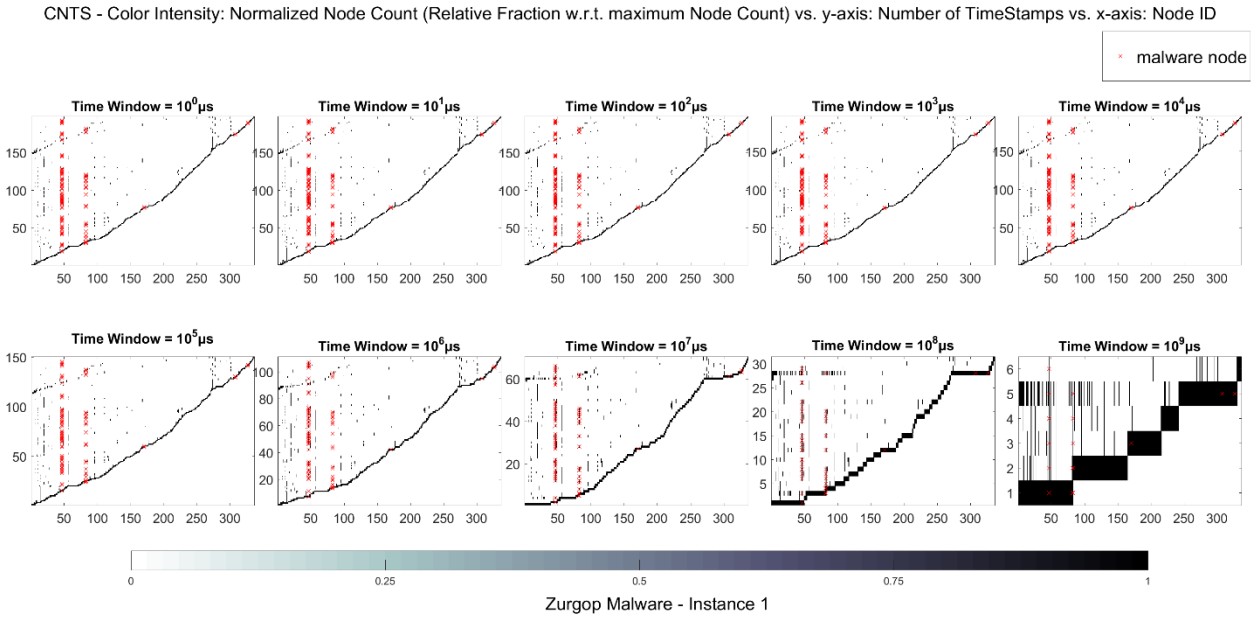

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Zurgop Malware - Instance 1

9) TSET

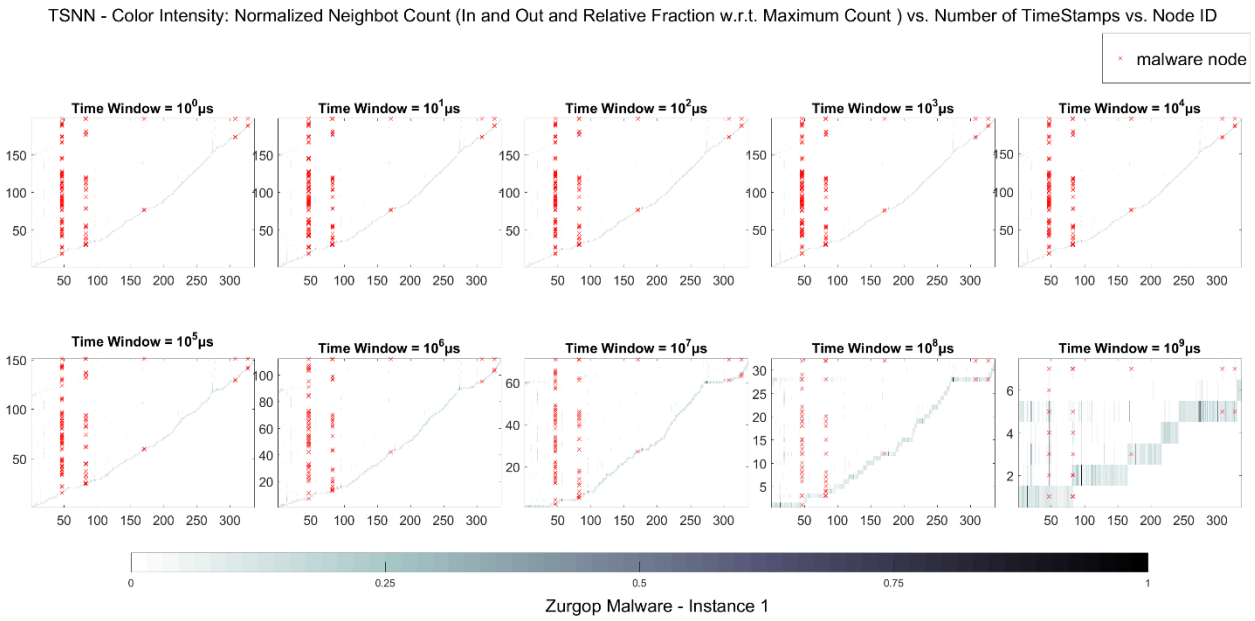


Time Graph Node Based Features

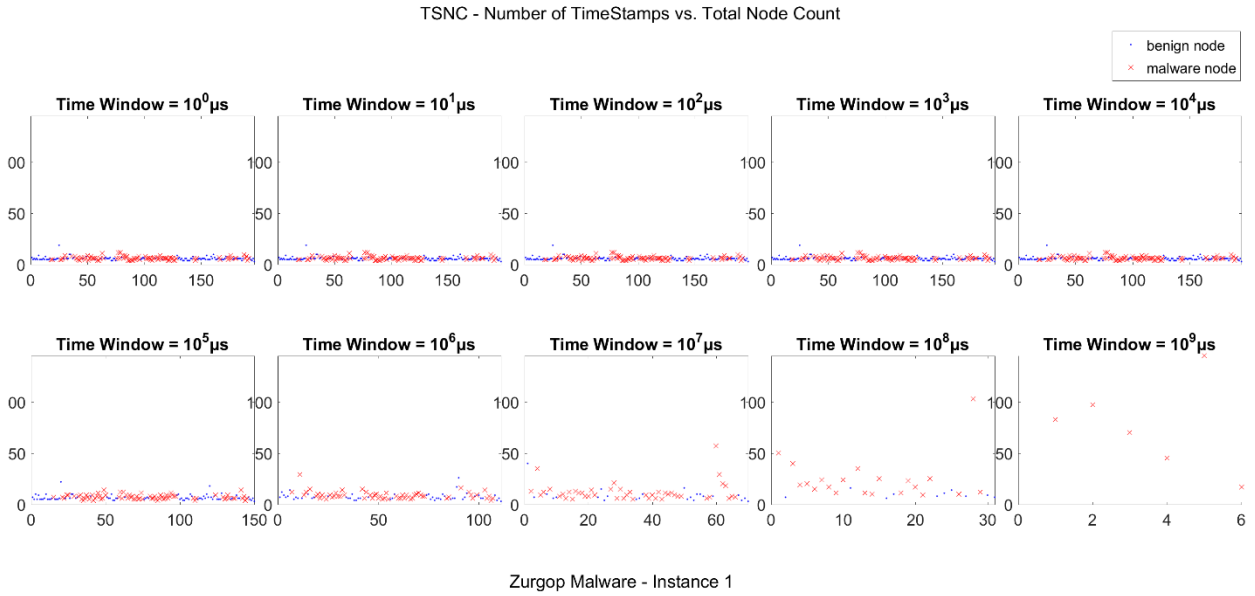
10) CNTS



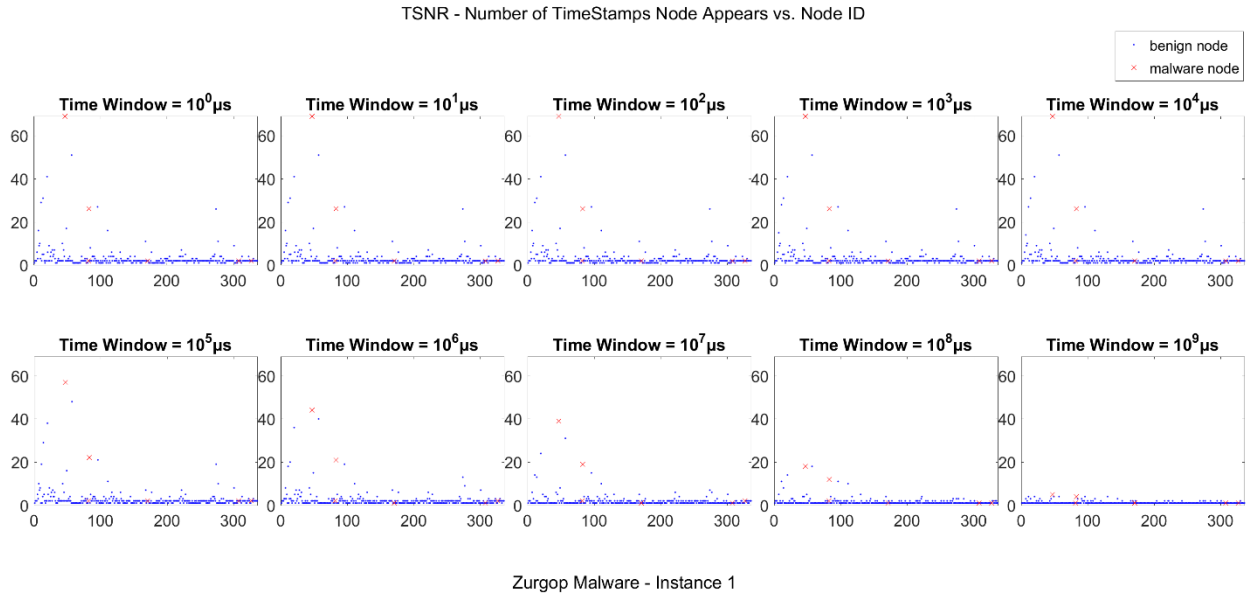
11) TSNN



12) TSNC



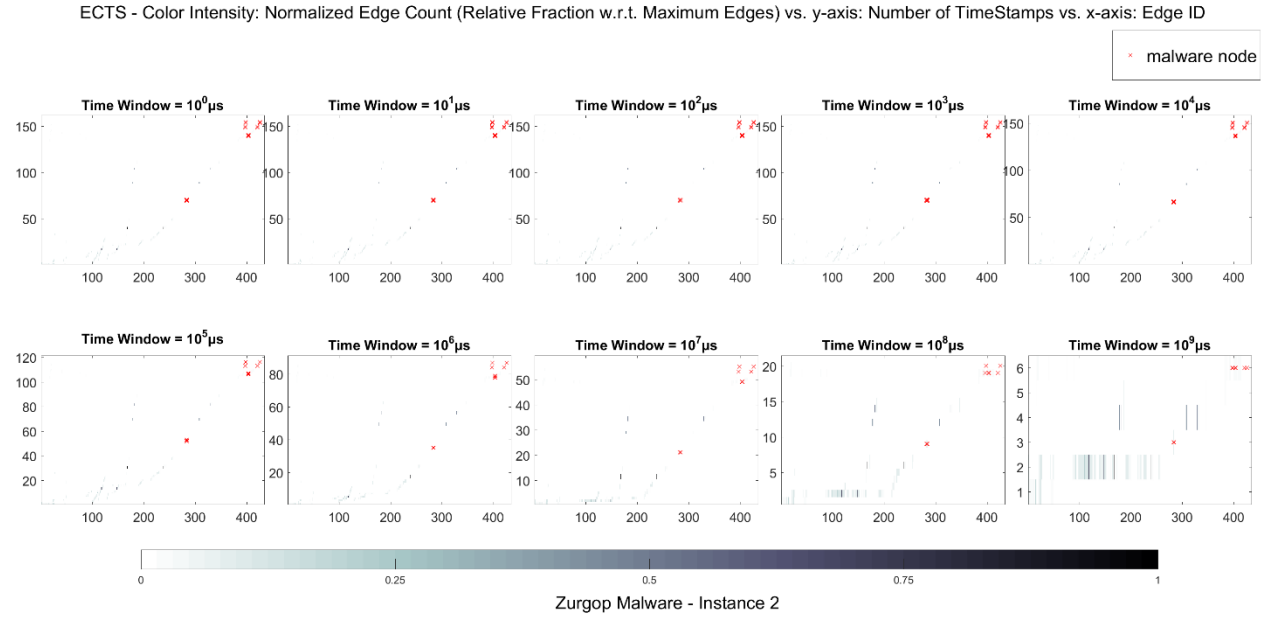
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
20
40
60
0
100
200
300
Zurgop Malware - Instance 1

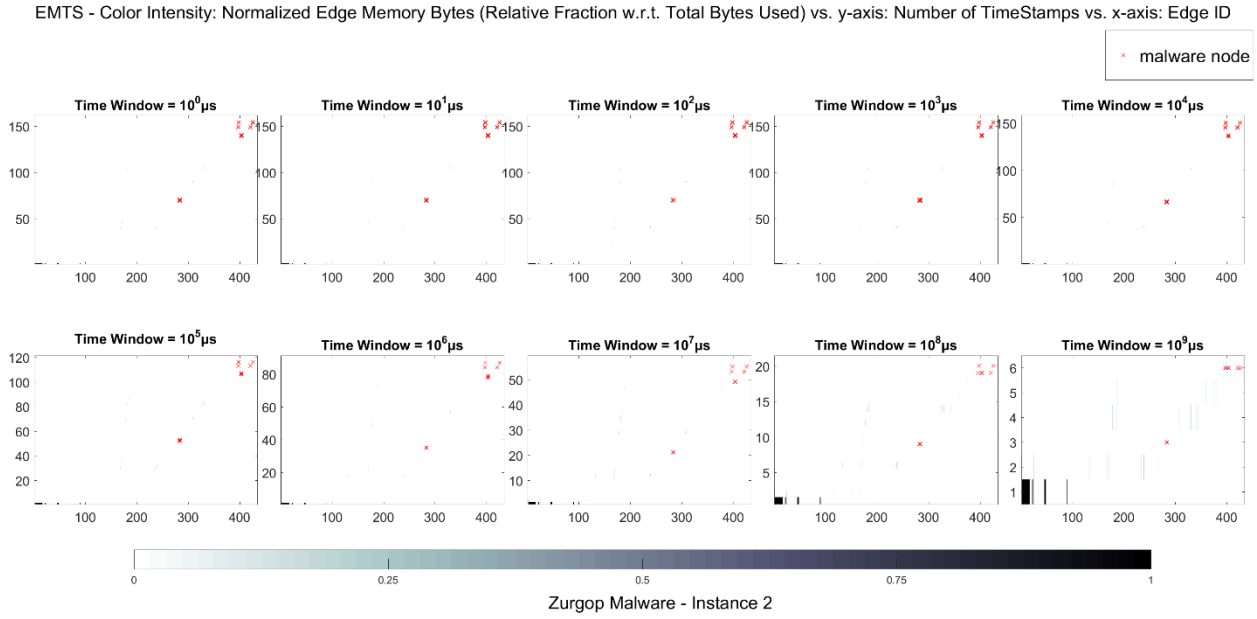
7.1.8 Zurgop Malware – Instance 2

Time Graph Edge Based Features

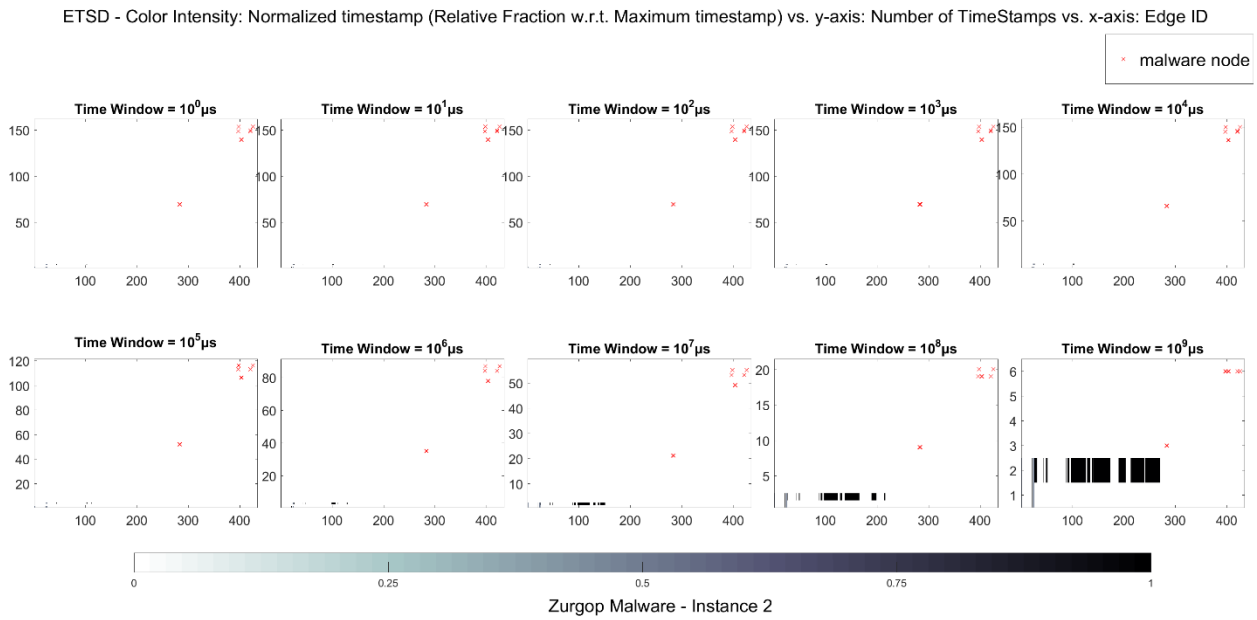
1) ECTS



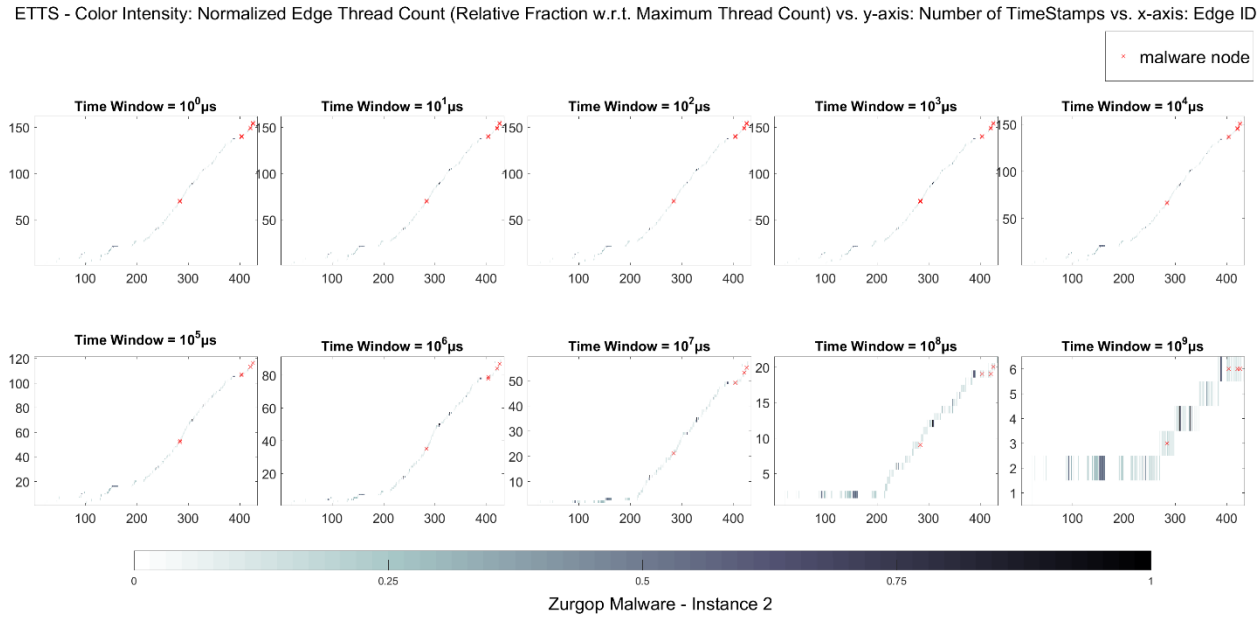
2) EMTS



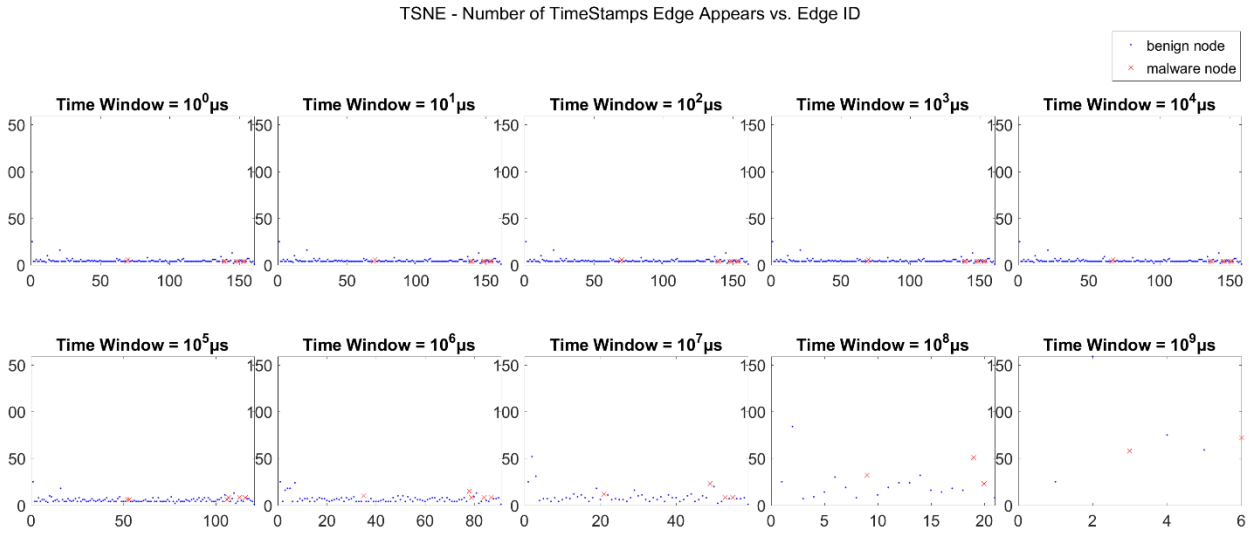
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Zurgop Malware - Instance 2

4) ETTS

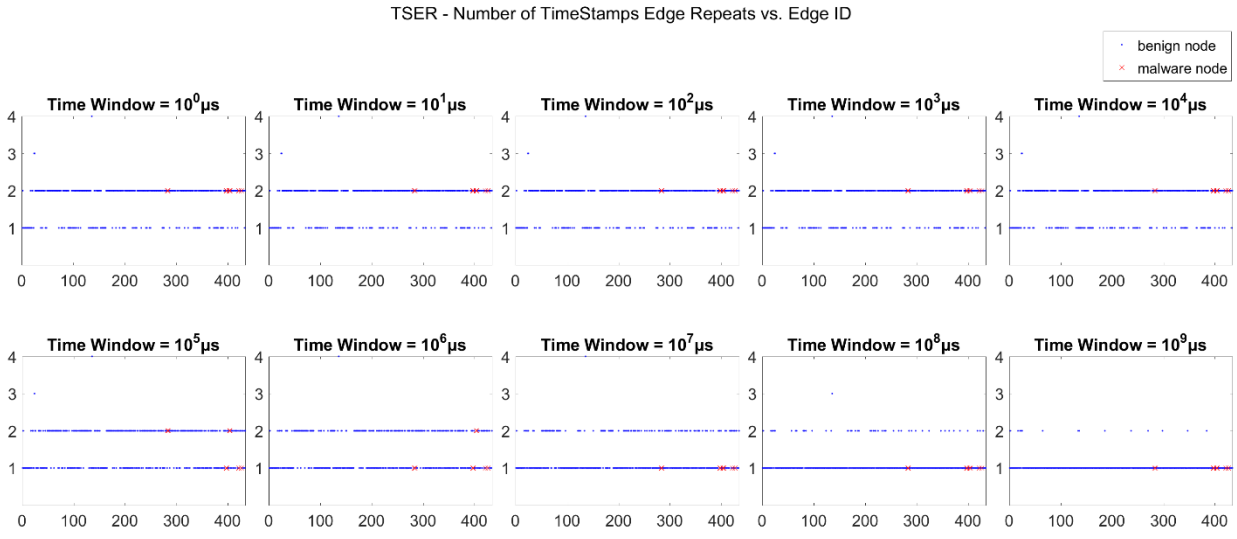

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Zurgop Malware - Instance 2

5) TSNE



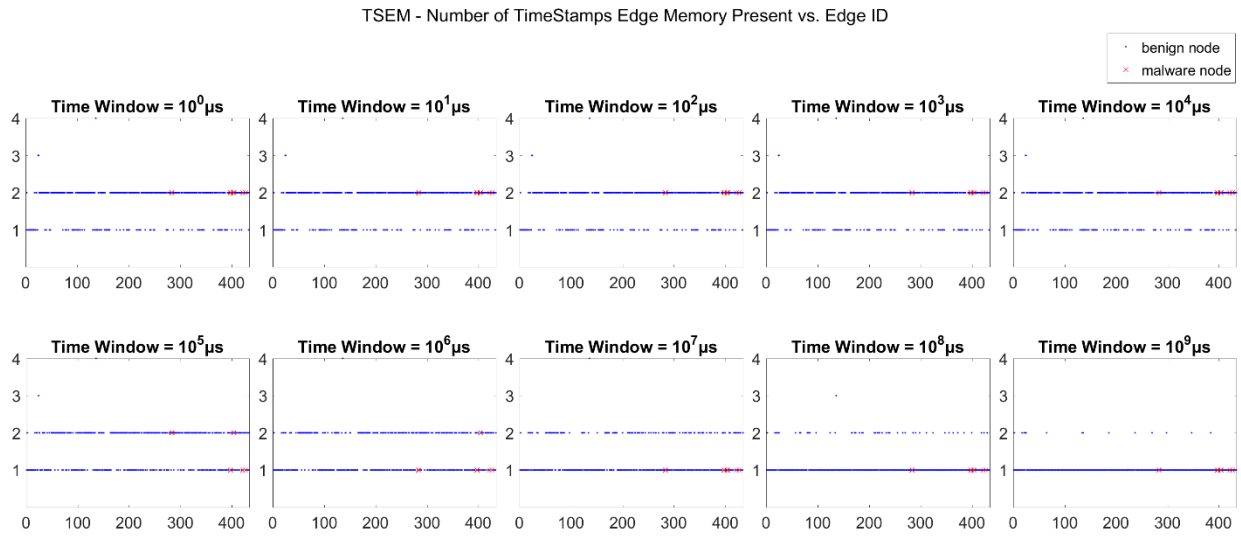
Zurgop Malware - Instance 2

6) TSER



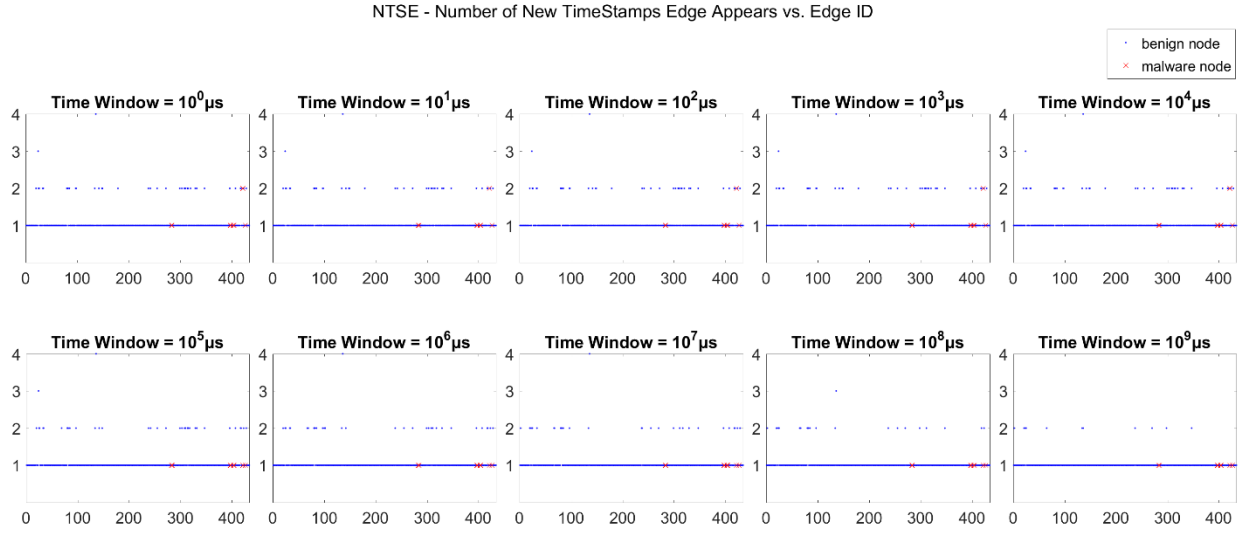
Zurgop Malware - Instance 2

7) TSEM



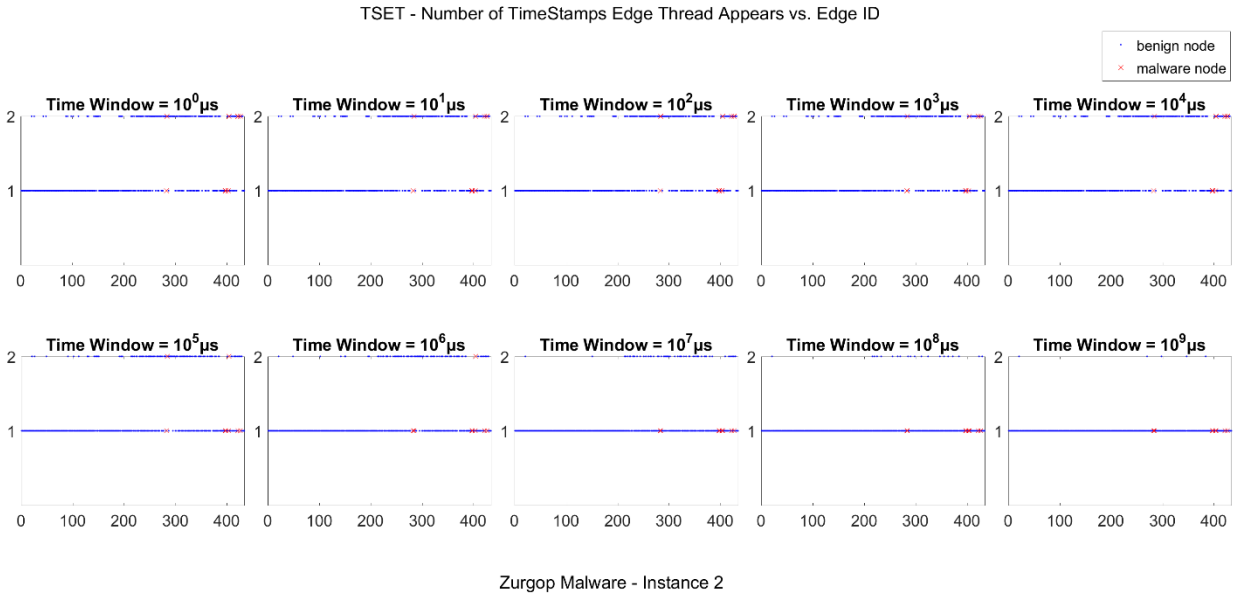
Zurgop Malware - Instance 2

8) NTSE



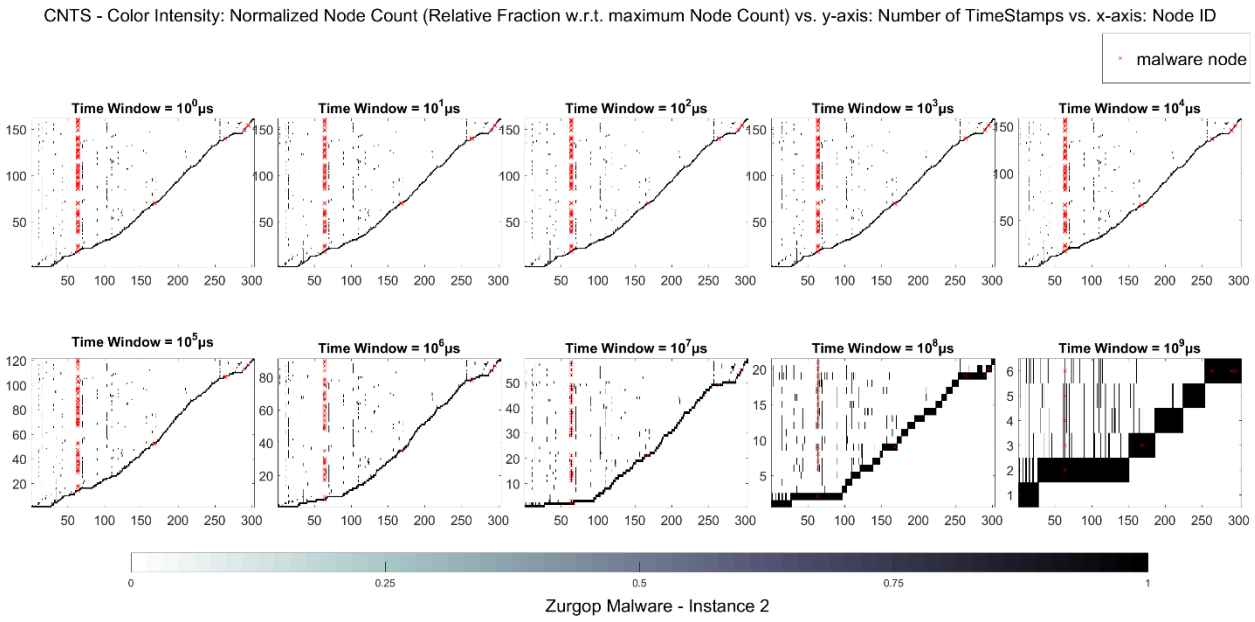
Zurgop Malware - Instance 2

9) TSET

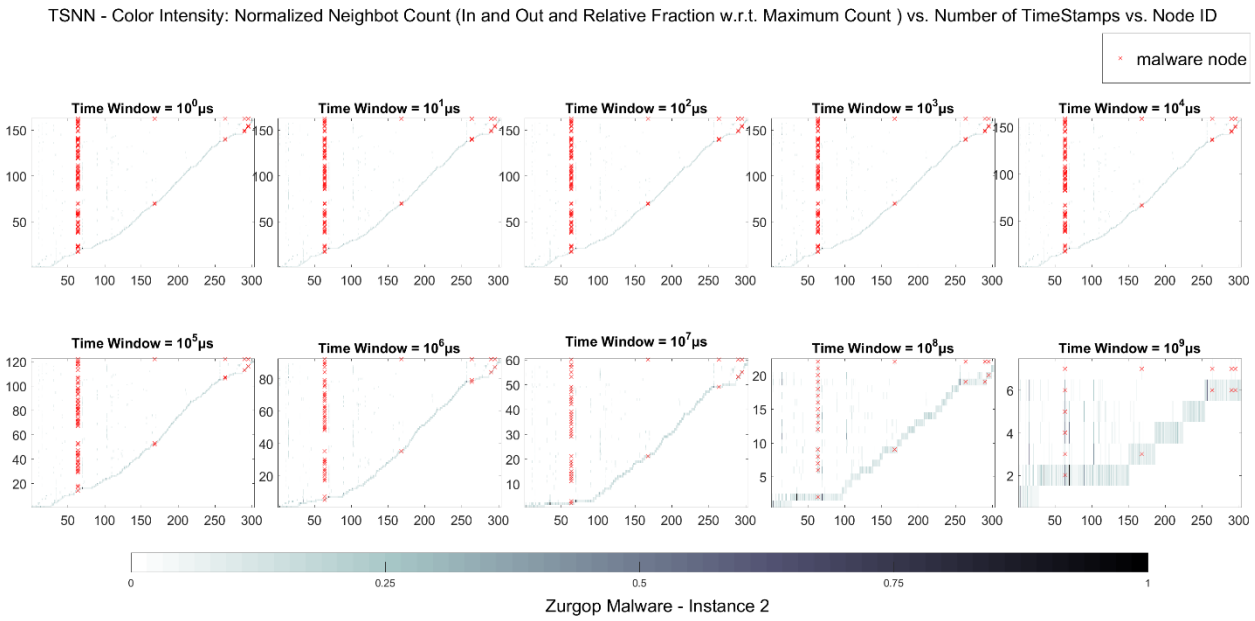


Time Graph Node Based Features

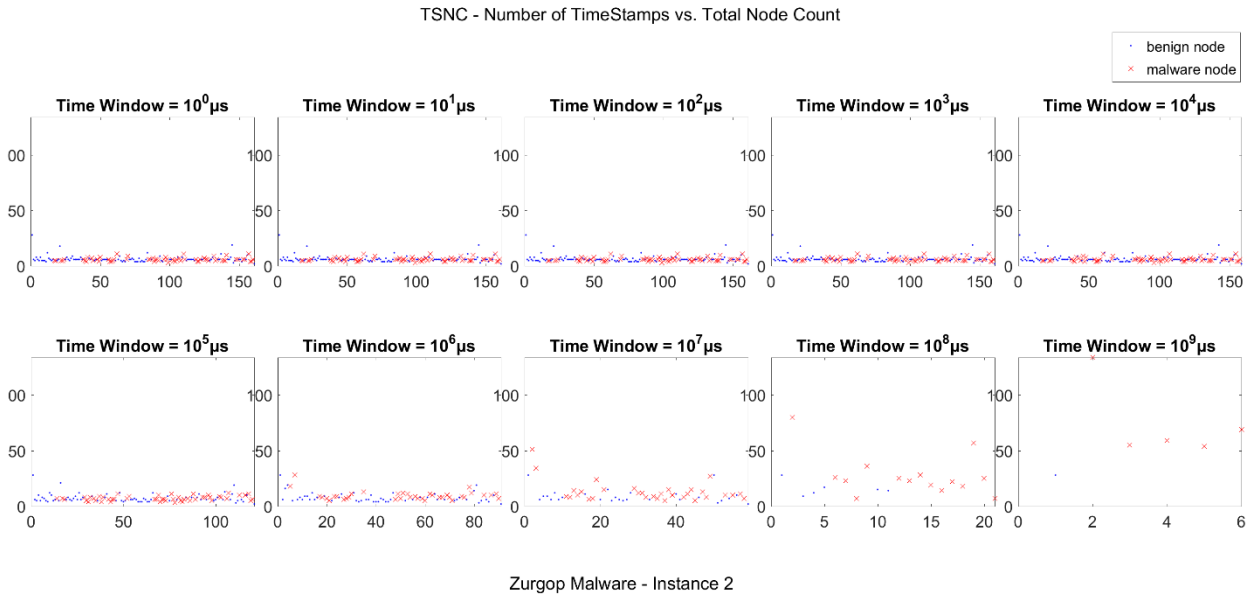
10) CNTS



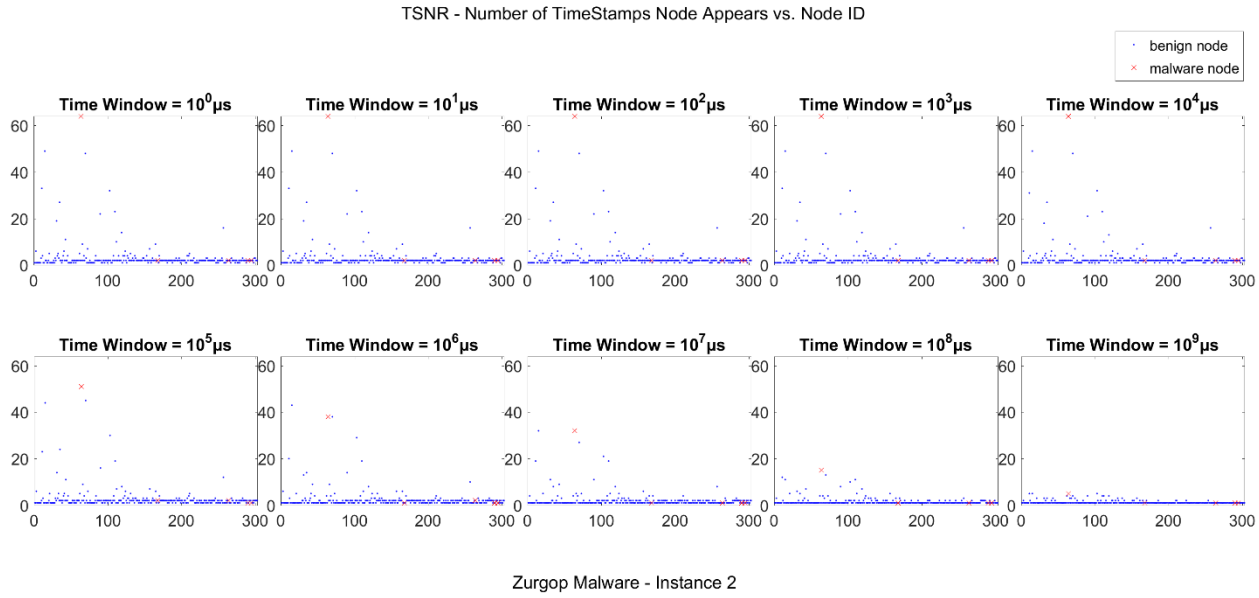
11) TSNN



12) TSNC



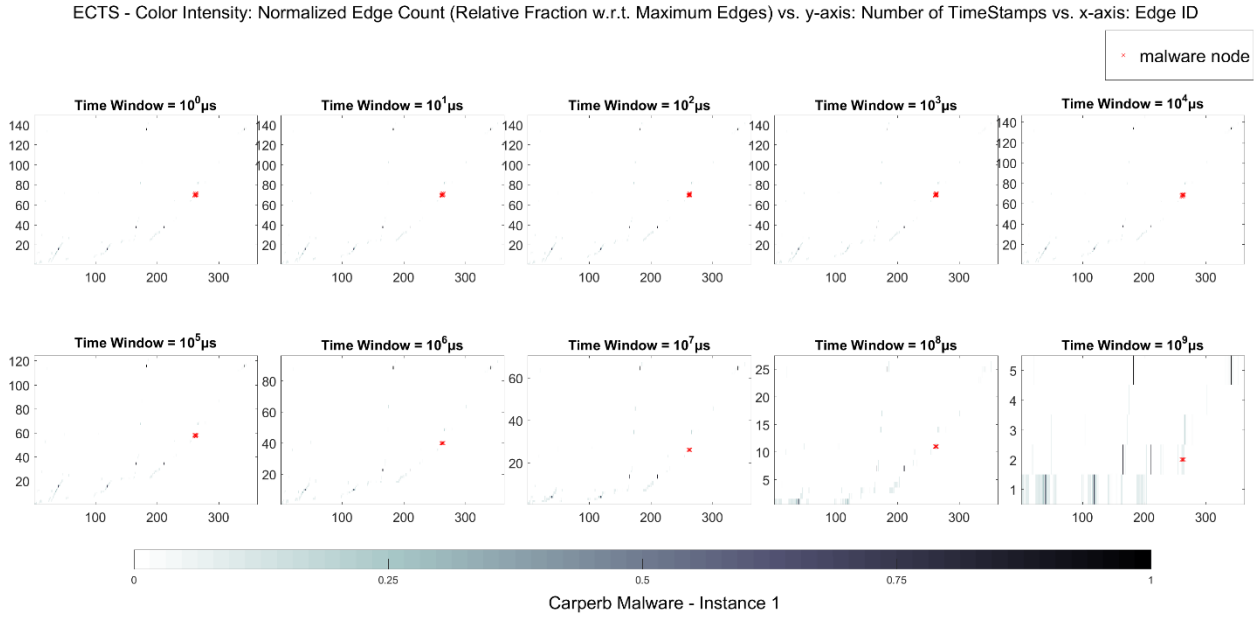
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
20
40
60
0
100
200
300
Zurgop Malware - Instance 2

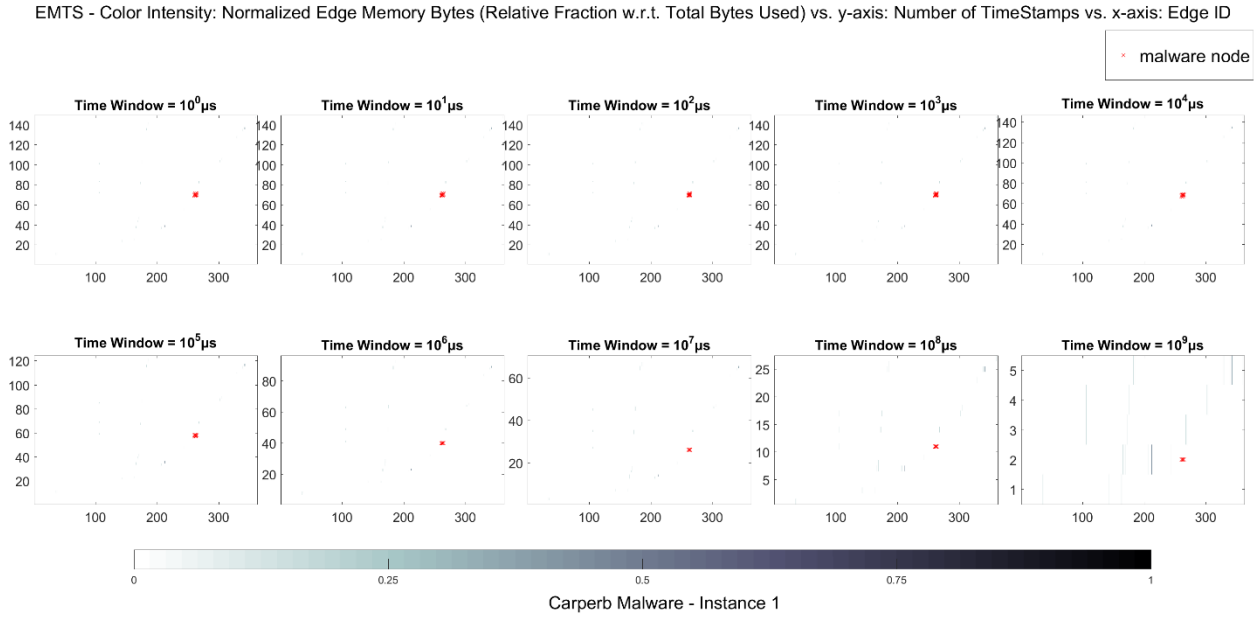
7.1.9 Carperb Malware – Instance 1

Time Graph Edge Based Features

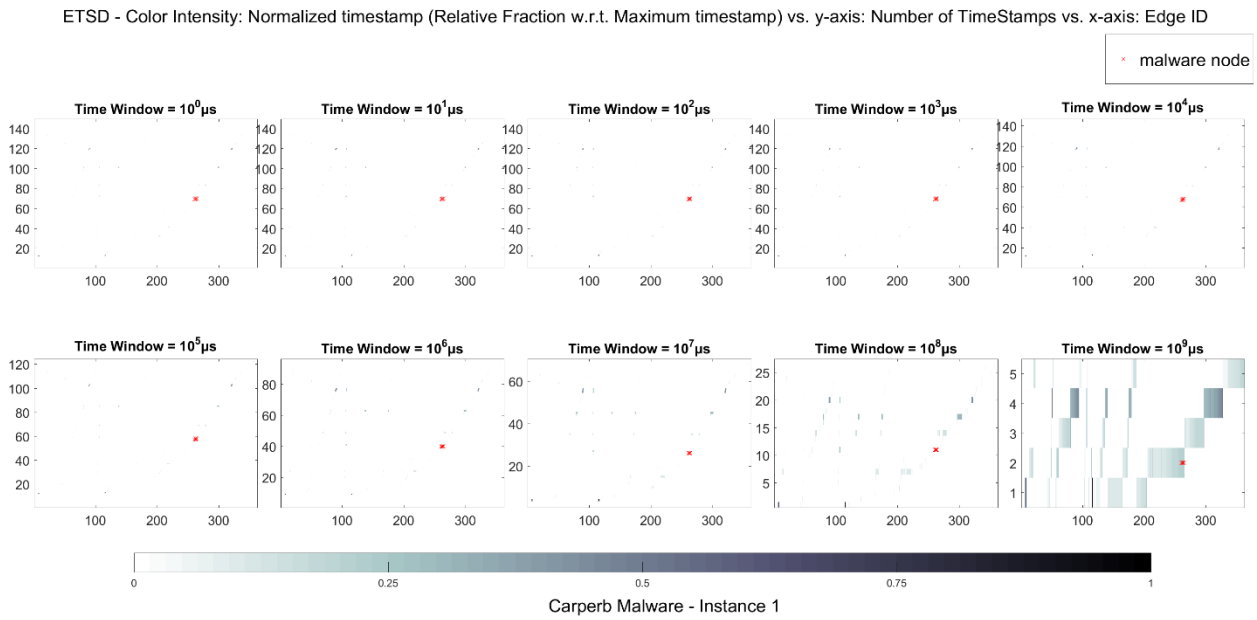
1) ECTS



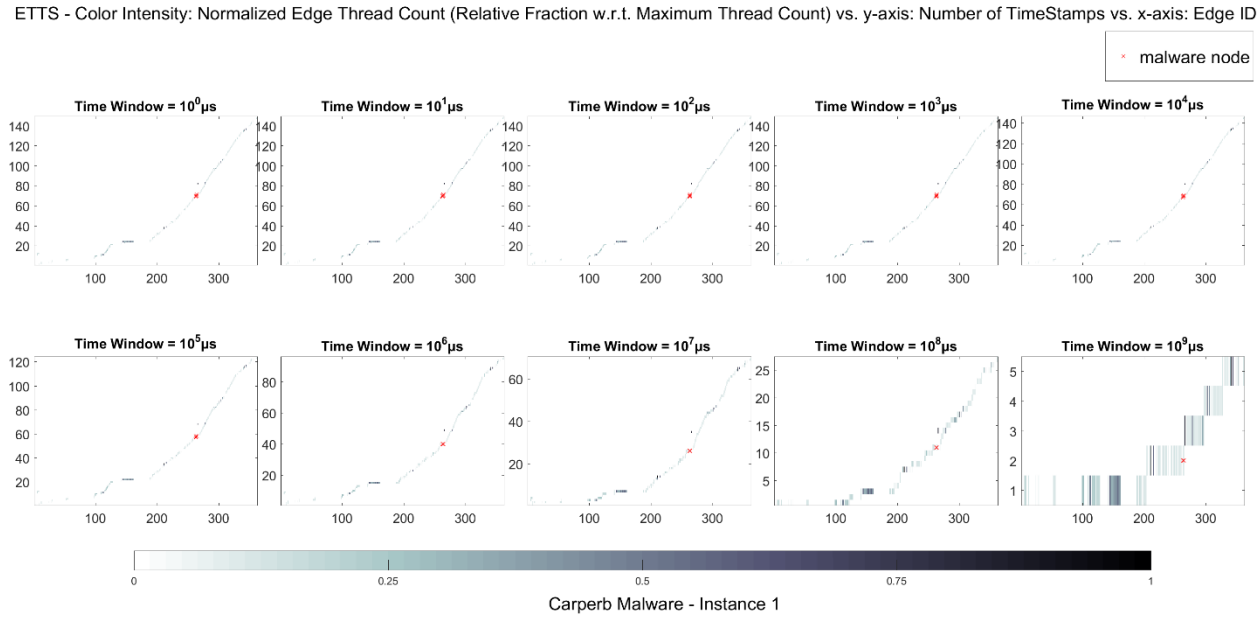
2) EMTS



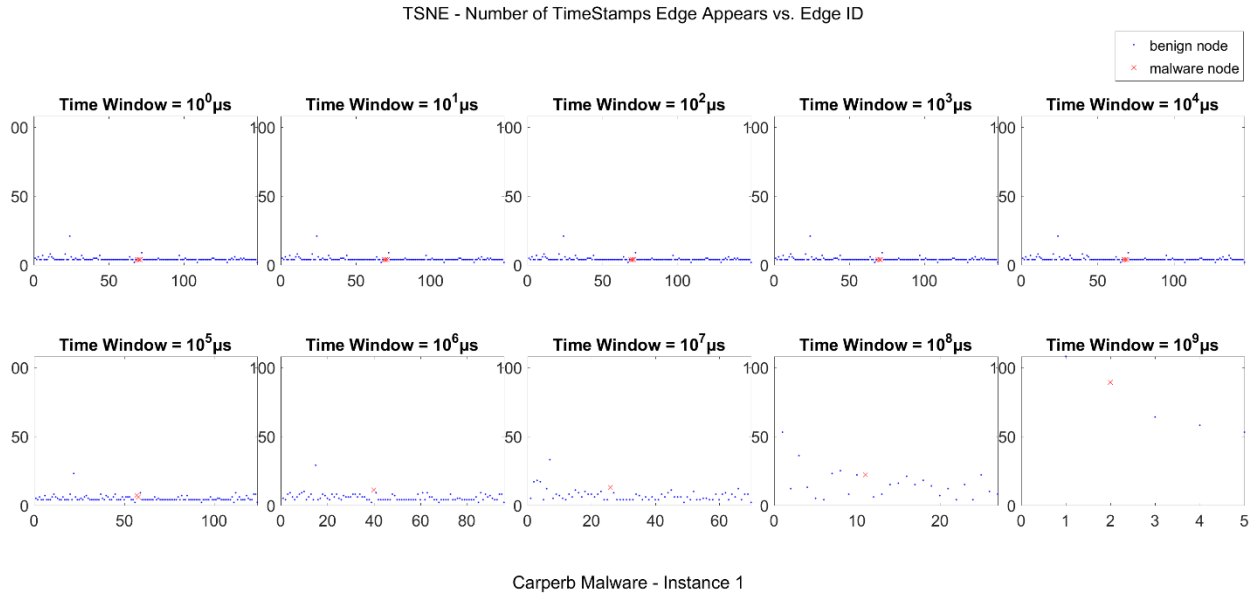
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Carperb Malware - Instance 1

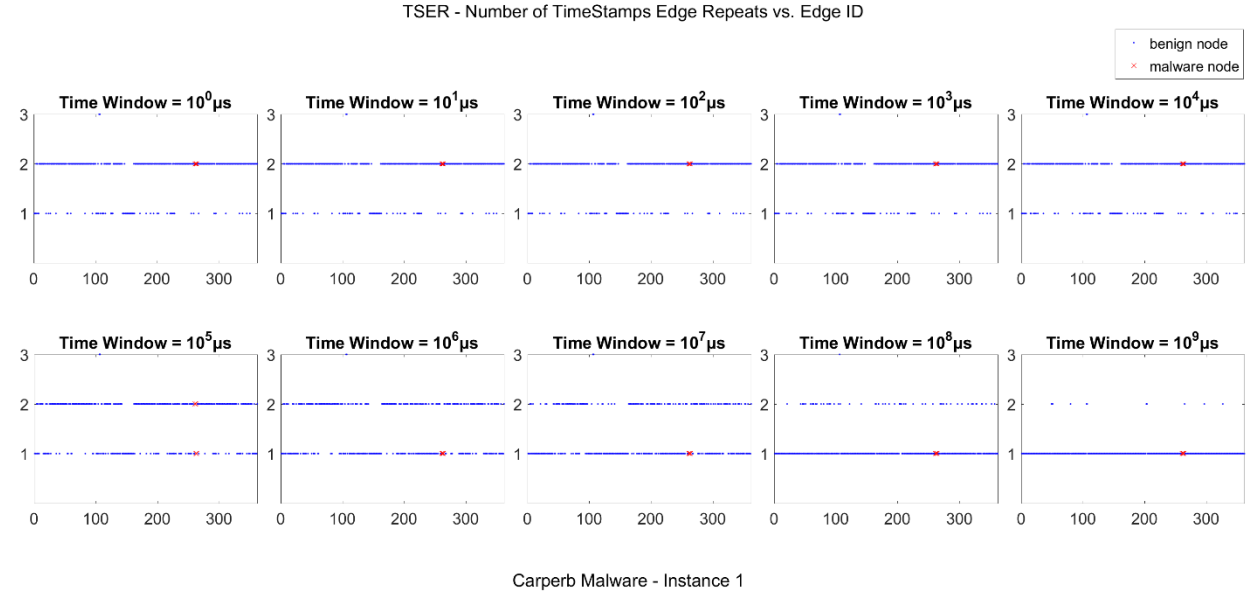
4) ETTS


ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Carperb Malware - Instance 1

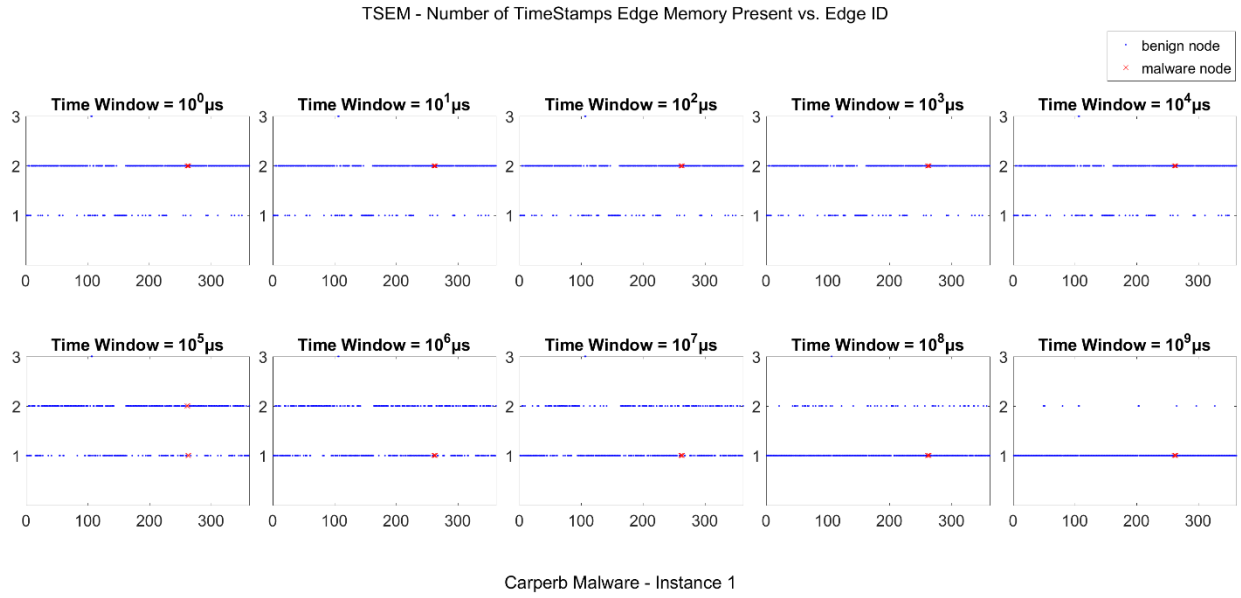
5) TSNE


TSNE - Number of TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Carperb Malware - Instance 1

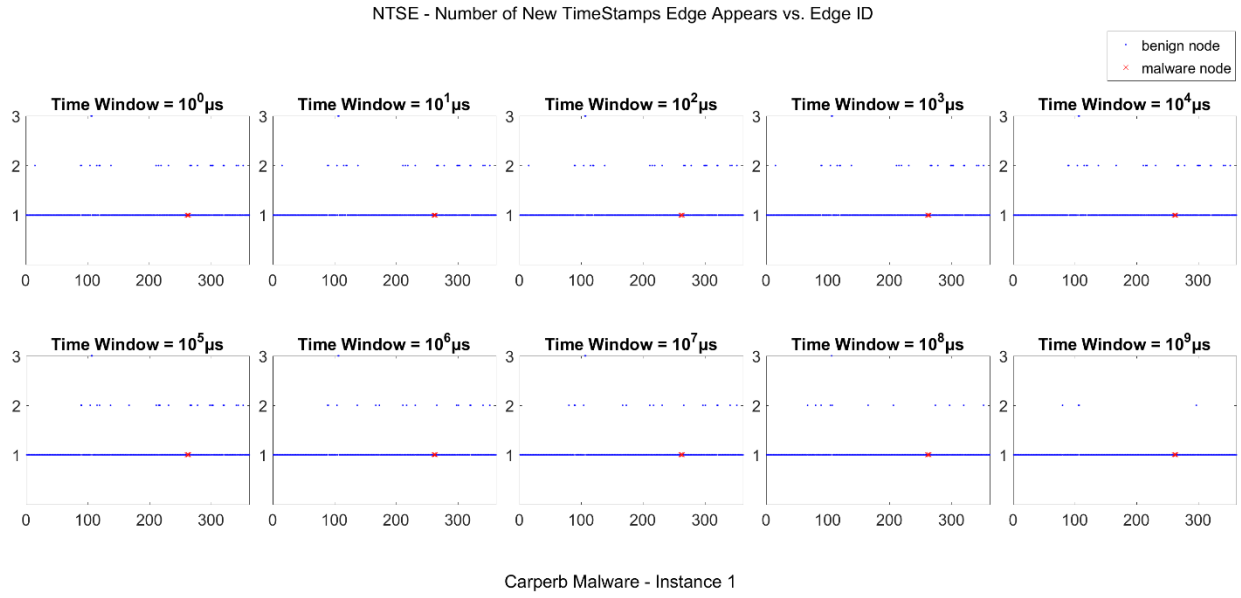
6) TSER


TSER - Number of TimeStamps Edge Repeats vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Carperb Malware - Instance 1

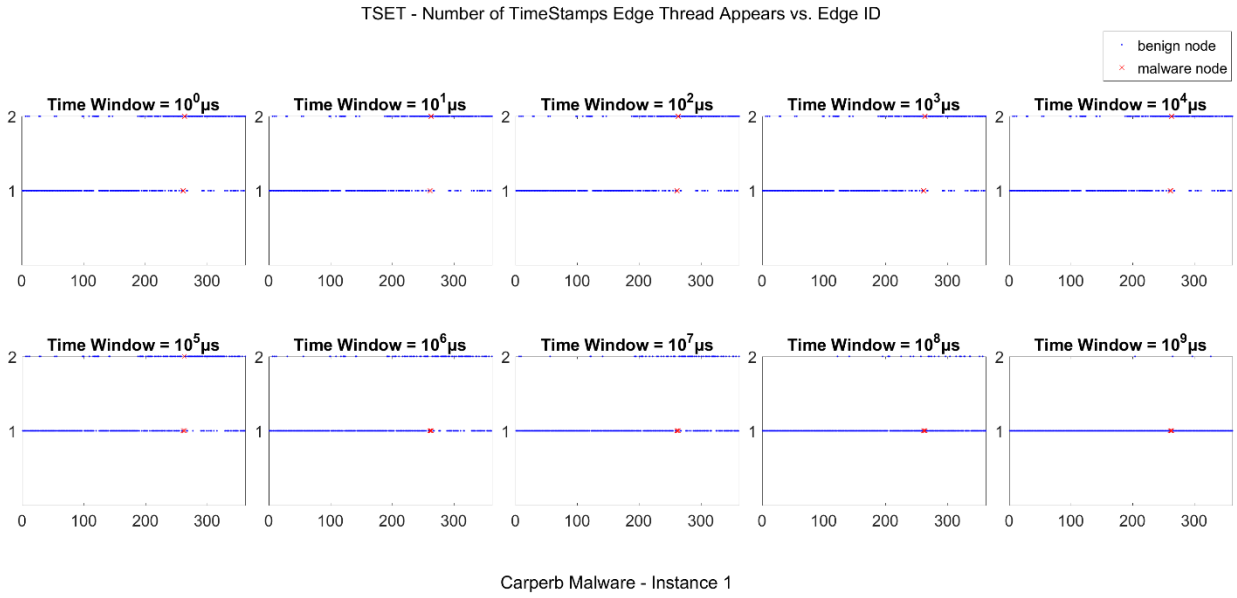
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Carperb Malware - Instance 1

8) NTSE

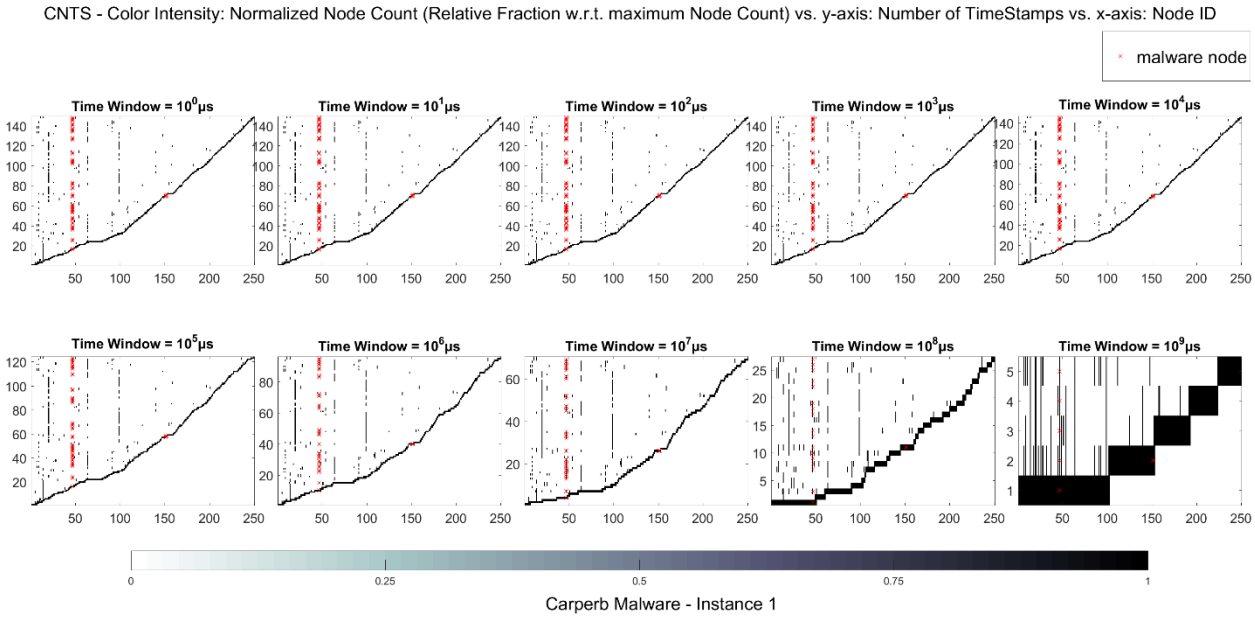

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Carperb Malware - Instance 1

9) TSET

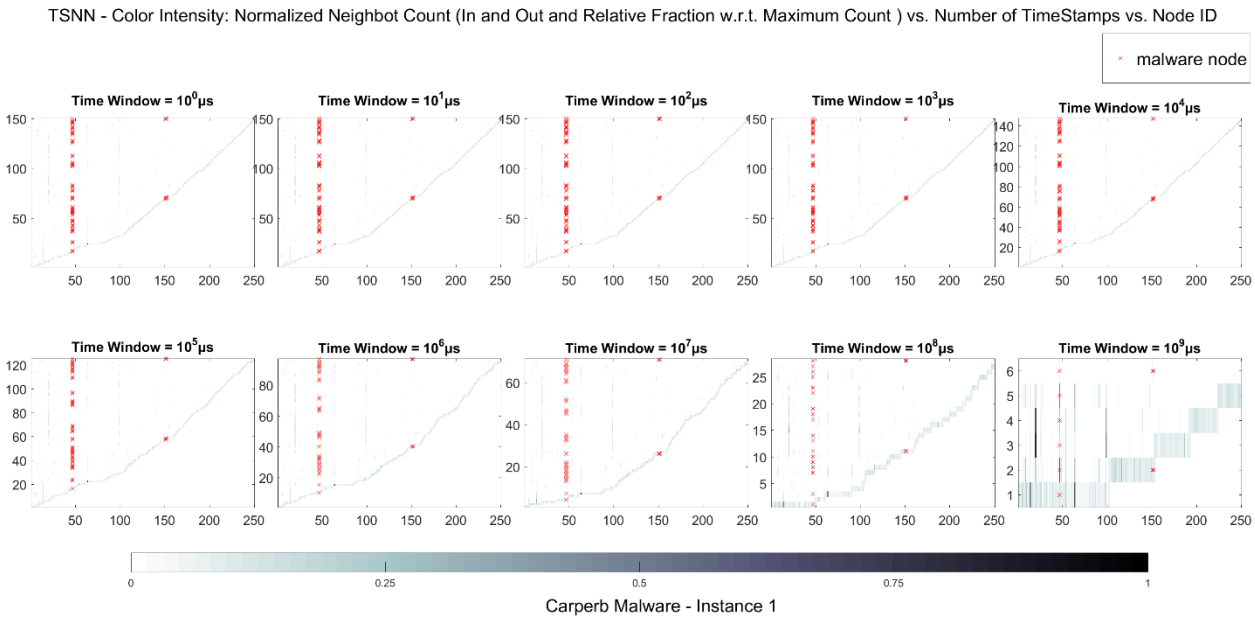


Time Graph Node Based Features

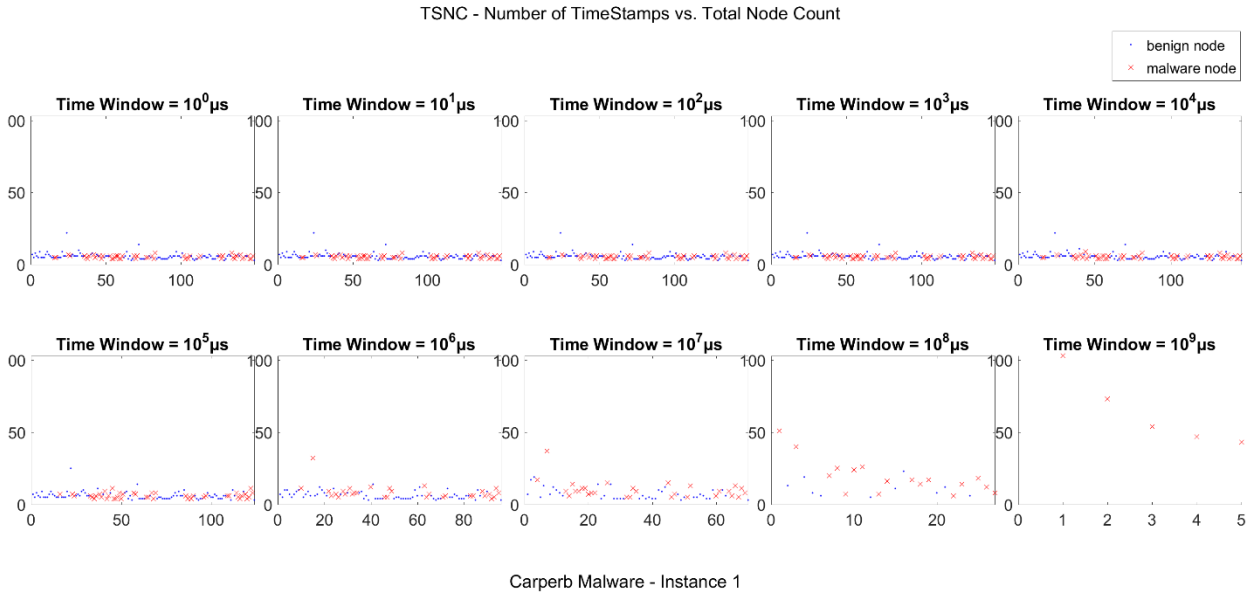
10) CNTS



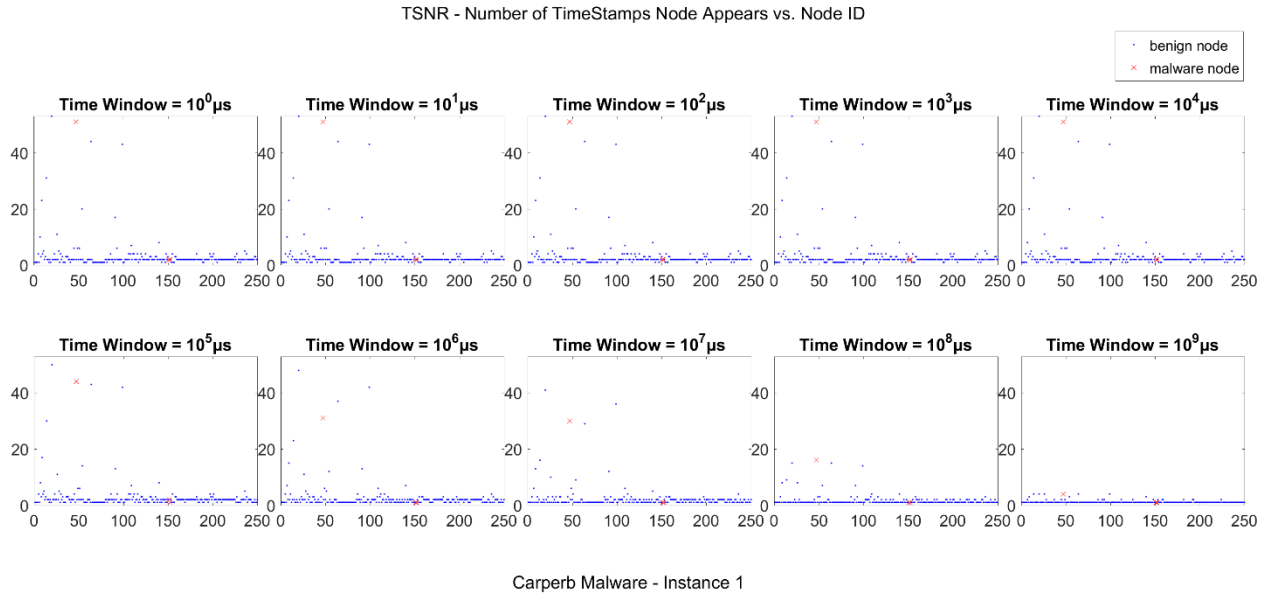
11) TSNN



12) TSNC



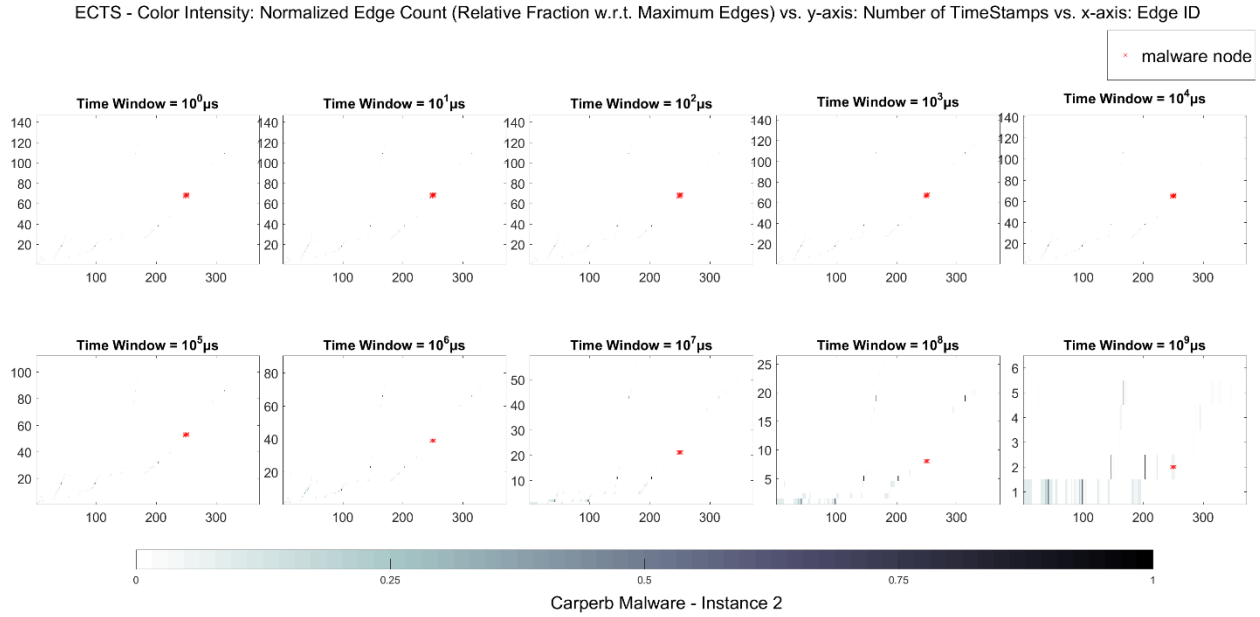
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Carperb Malware - Instance 1

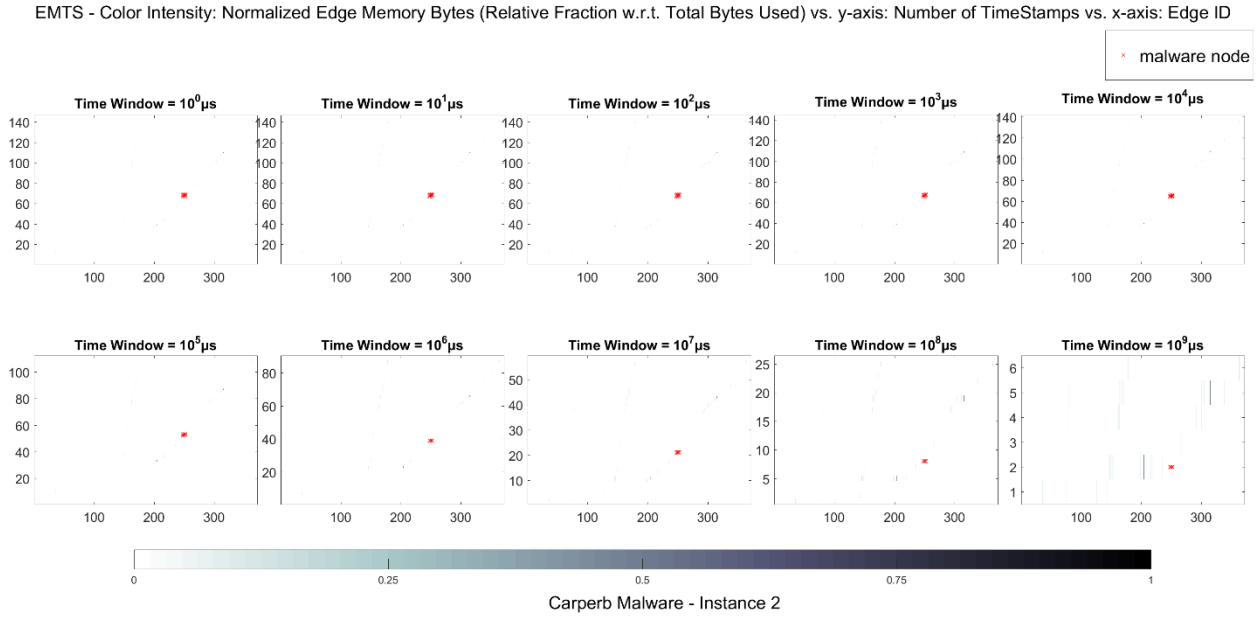
7.1.10 Carperb Malware – Instance 2

Time Graph Edge Based Features

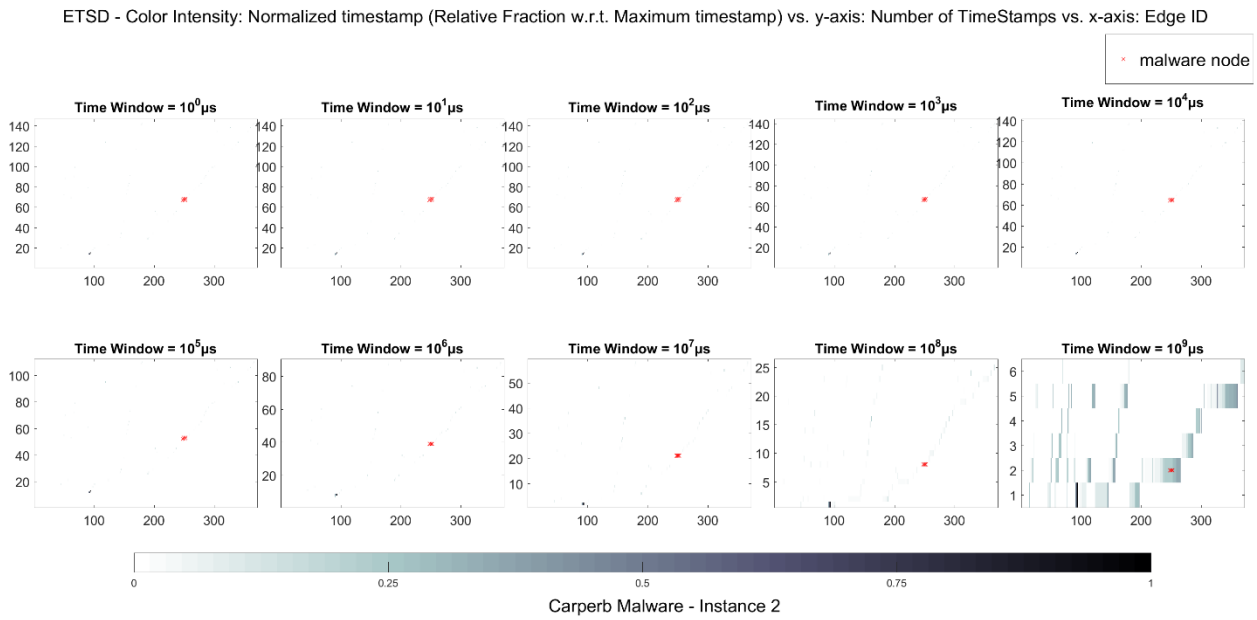
1) ECTS



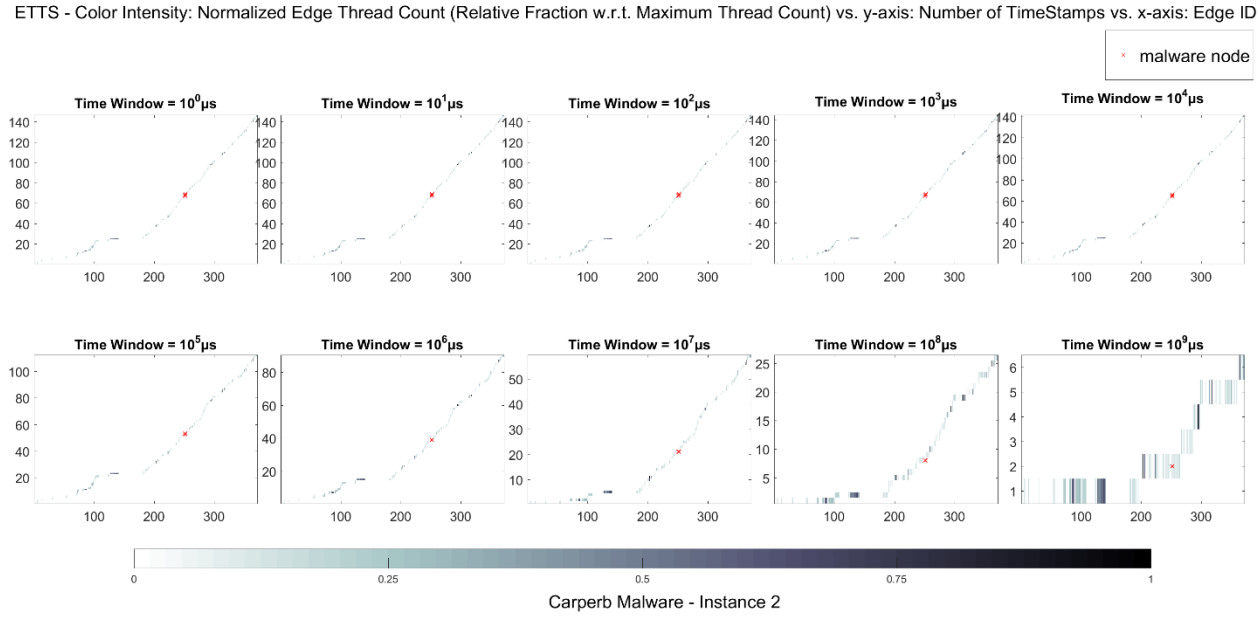
2) EMTS



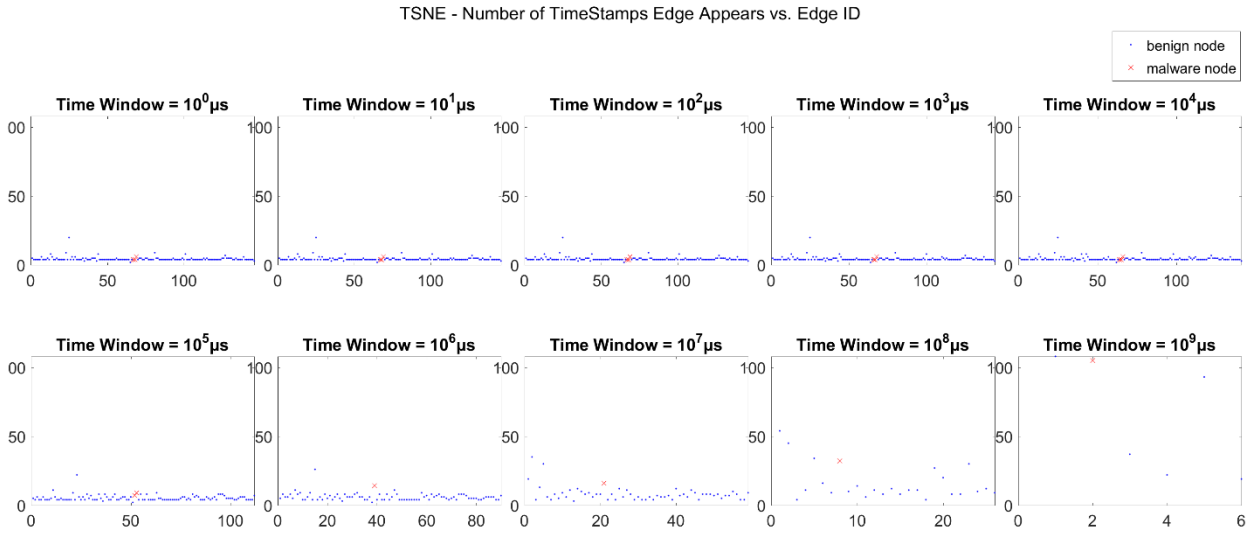
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Carperb Malware - Instance 2

4) ETTS

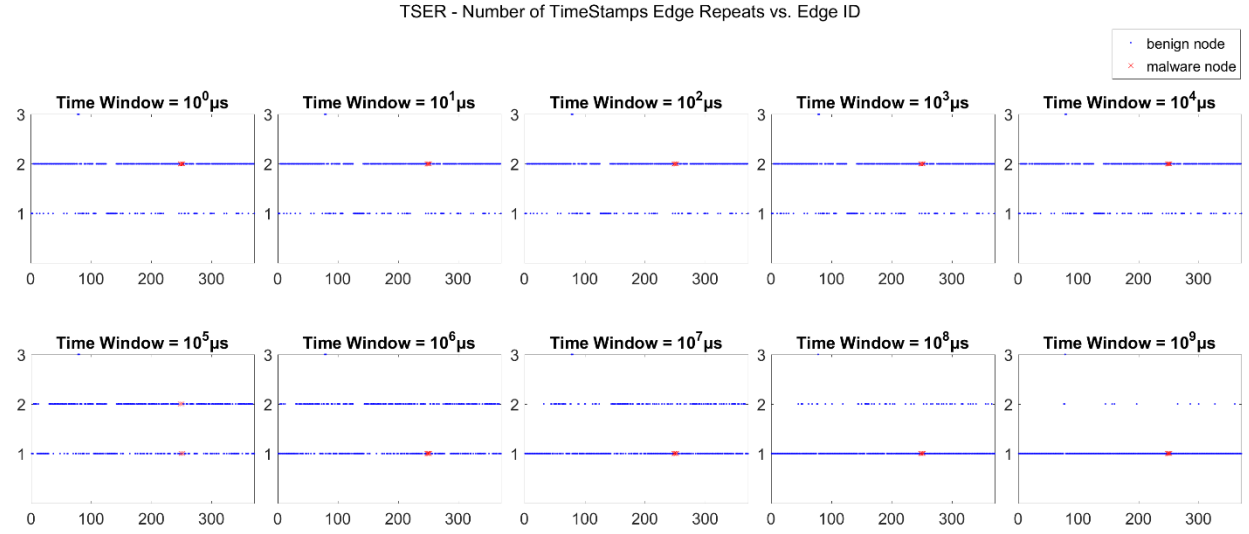

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Carperb Malware - Instance 2

5) TSNE



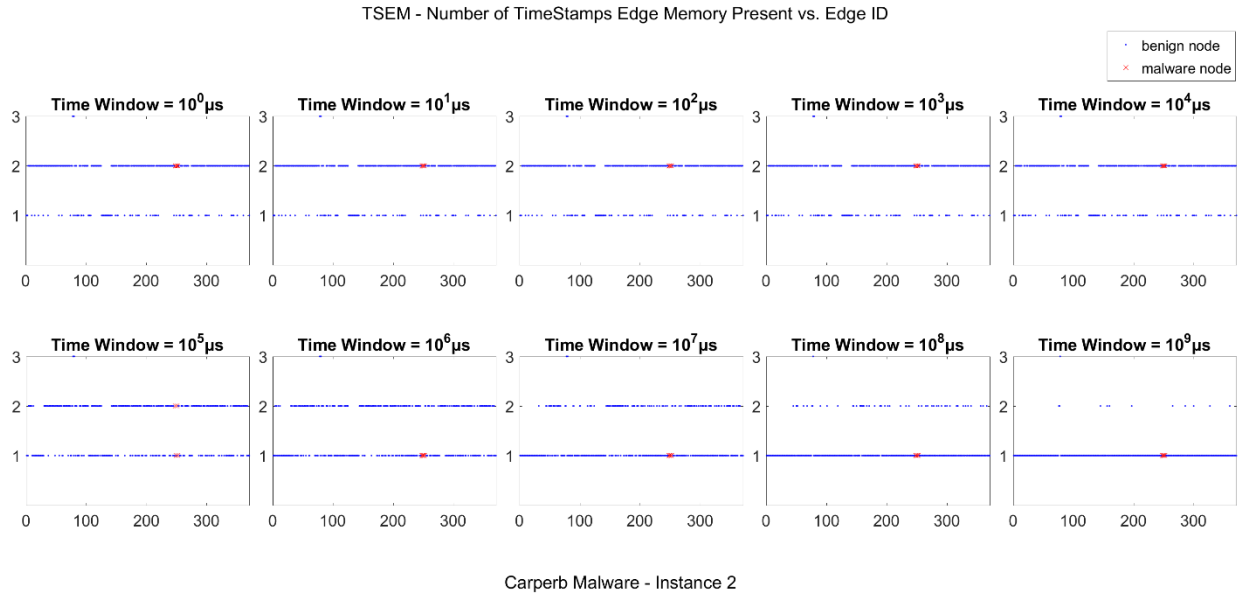
Carperb Malware - Instance 2

6) TSER

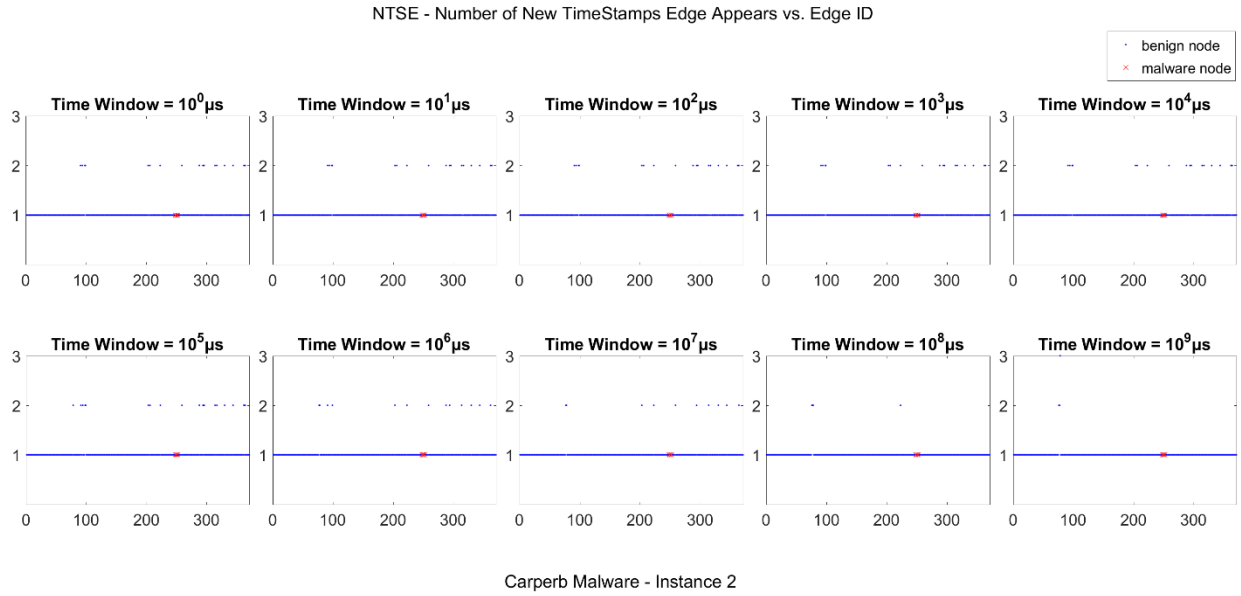


Carperb Malware - Instance 2

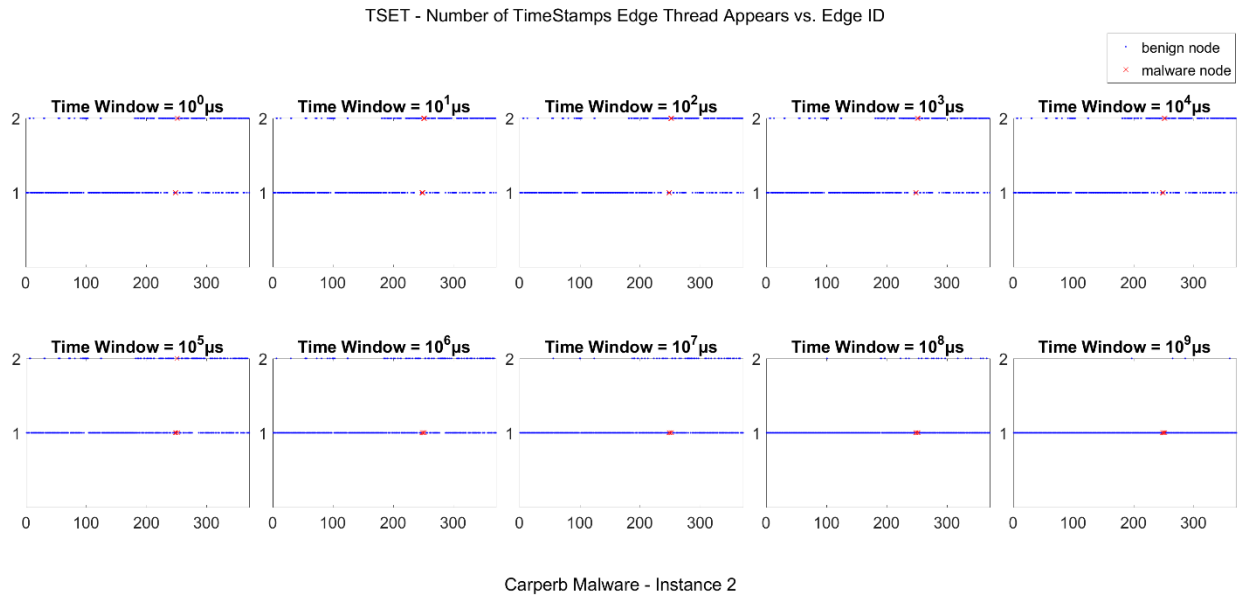
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Carperb Malware - Instance 2

8) NTSE

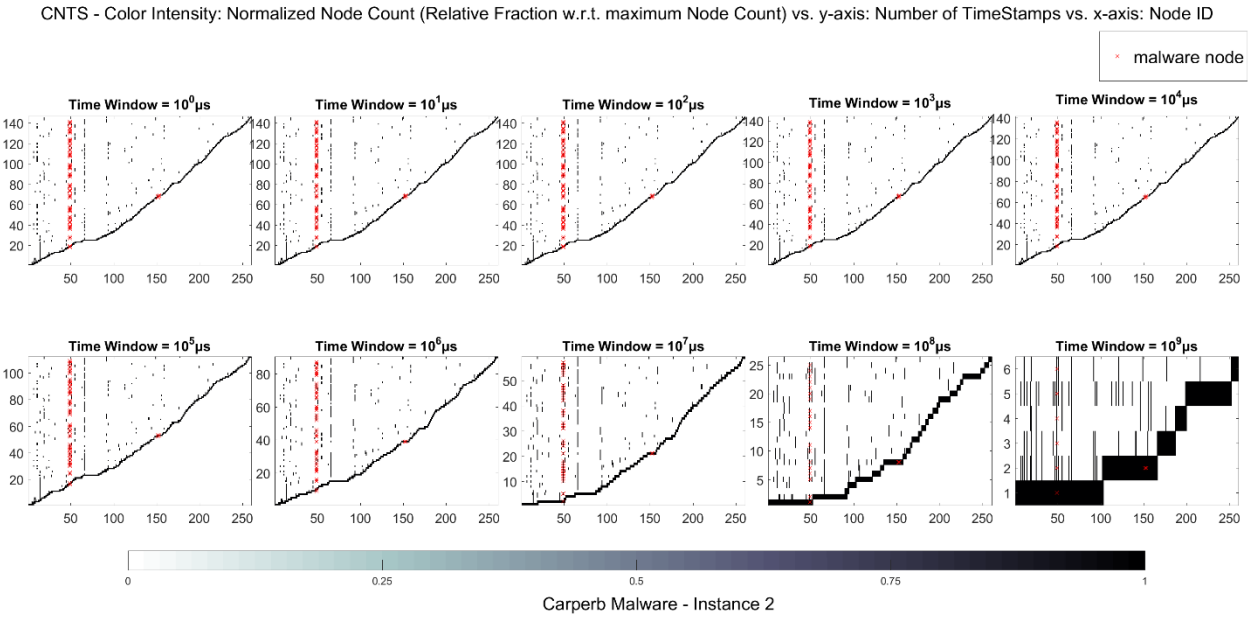

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Carperb Malware - Instance 2

9) TSET

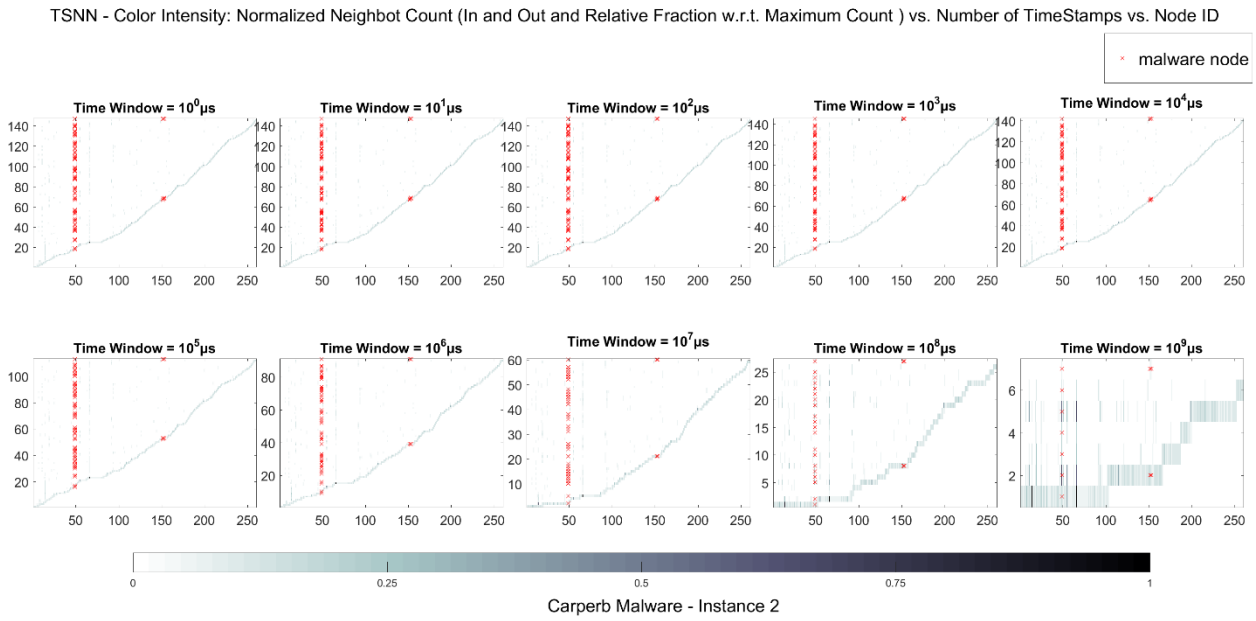


Time Graph Node Based Features

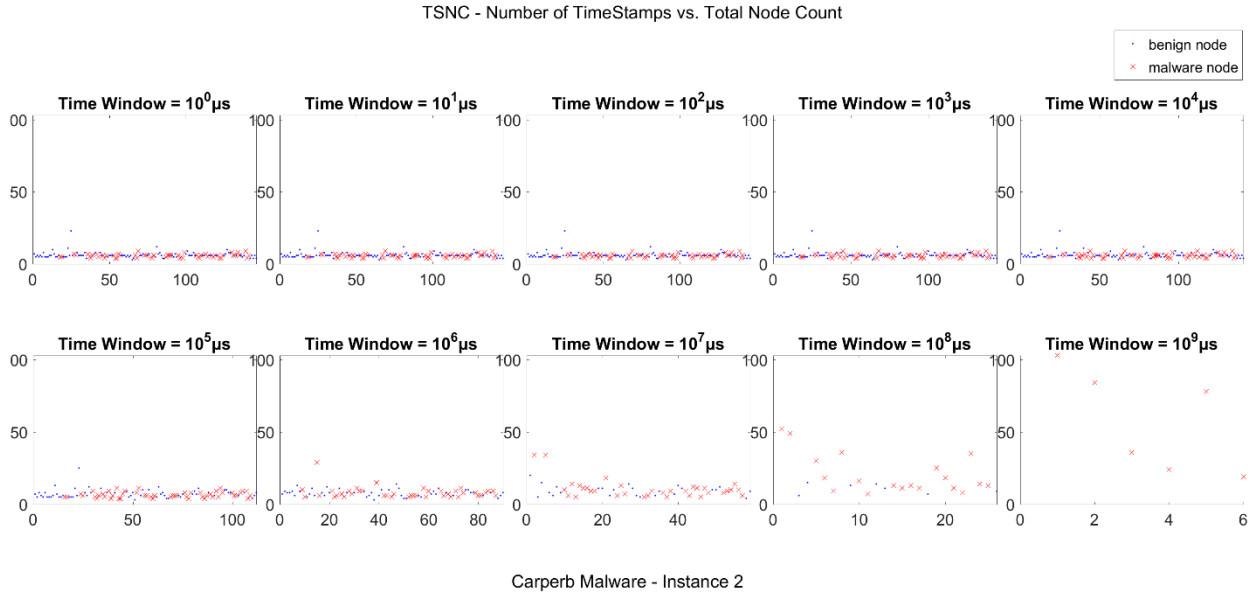
10) CNTS



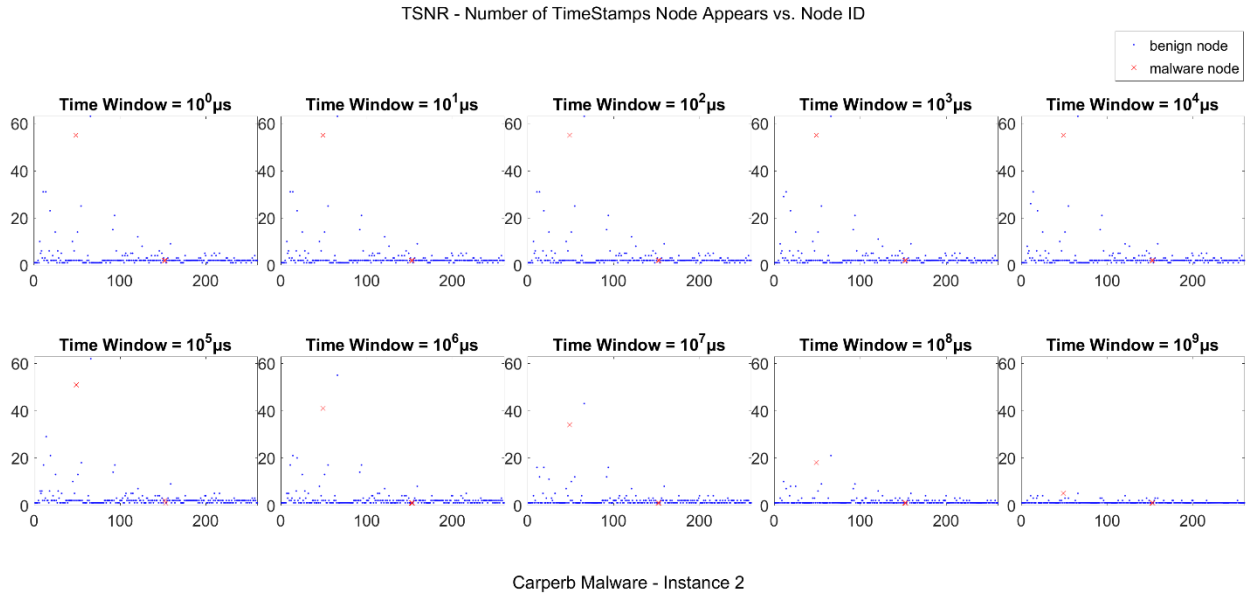
11) TSNN



12) TSNC



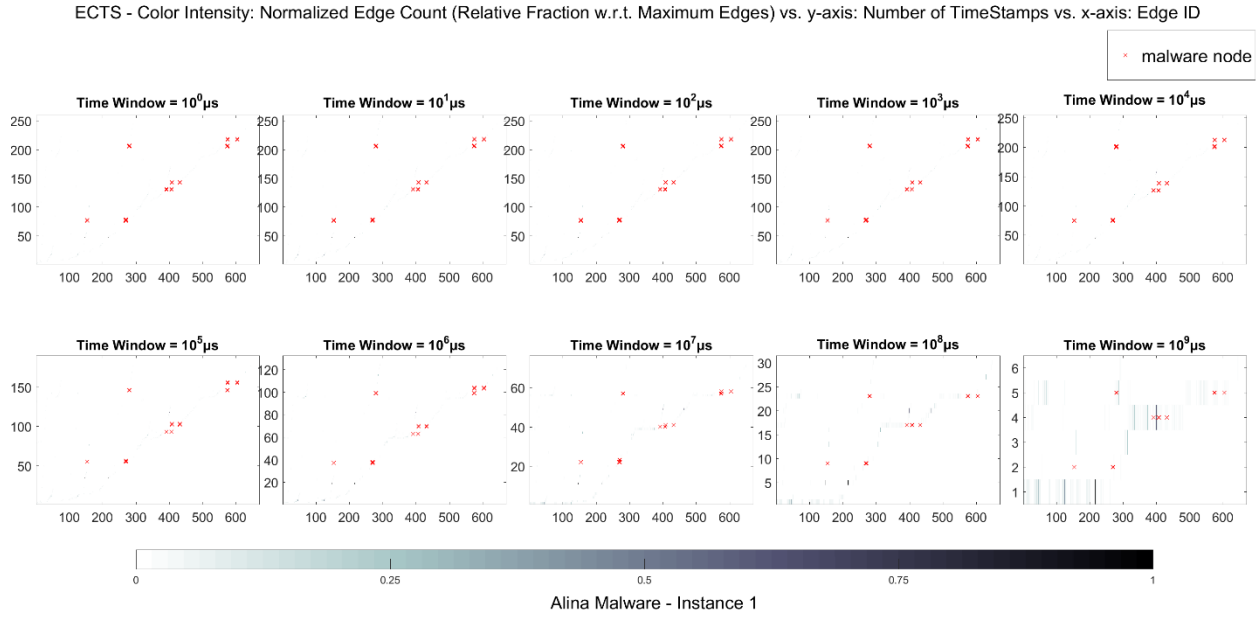
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Carperb Malware - Instance 2

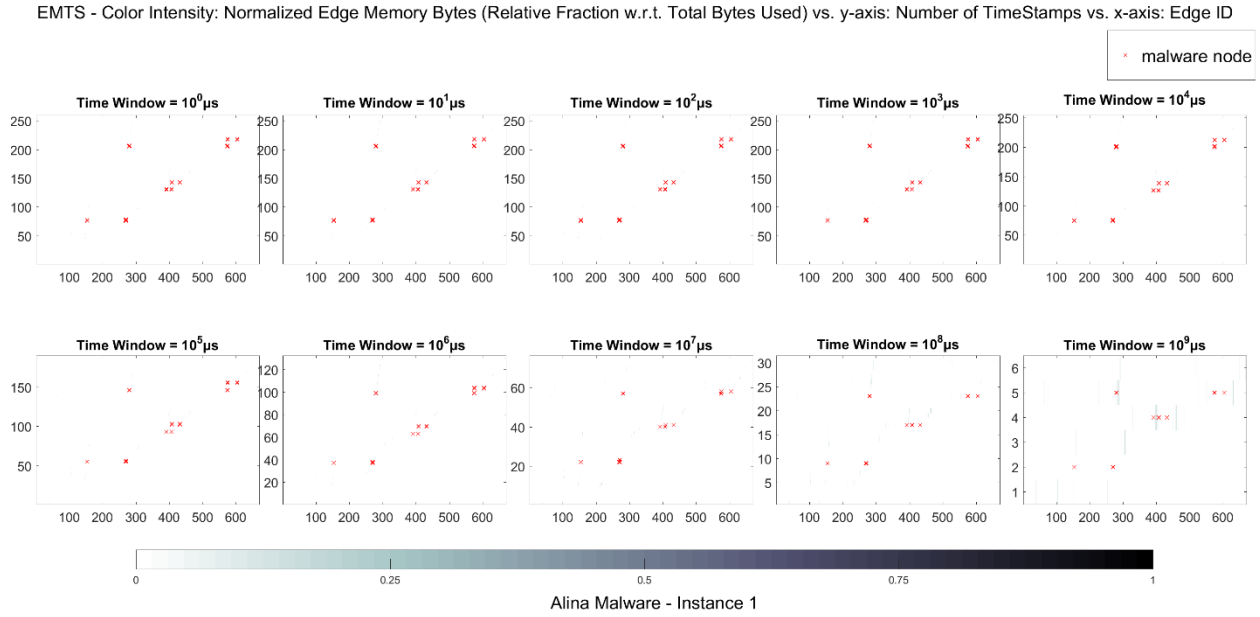
7.1.11 Alina Malware – Instance 1

Time Graph Edge Based Features

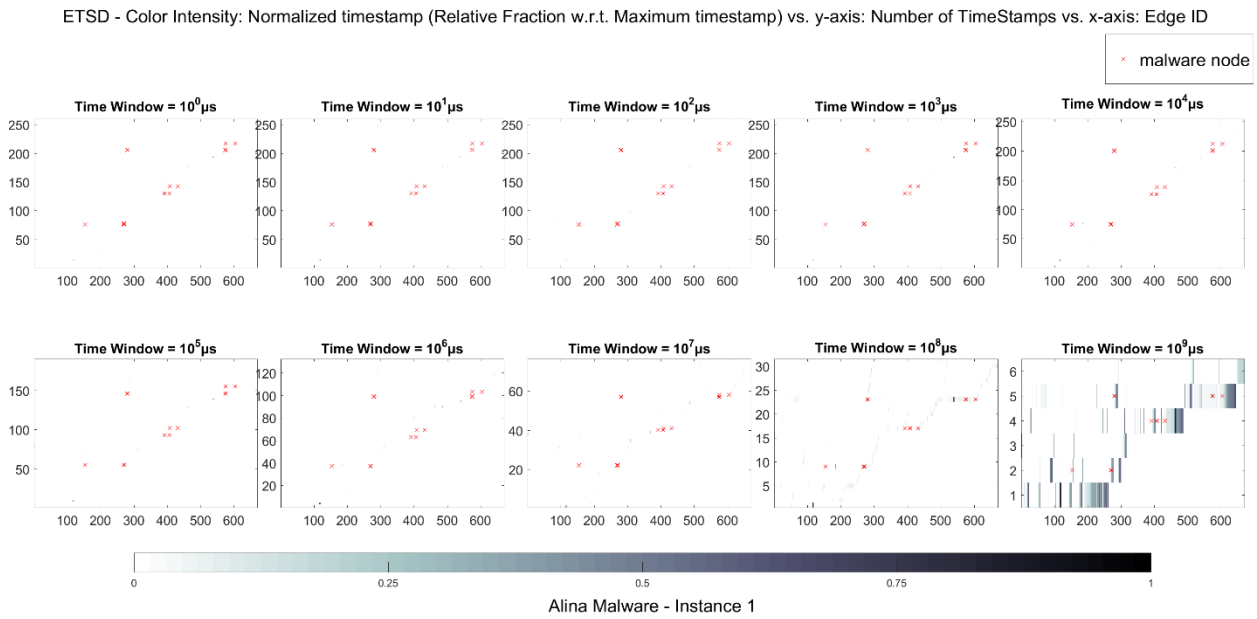
1) ECTS



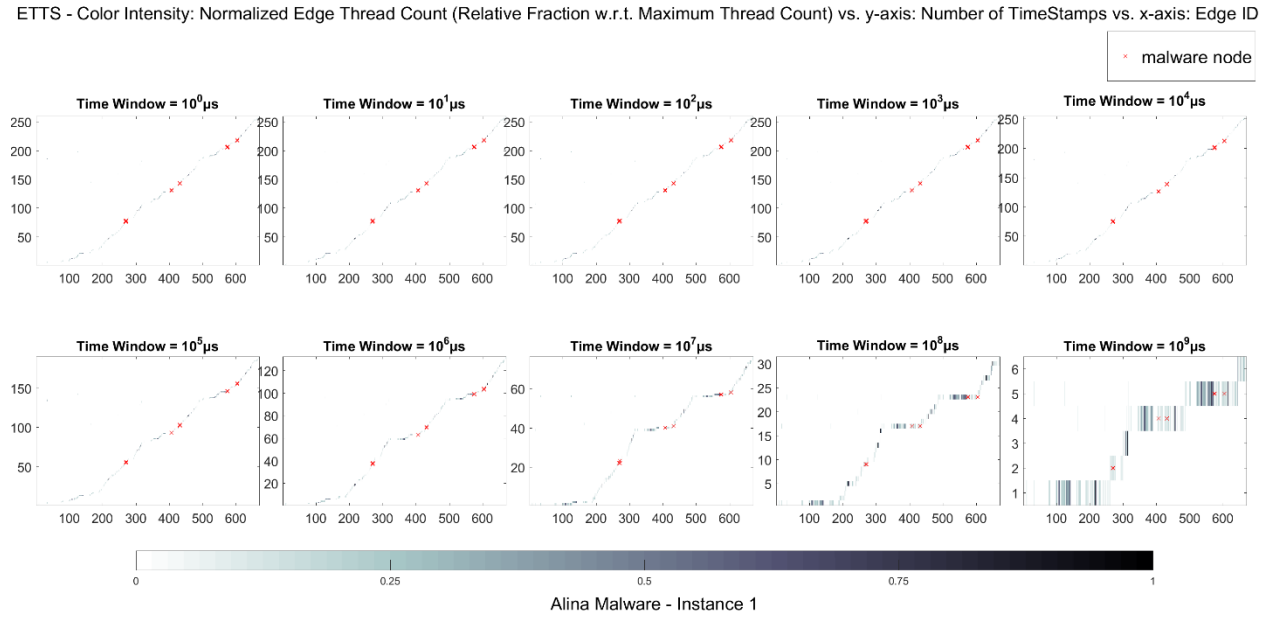
2) EMTS



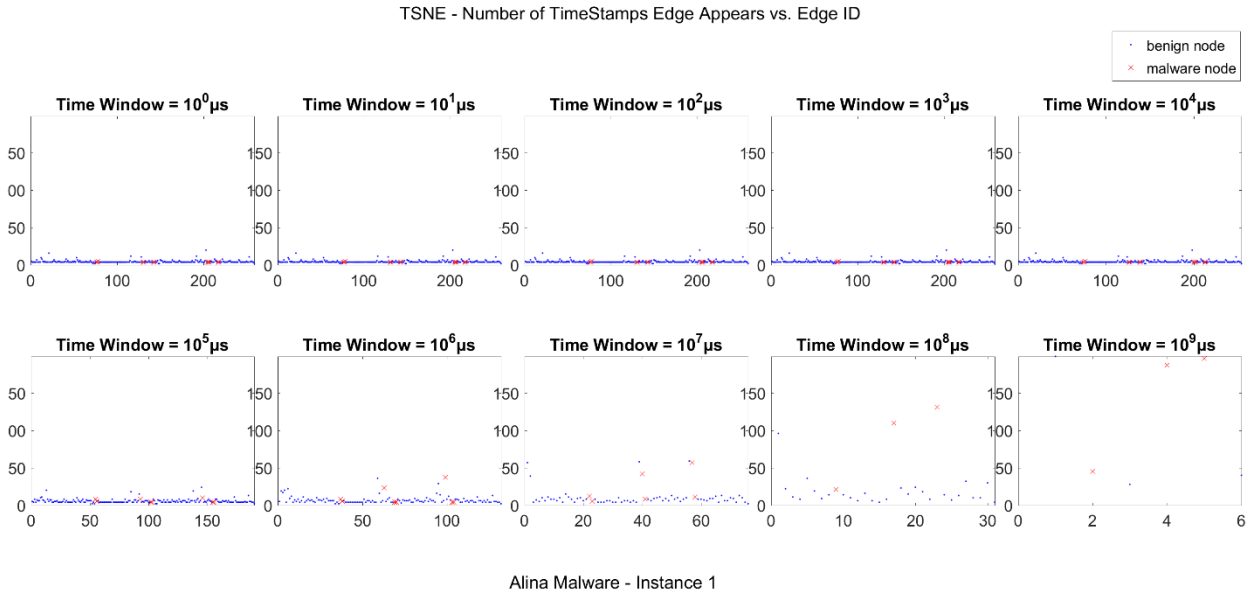
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Alina Malware - Instance 1

4) ETTS

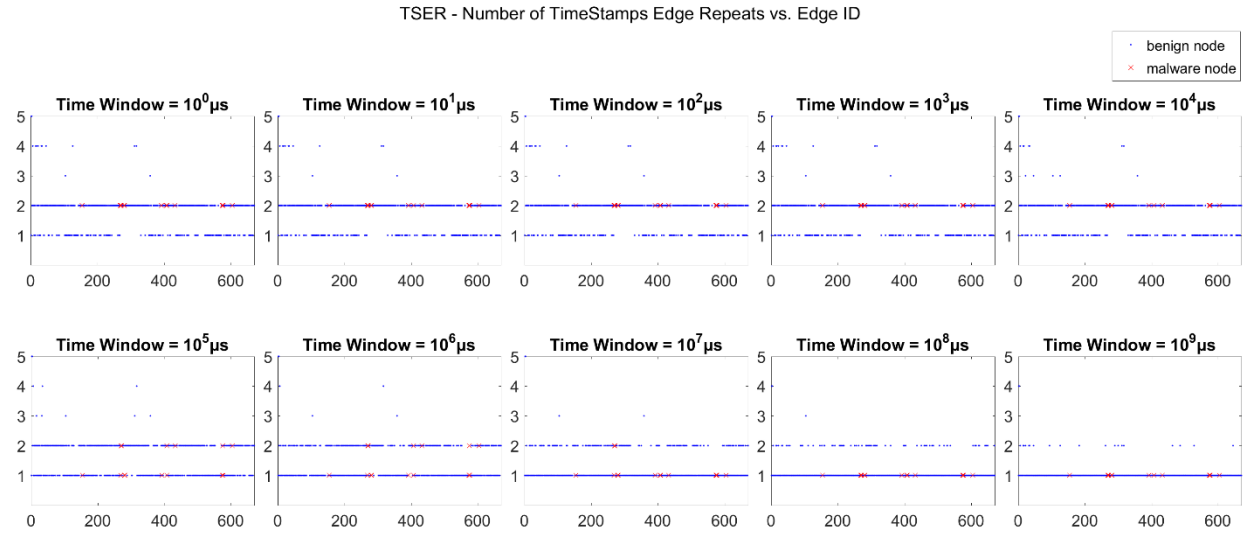

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Alina Malware - Instance 1

5) TSNE



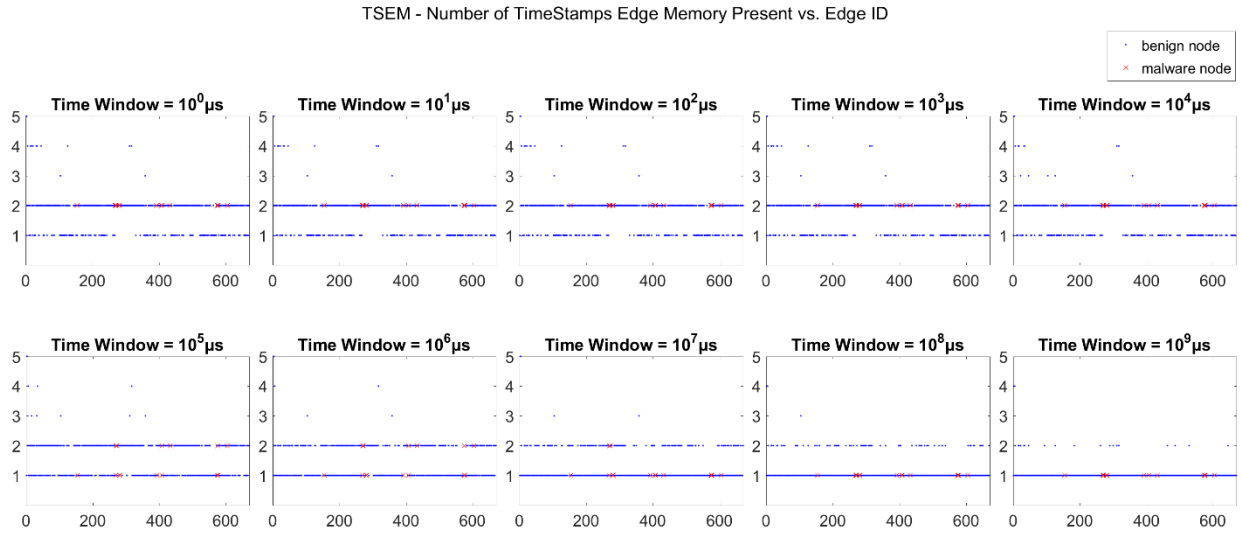
Alina Malware - Instance 1

6) TSER

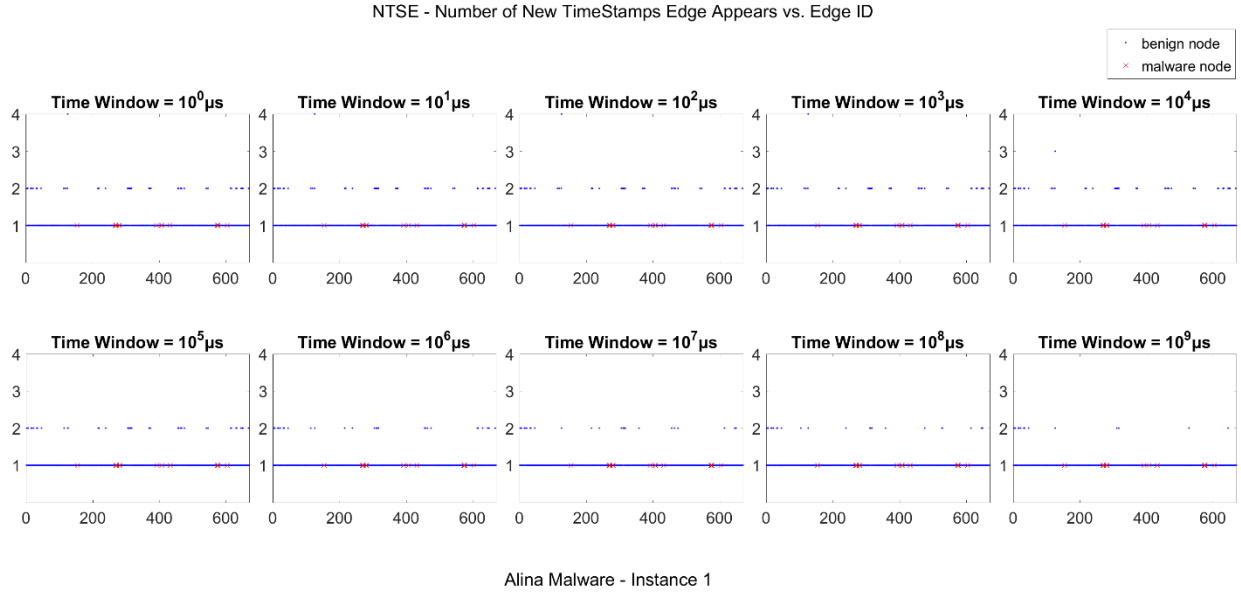


Alina Malware - Instance 1

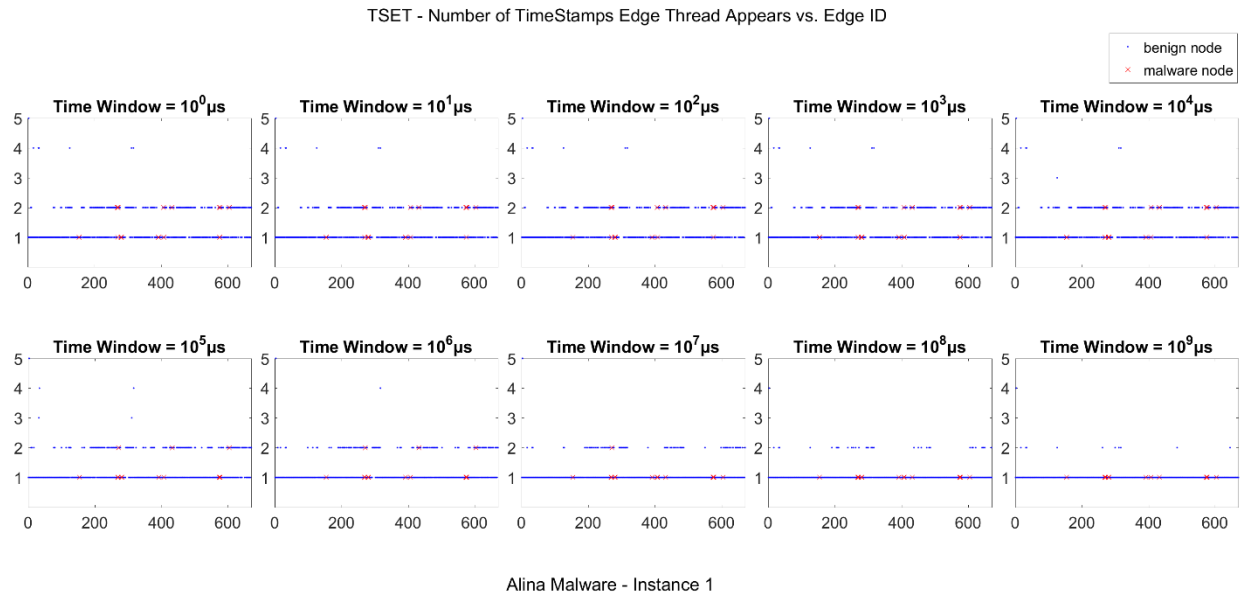
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Alina Malware - Instance 1

8) NTSE

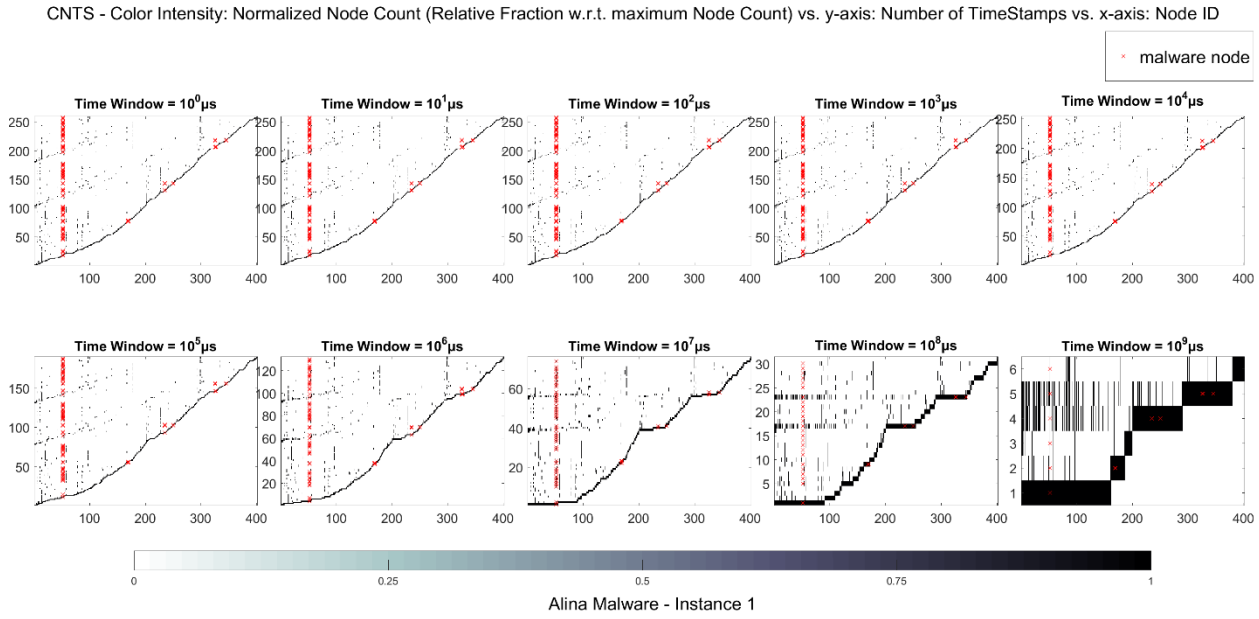

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Alina Malware - Instance 1

9) TSET

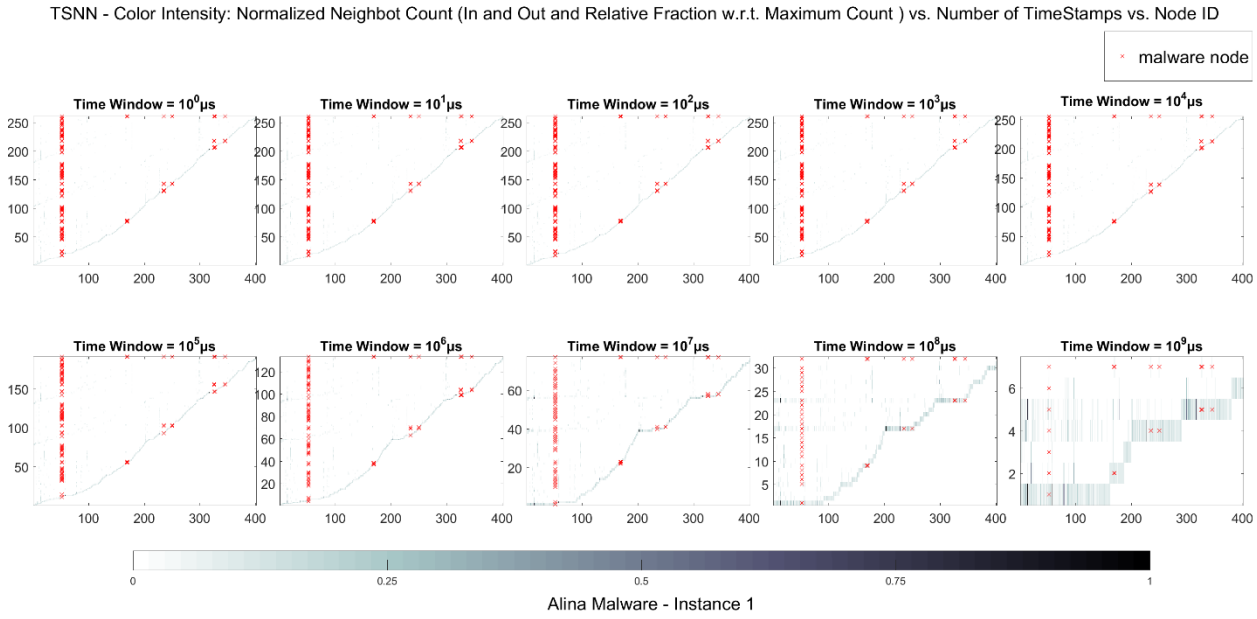


Time Graph Node Based Features

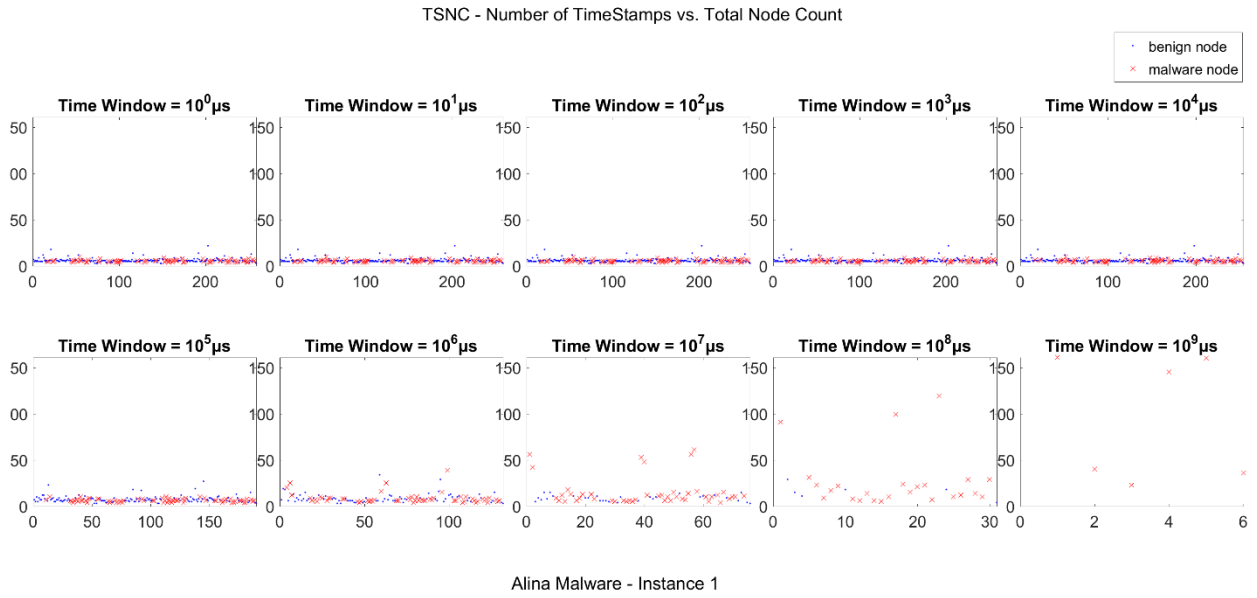
10) CNTS



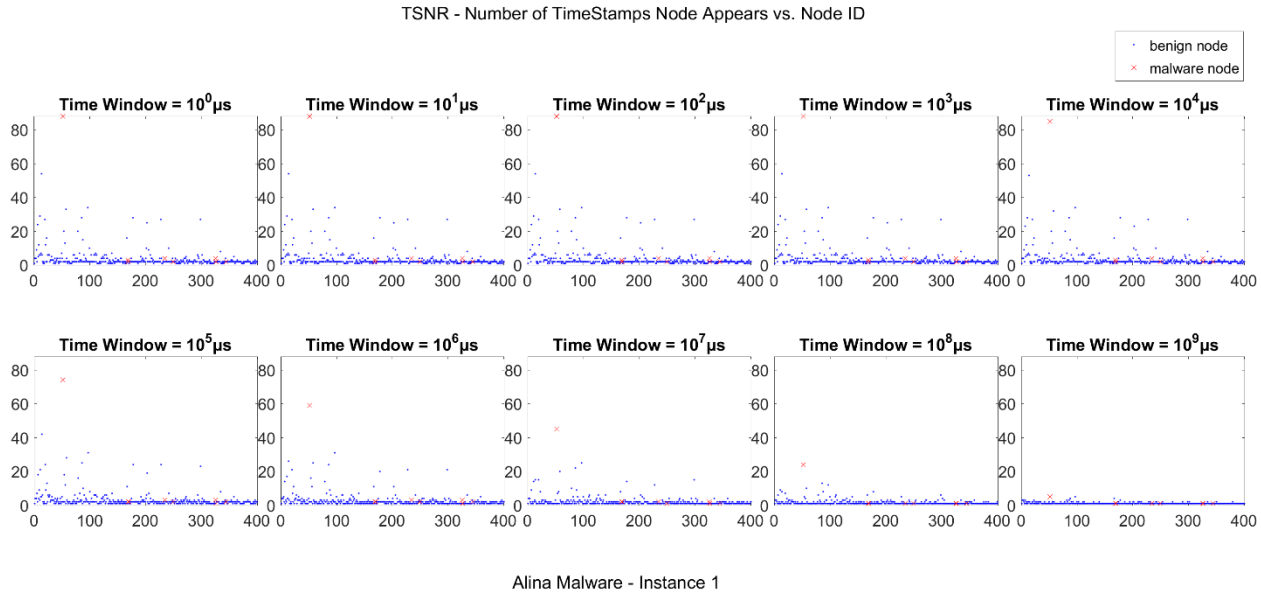
11) TSNN



12) TSNC



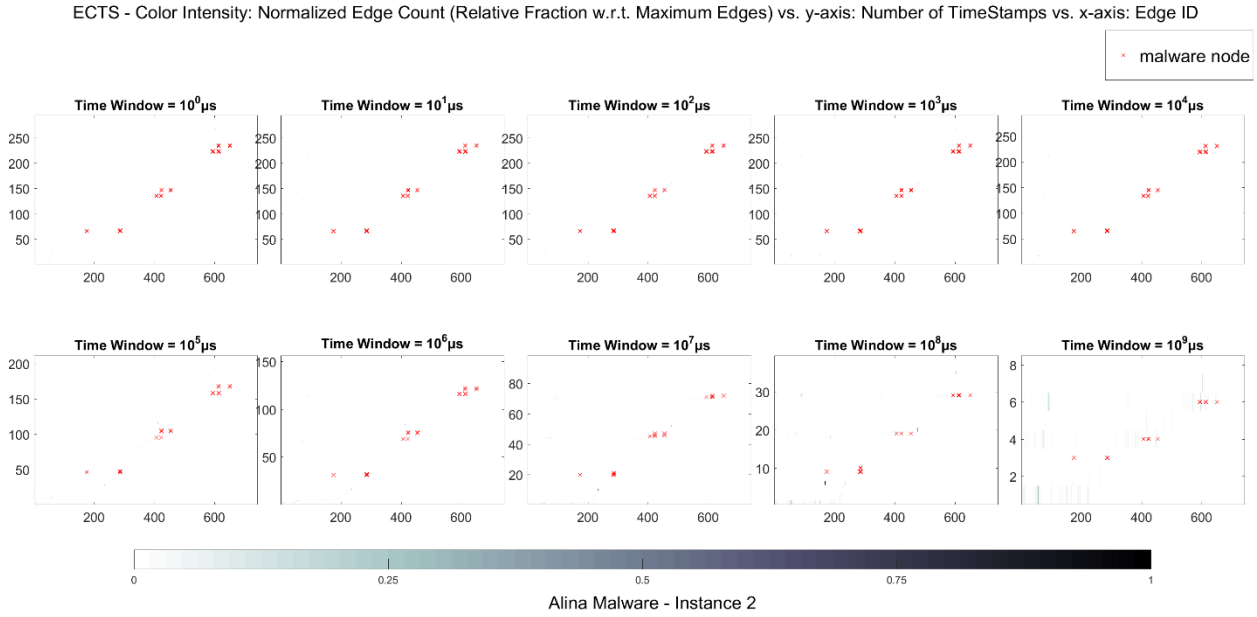
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Alina Malware - Instance 1

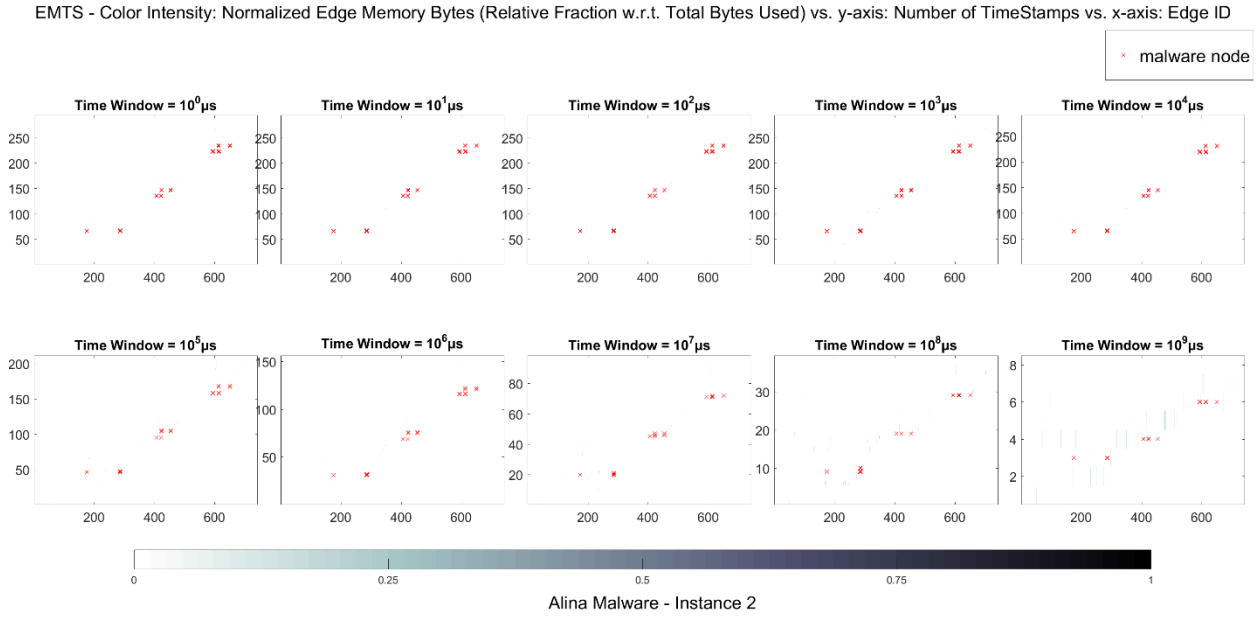
7.1.12 Alina Malware – Instance 2

Time Graph Edge Based Features

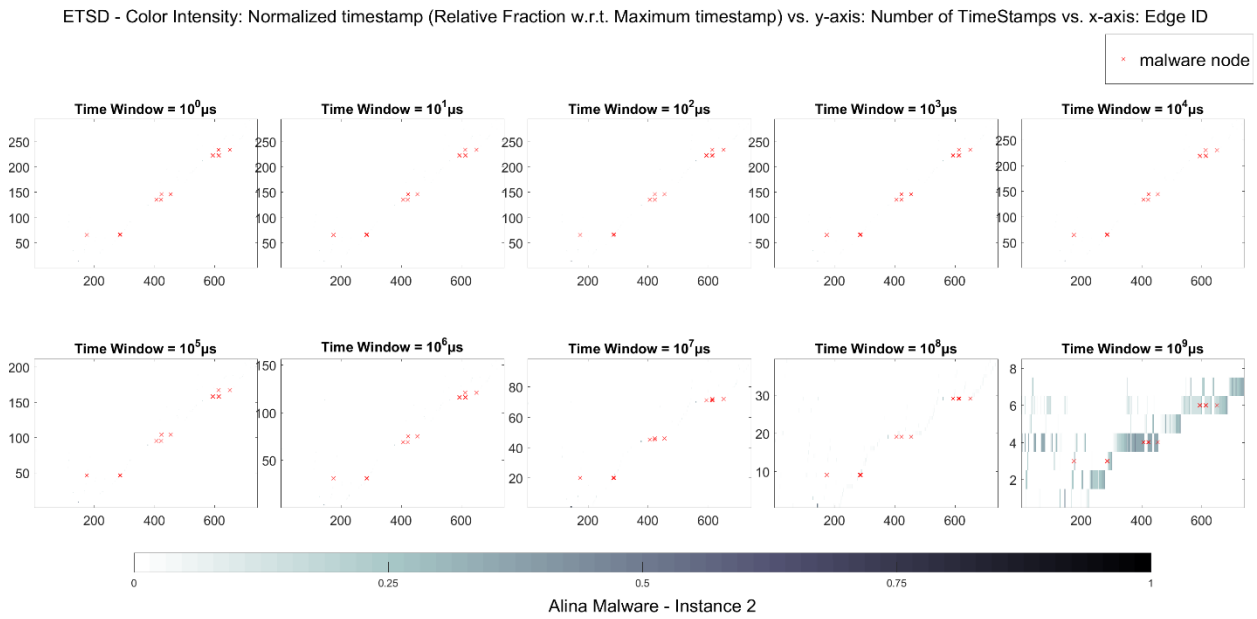
1) ECTS



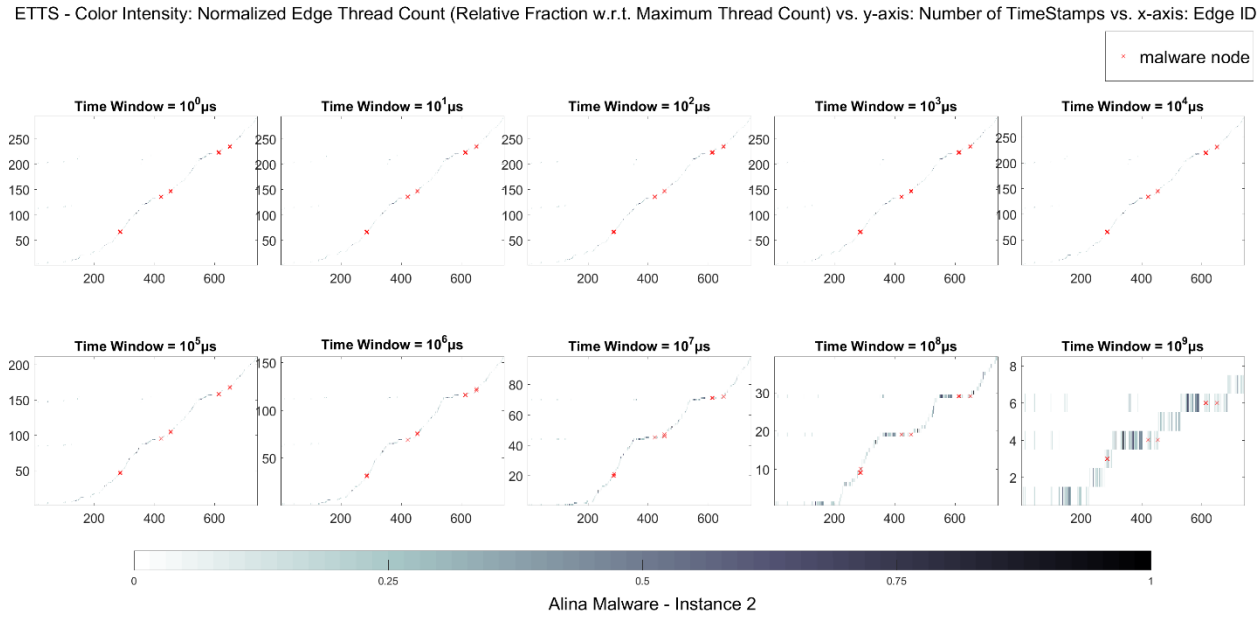
2) EMTS



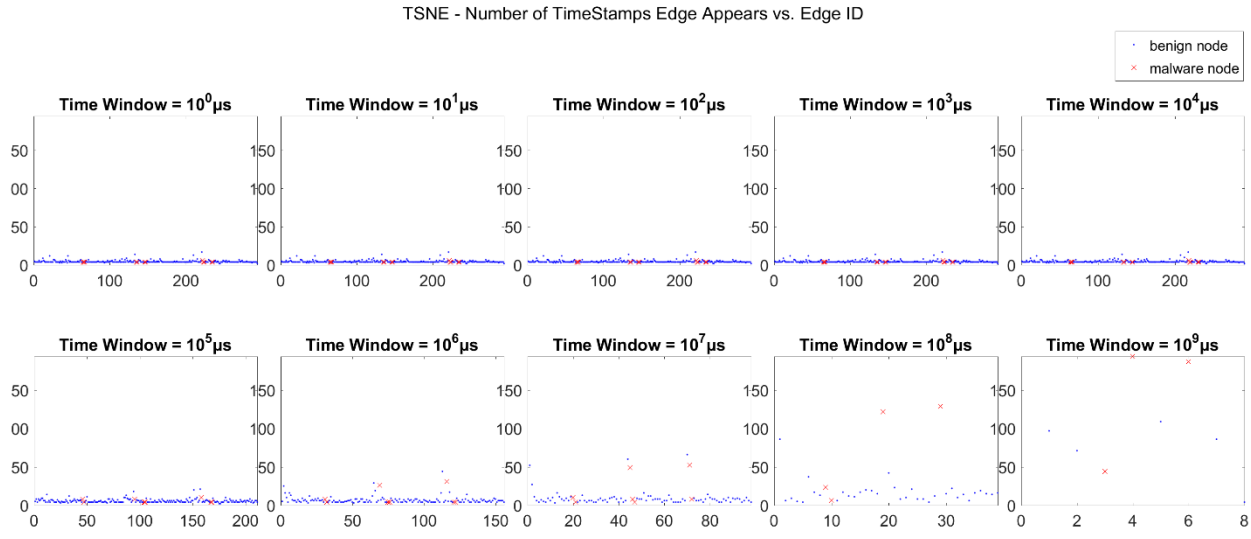
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Alina Malware - Instance 2

4) ETTS

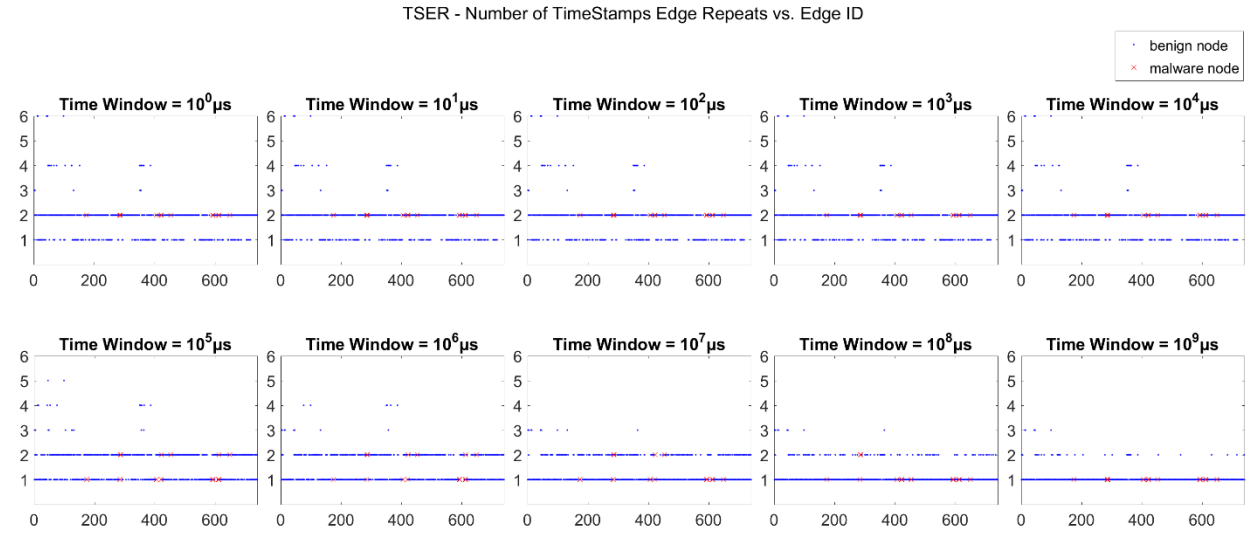

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Alina Malware - Instance 2

5) TSNE



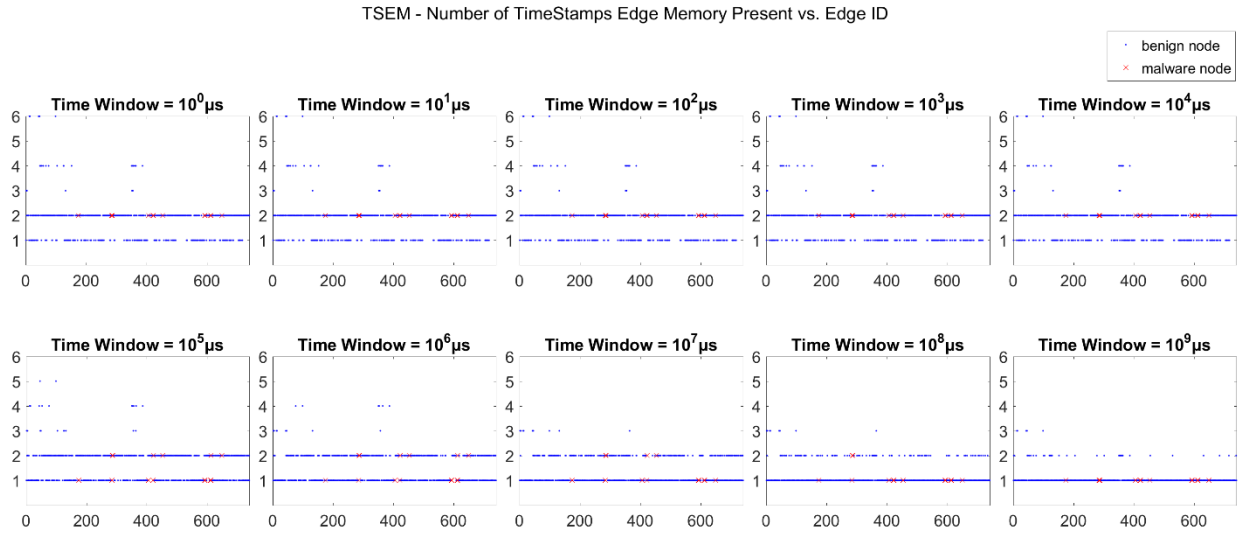
Alina Malware - Instance 2

6) TSER

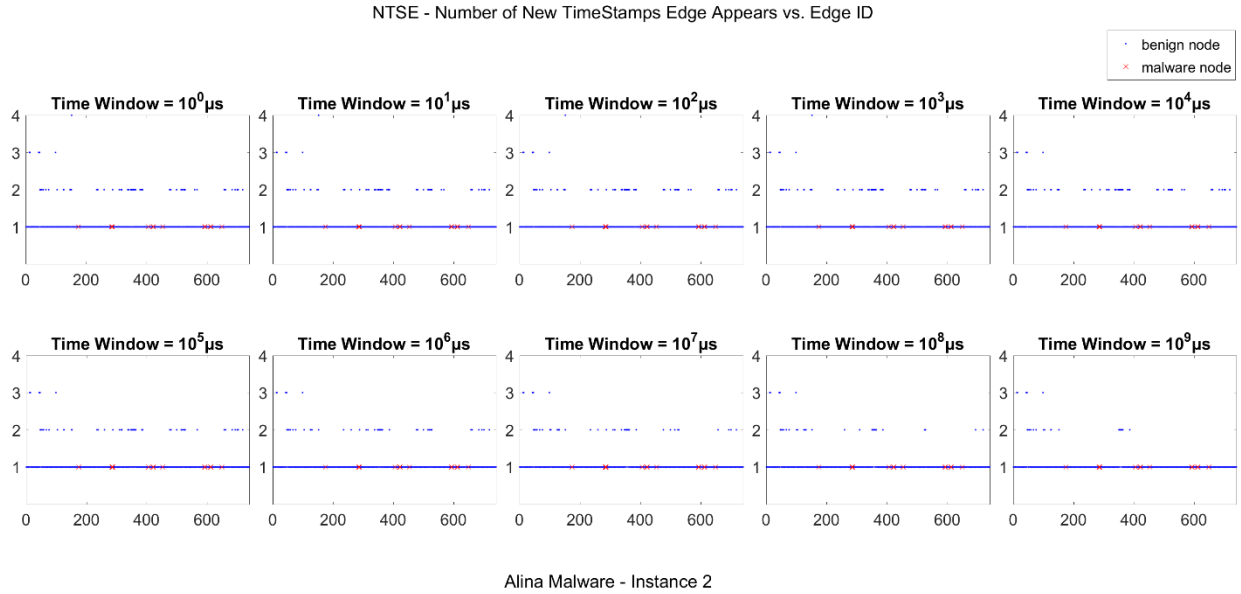


Alina Malware - Instance 2

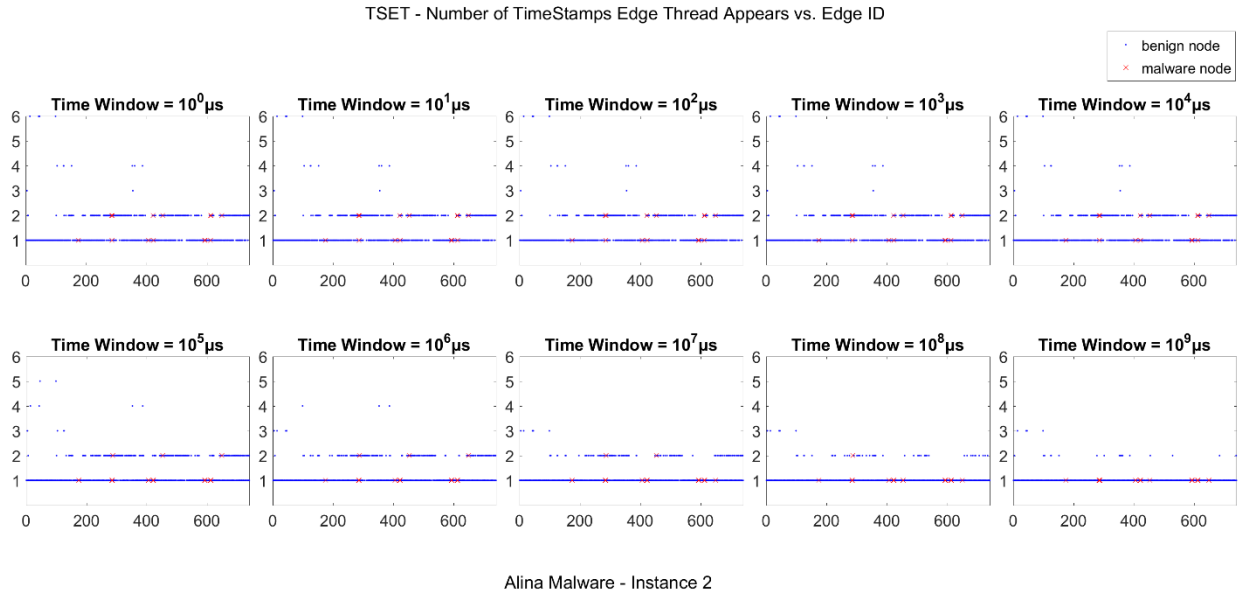
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Alina Malware - Instance 2

8) NTSE

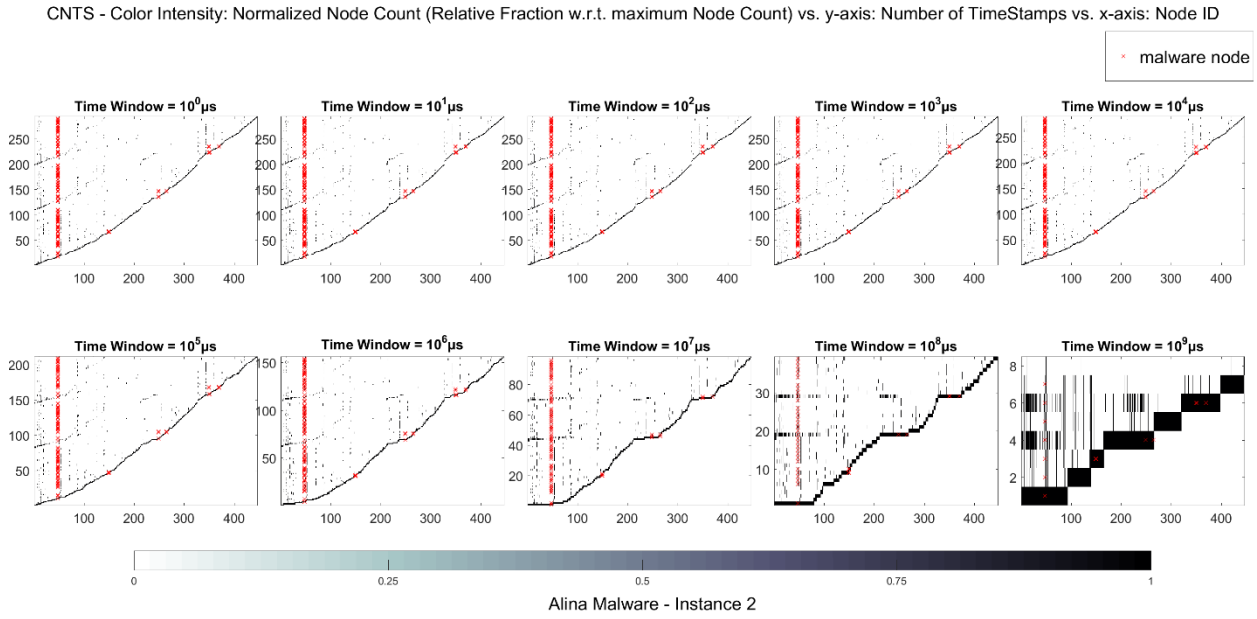

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Alina Malware - Instance 2

9) TSET

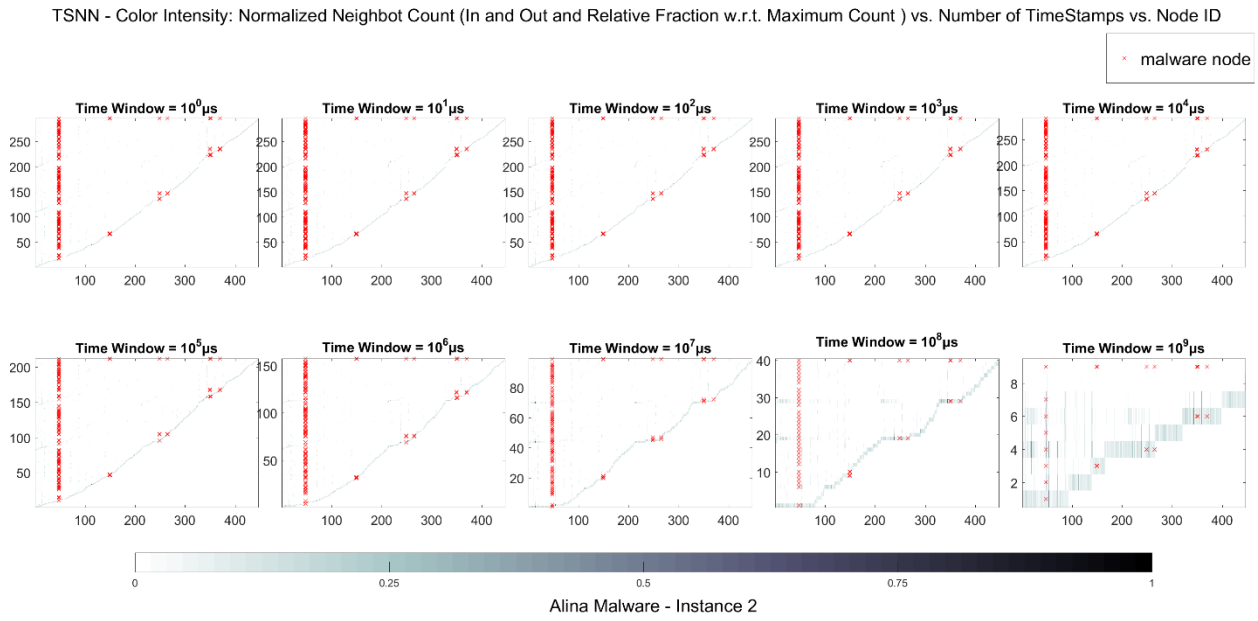


Time Graph Node Based Features

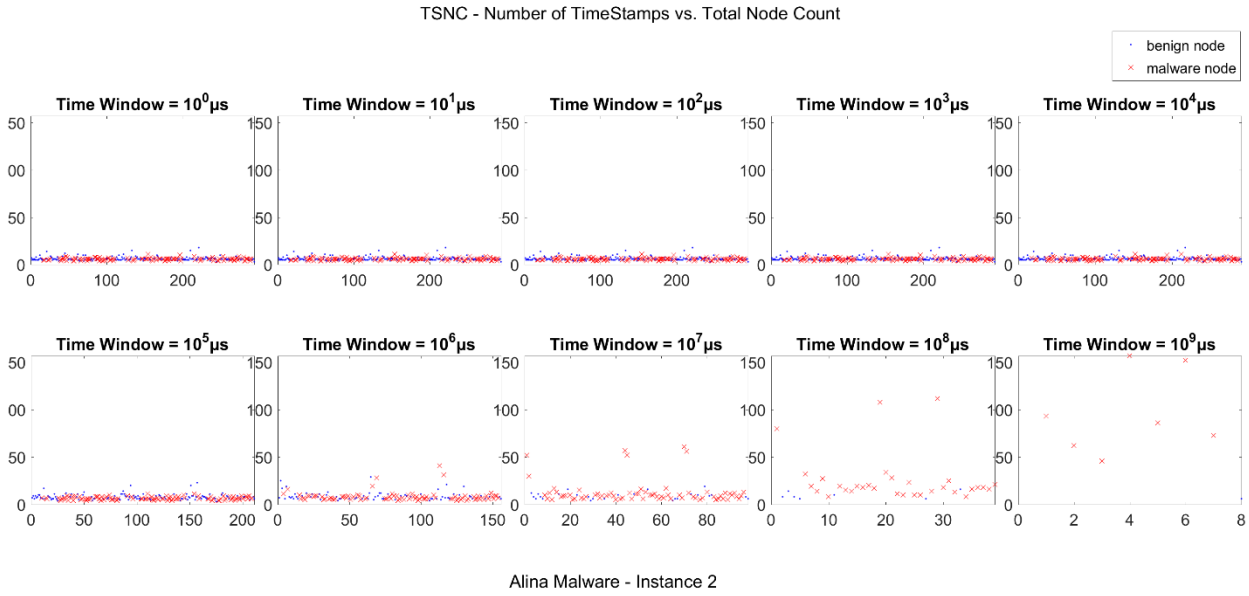
10) CNTS



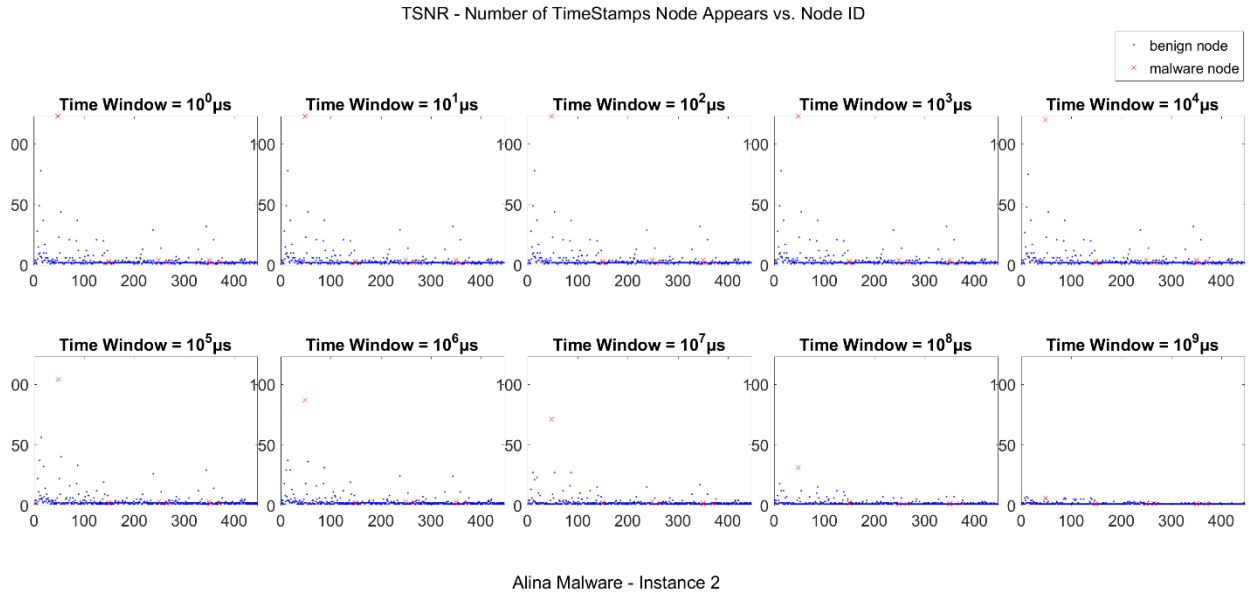
11) TSNN



12) TSNC



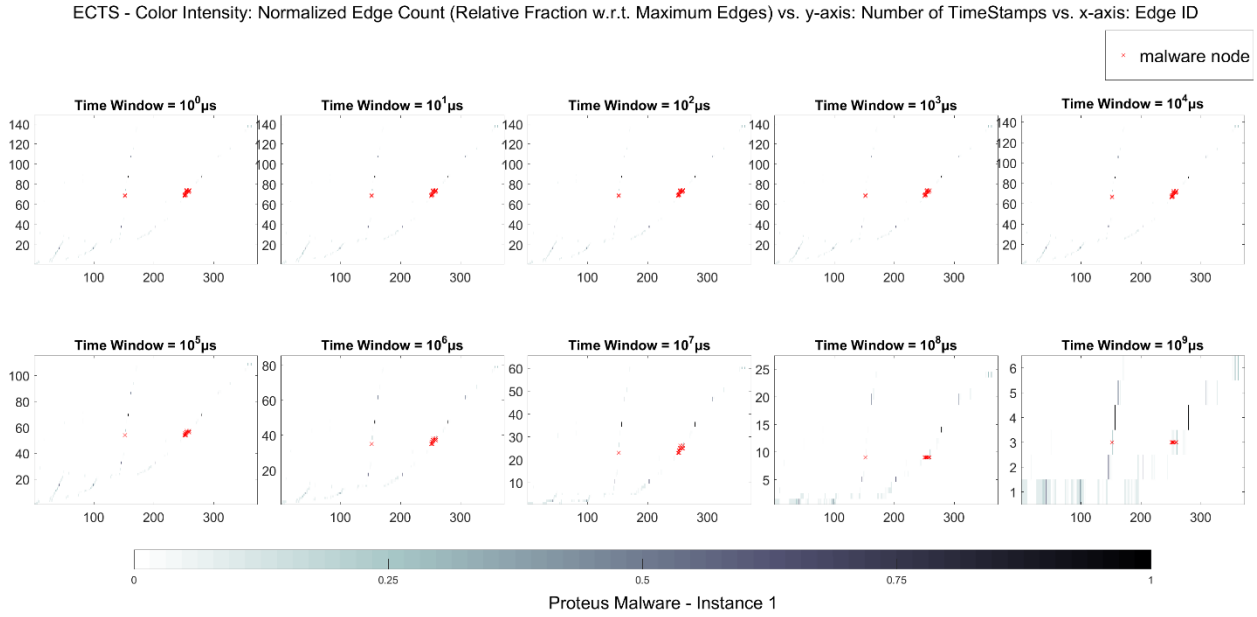
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
50
100
0
100
200
300
400
Alina Malware - Instance 2

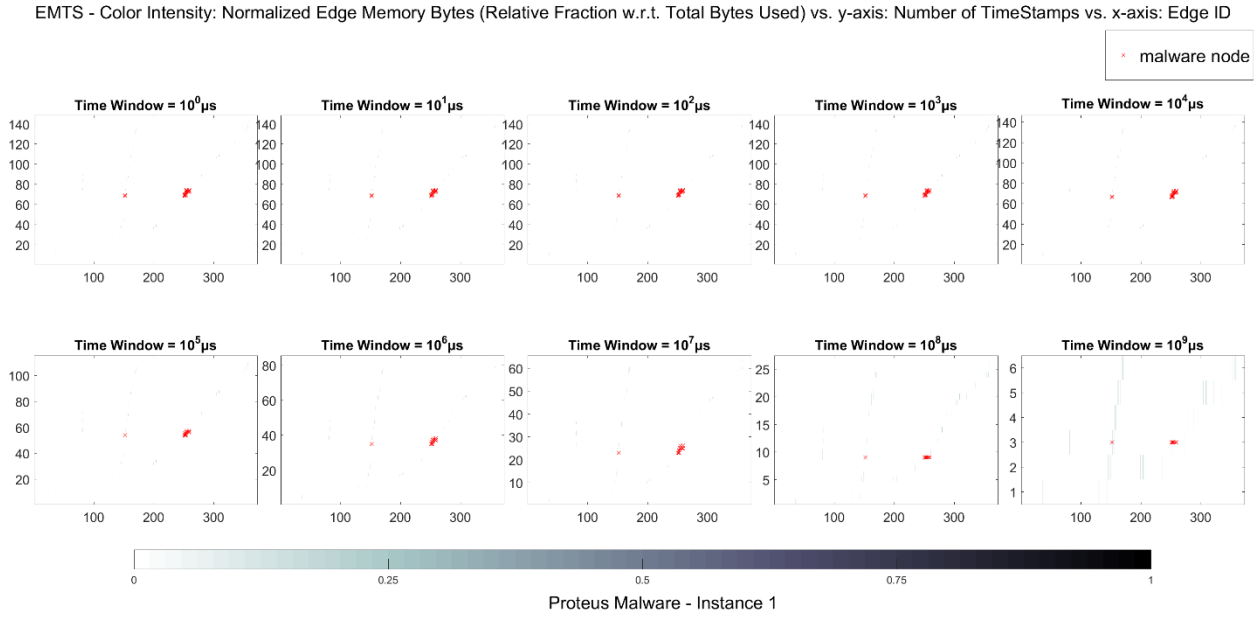
7.1.13 Proteus Malware – Instance 1

Time Graph Edge Based Features

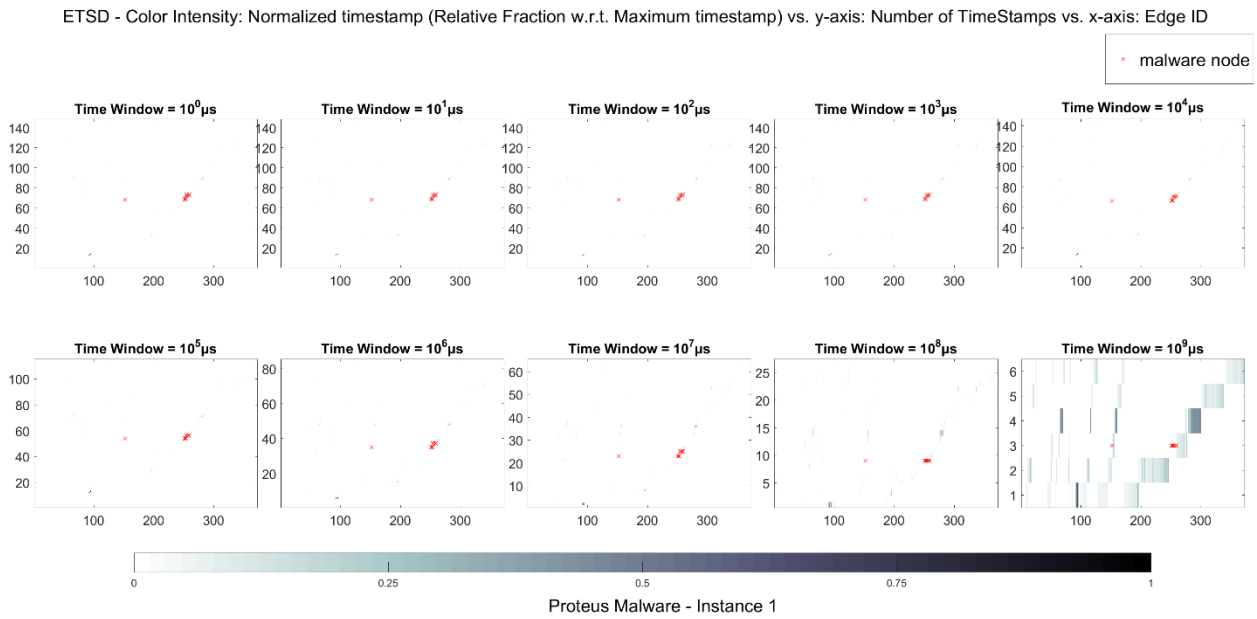
1) ECTS



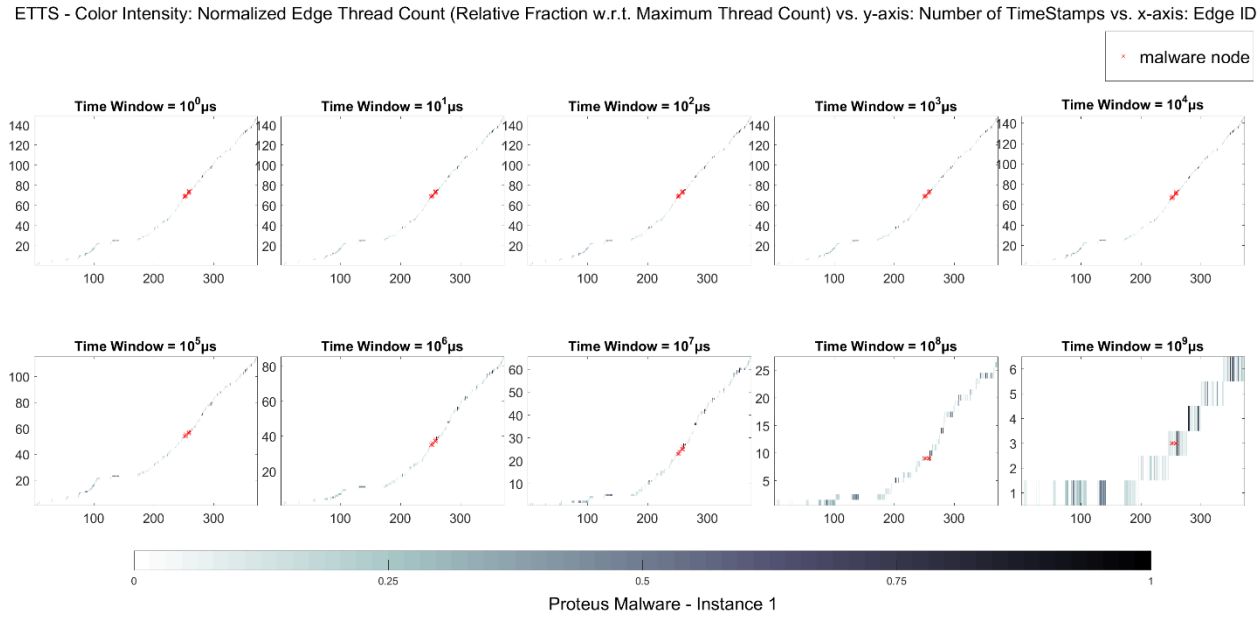
2) EMTS



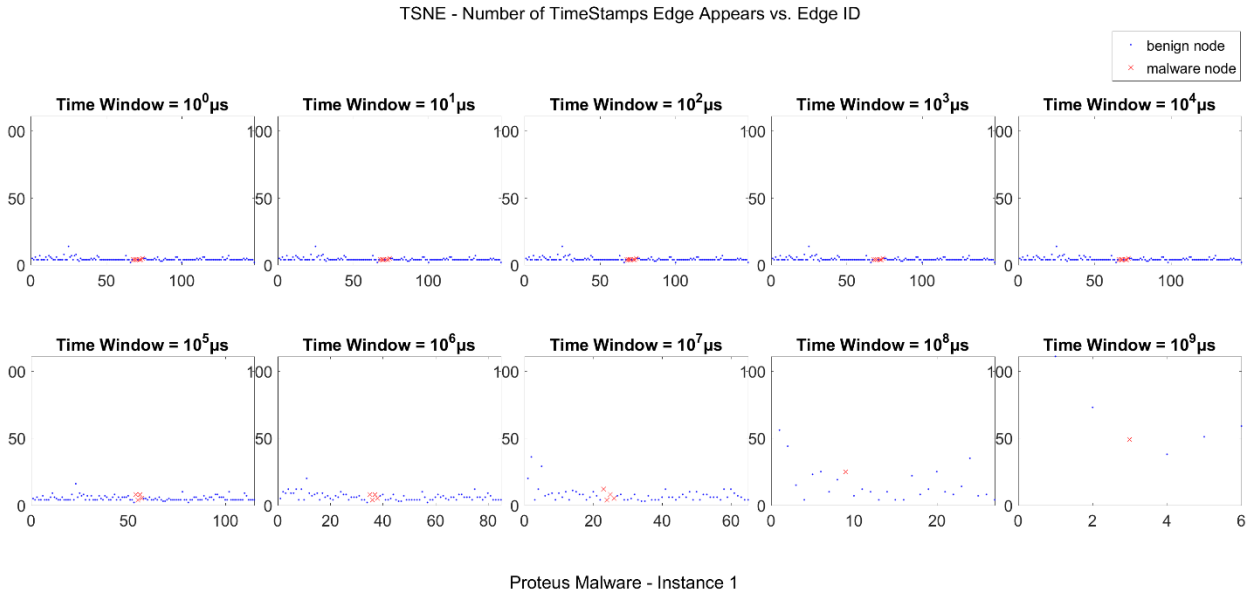
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Proteus Malware - Instance 1

4) ETTS

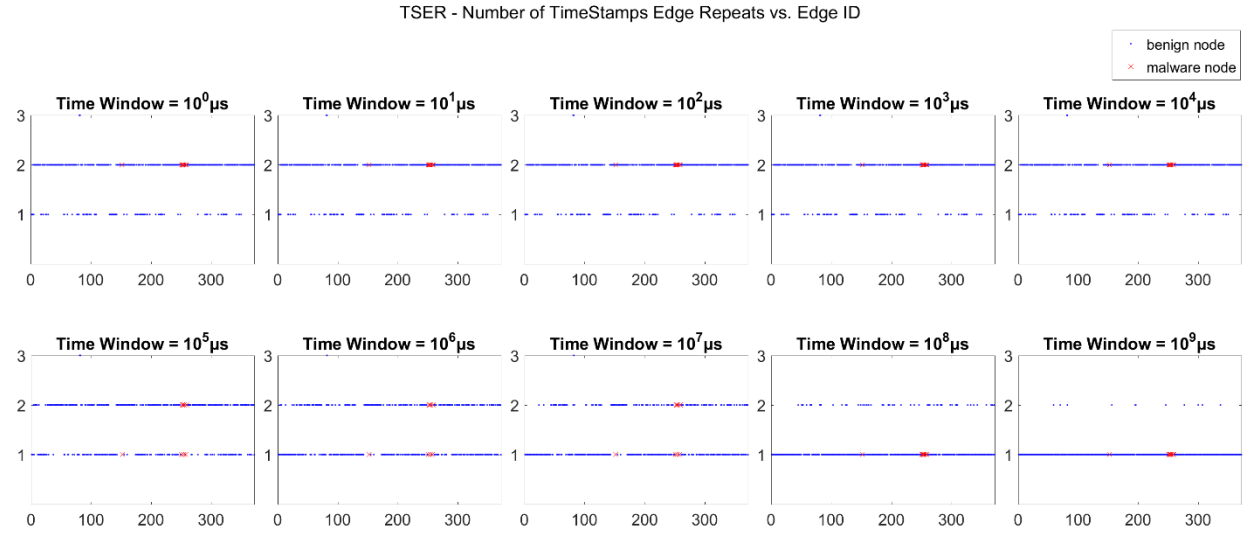

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Proteus Malware - Instance 1

5) TSNE



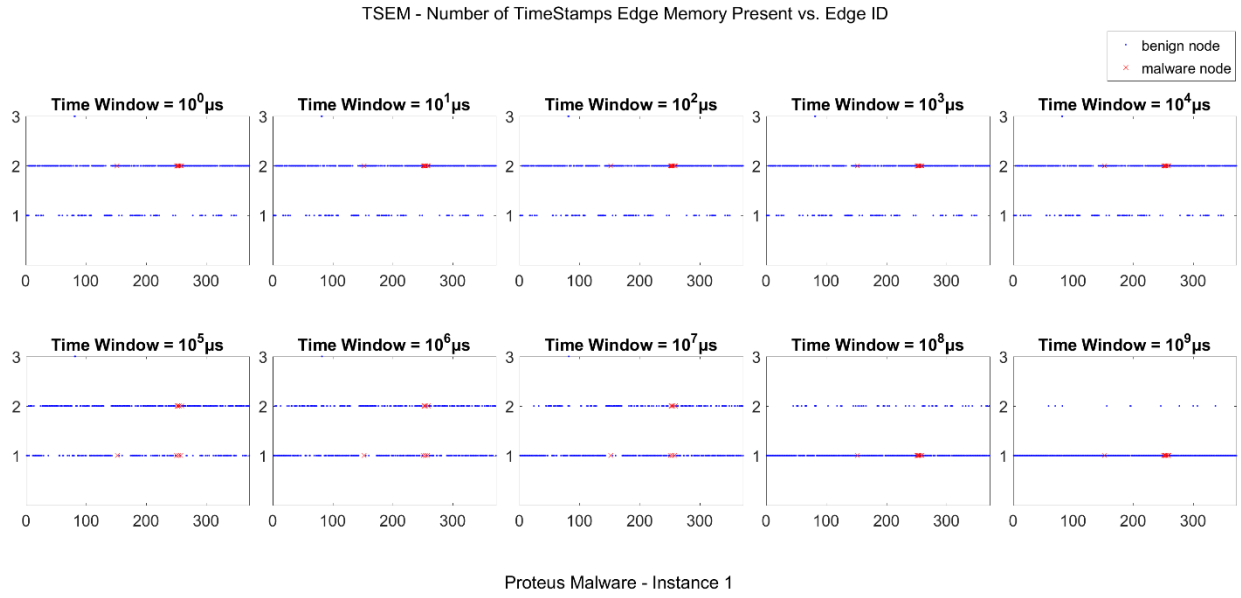
Proteus Malware - Instance 1

6) TSER

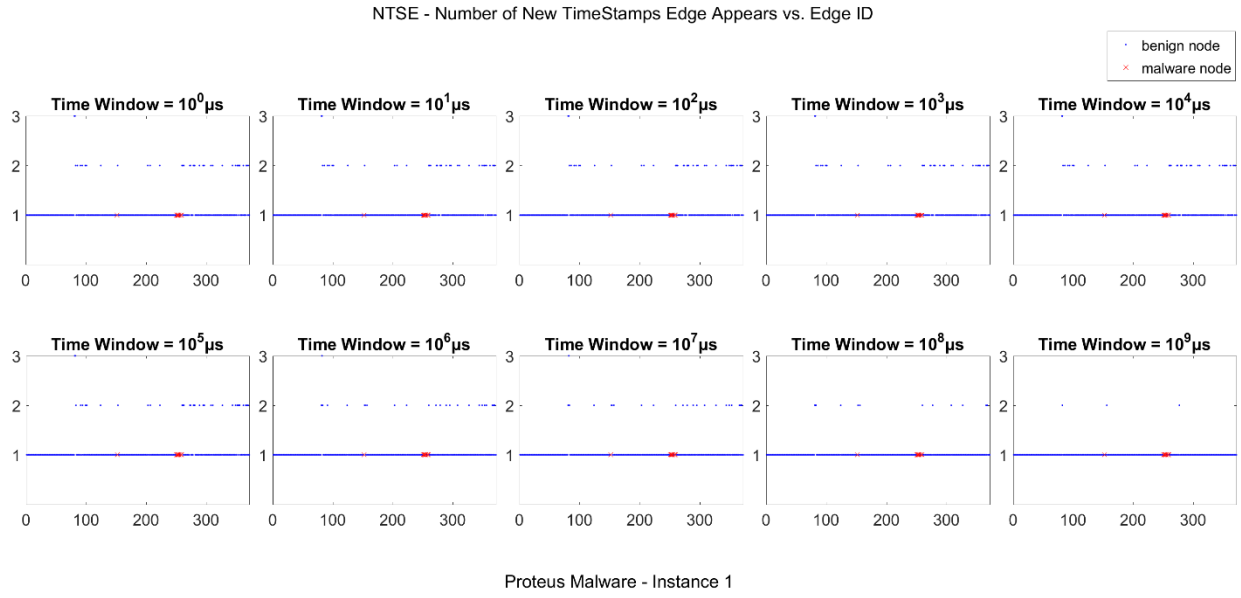


Proteus Malware - Instance 1

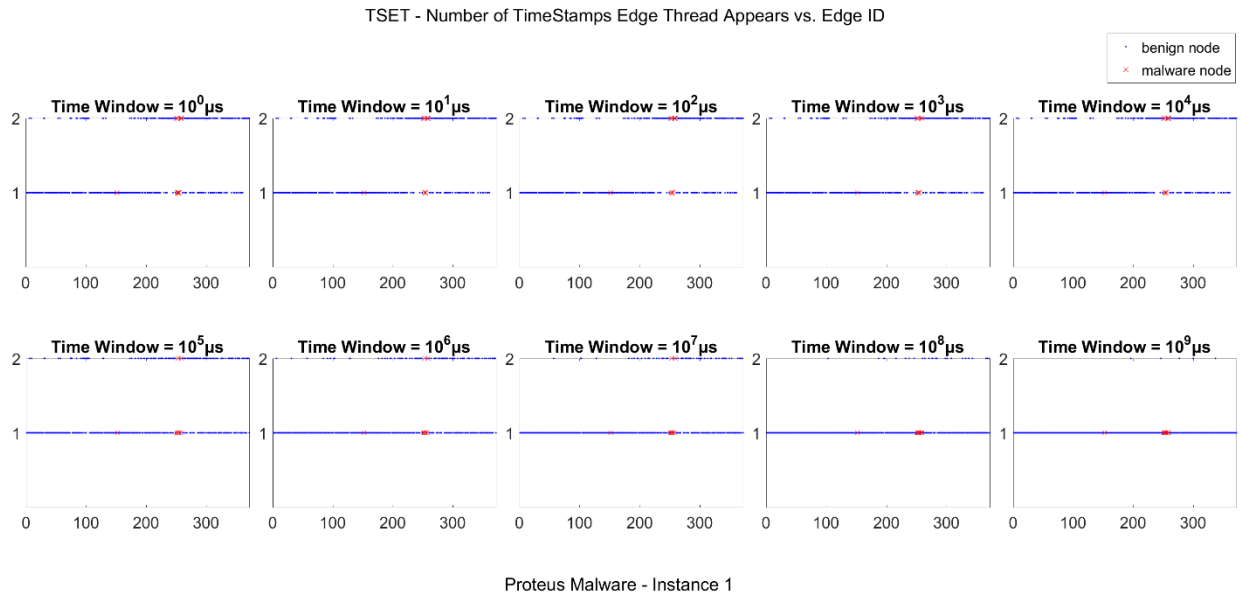
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Proteus Malware - Instance 1

8) NTSE

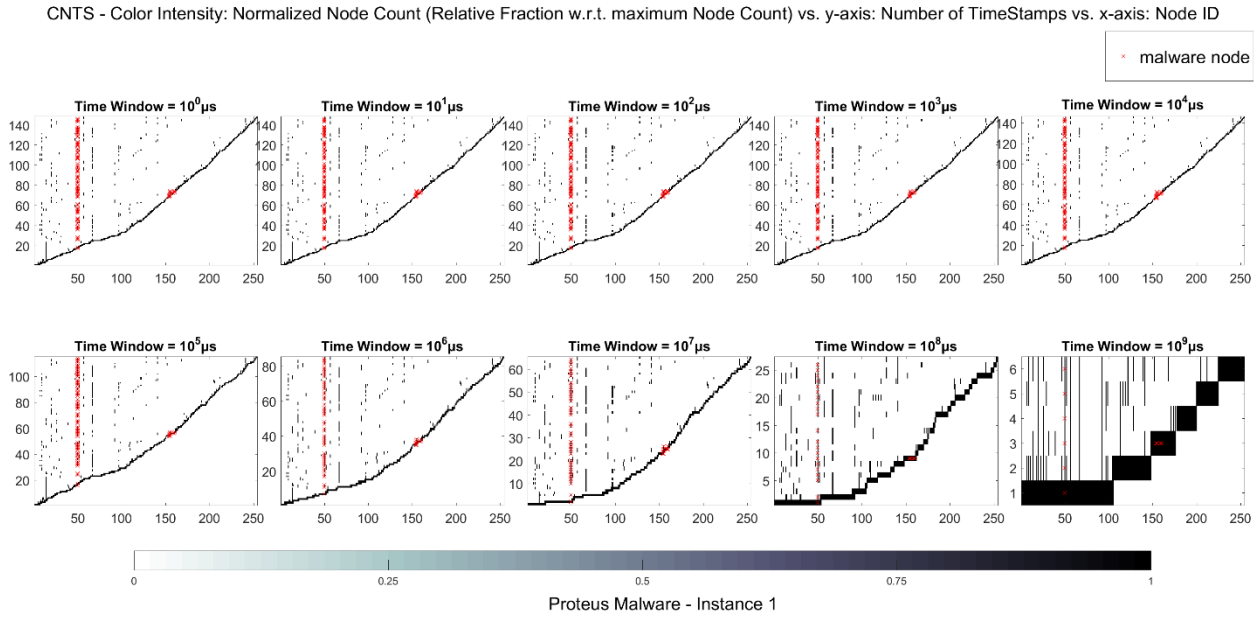

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Proteus Malware - Instance 1

9) TSET

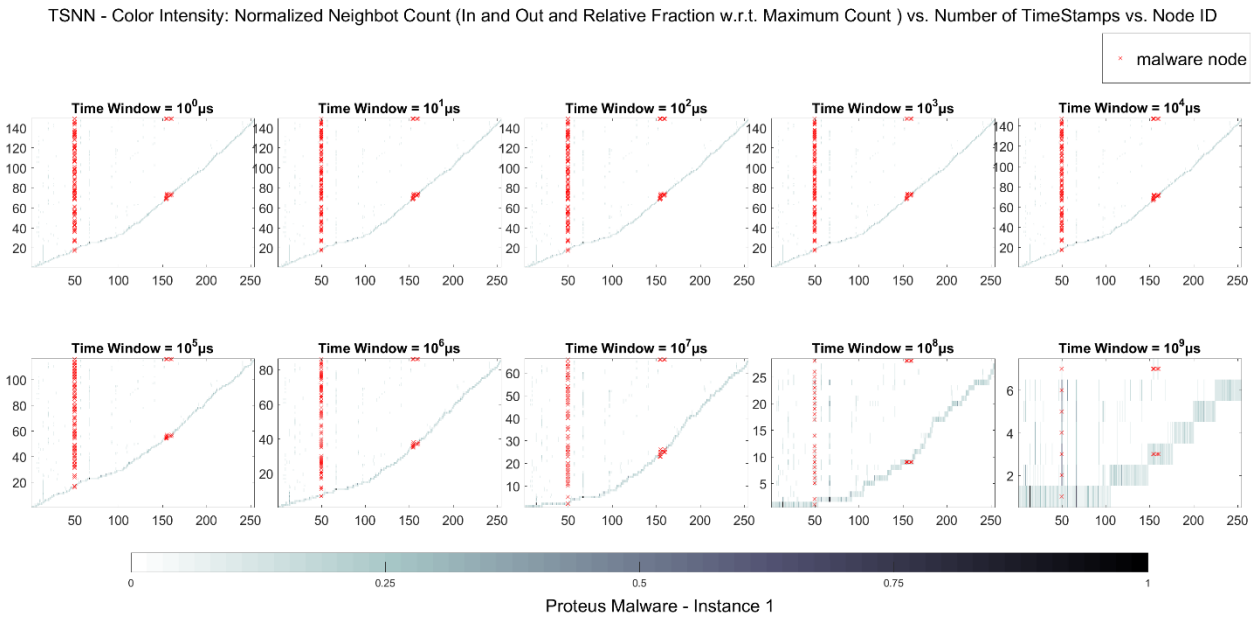


Time Graph Node Based Features

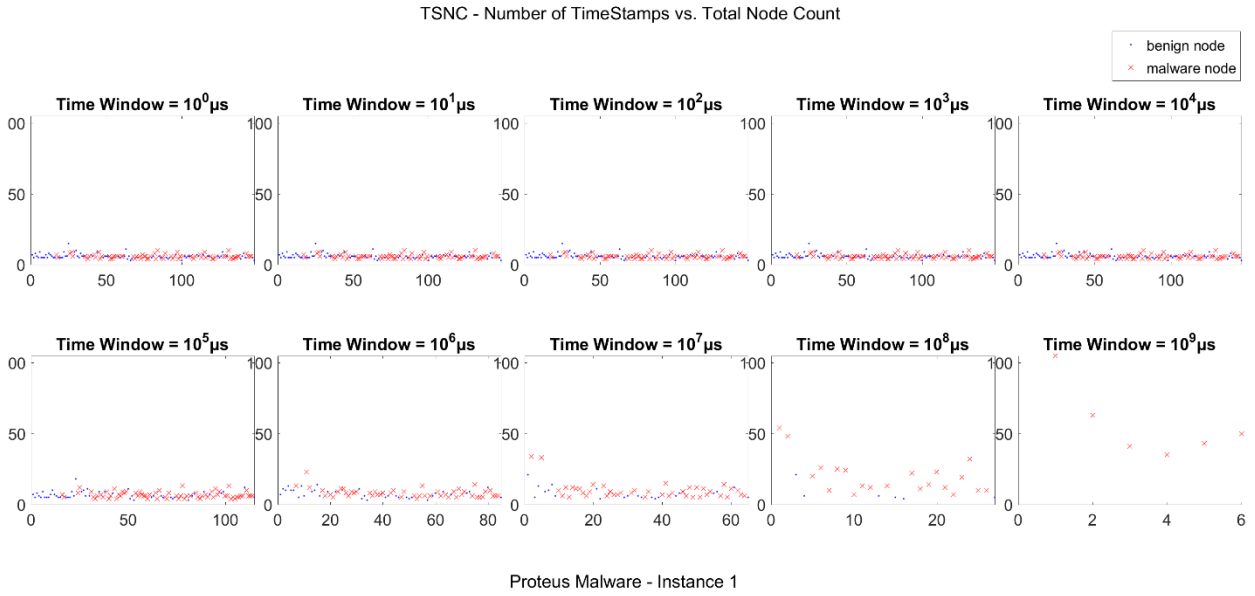
10) CNTS



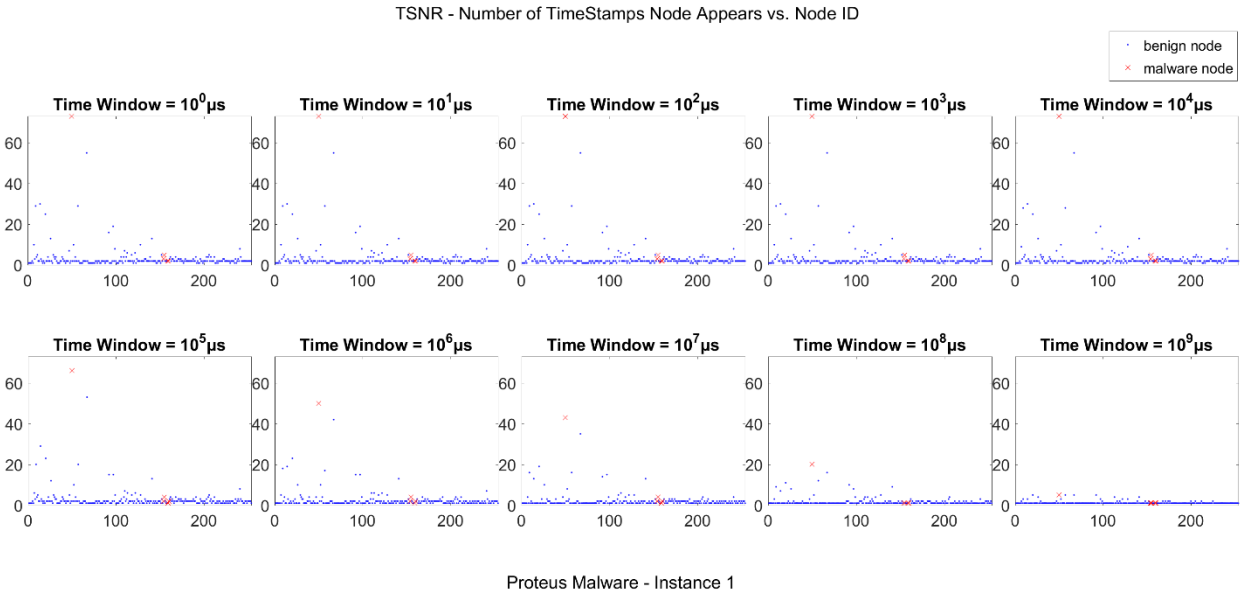
11) TSNN



12) TSNC



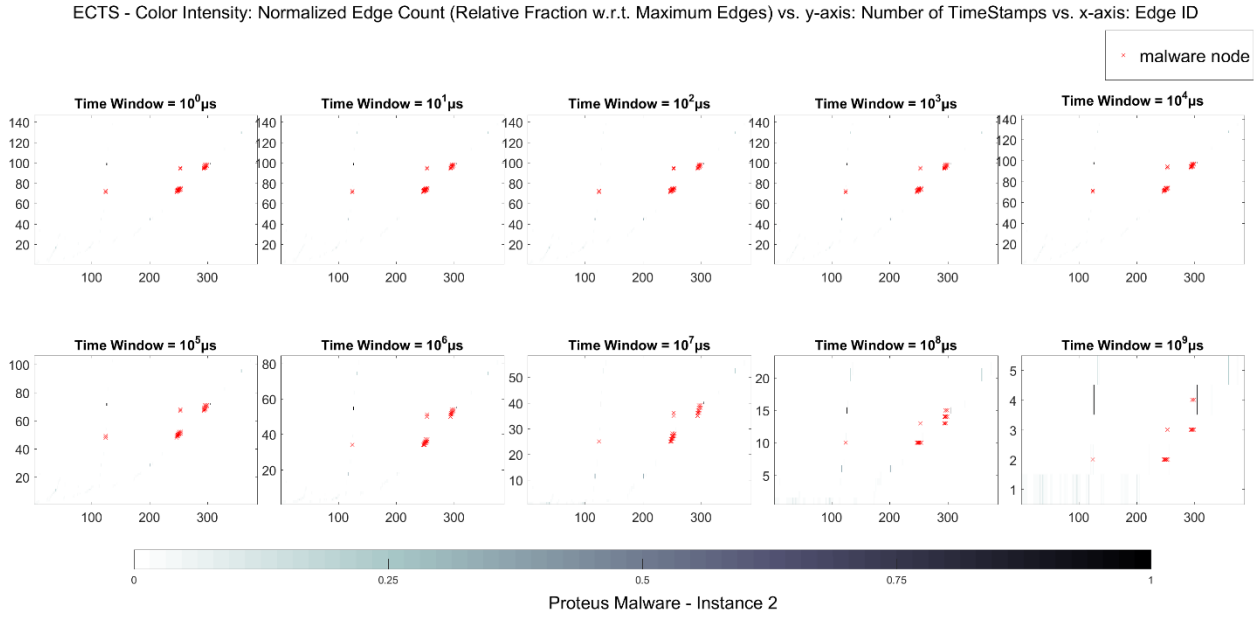
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Proteus Malware - Instance 1

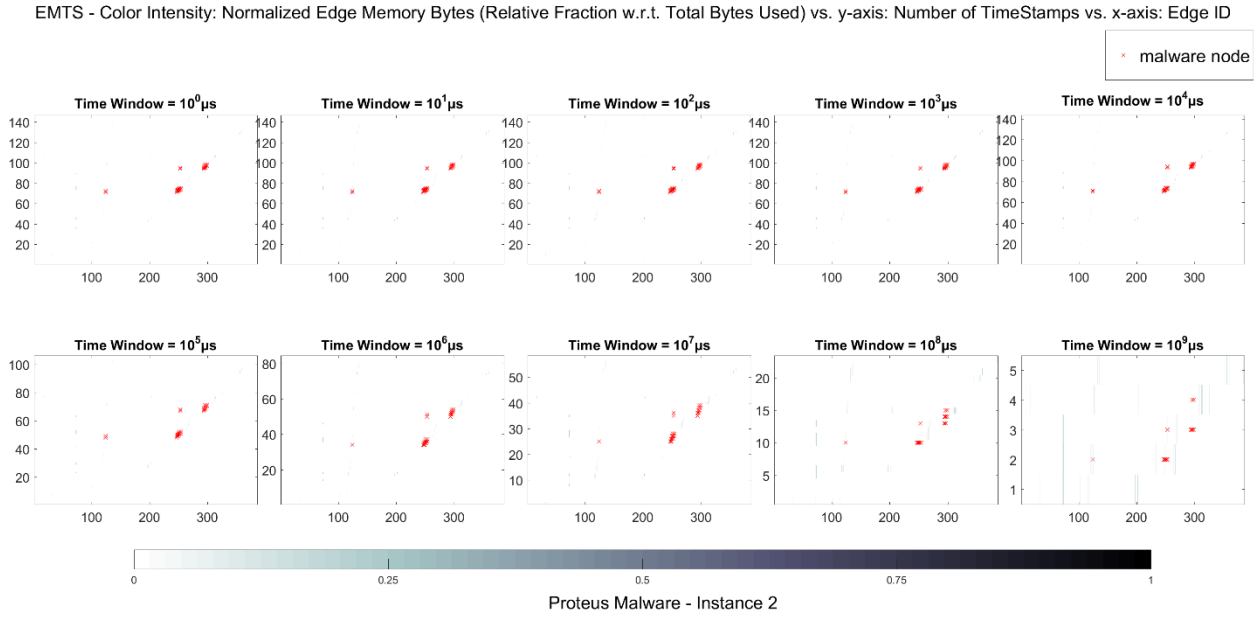
7.1.14 Proteus Malware – Instance 2

Time Graph Edge Based Features

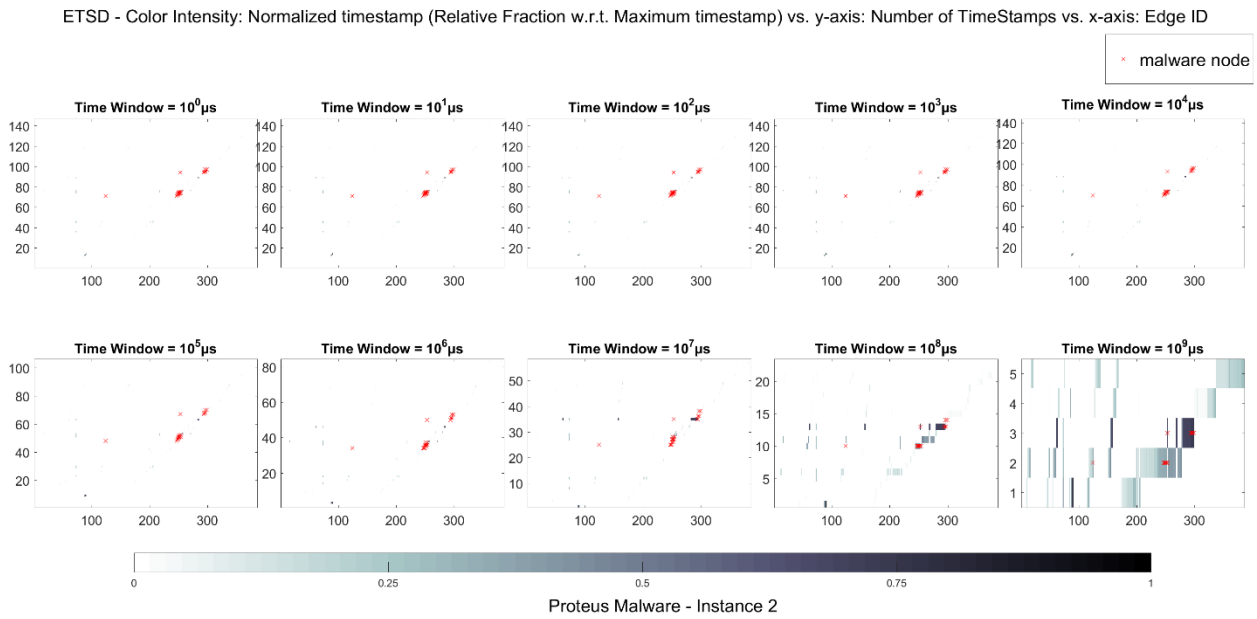
1) ECTS



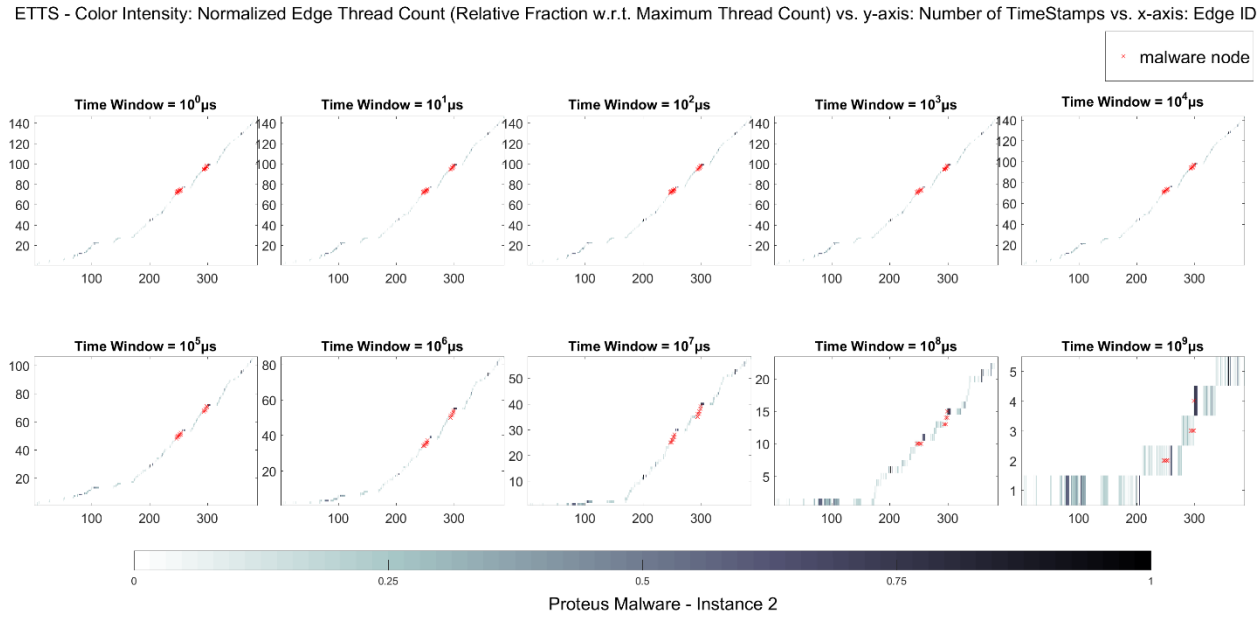
2) EMTS



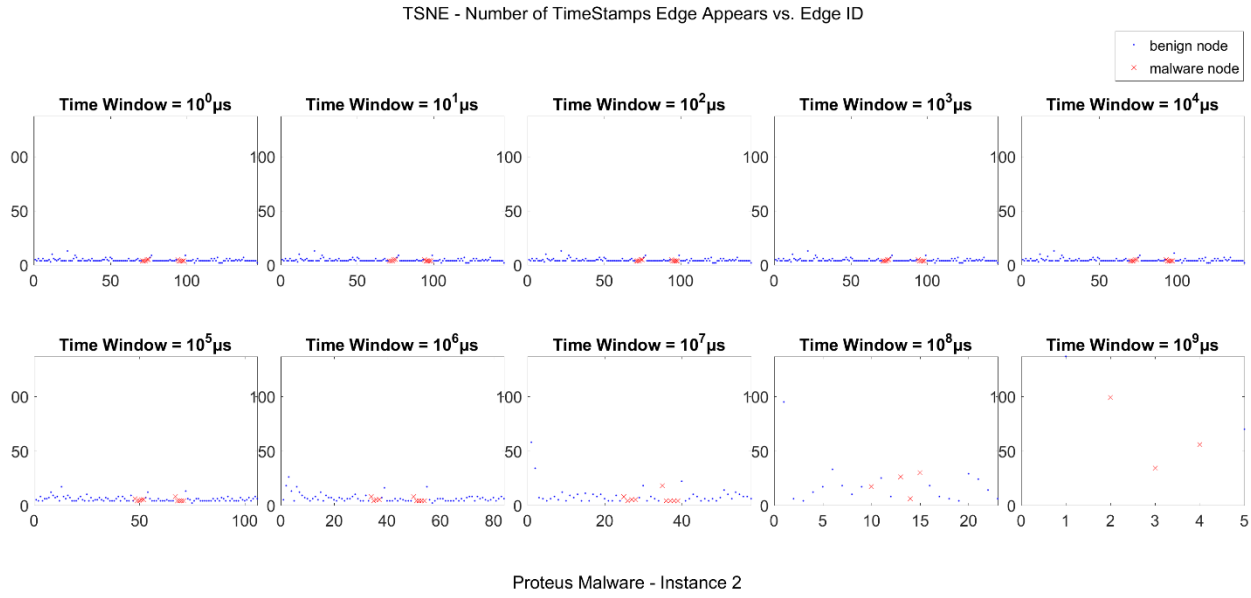
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0 µs
Time Window = 10^1 µs
Time Window = 10^2 µs
Time Window = 10^3 µs
Time Window = 10^4 µs
Time Window = 10^5 µs
Time Window = 10^6 µs
Time Window = 10^7 µs
Time Window = 10^8 µs
Time Window = 10^9 µs
0
0.25
0.5
0.75
1
Proteus Malware - Instance 2

4) ETTS

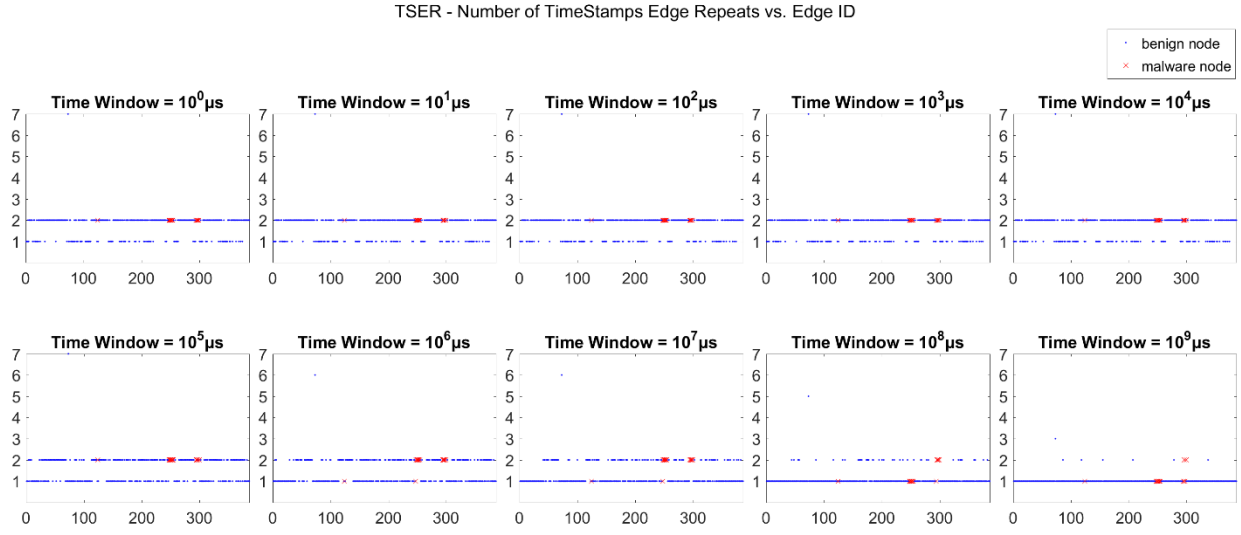

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0 µs
Time Window = 10^1 µs
Time Window = 10^2 µs
Time Window = 10^3 µs
Time Window = 10^4 µs
Time Window = 10^5 µs
Time Window = 10^6 µs
Time Window = 10^7 µs
Time Window = 10^8 µs
Time Window = 10^9 µs
0
0.25
0.5
0.75
1
Proteus Malware - Instance 2

5) TSNE



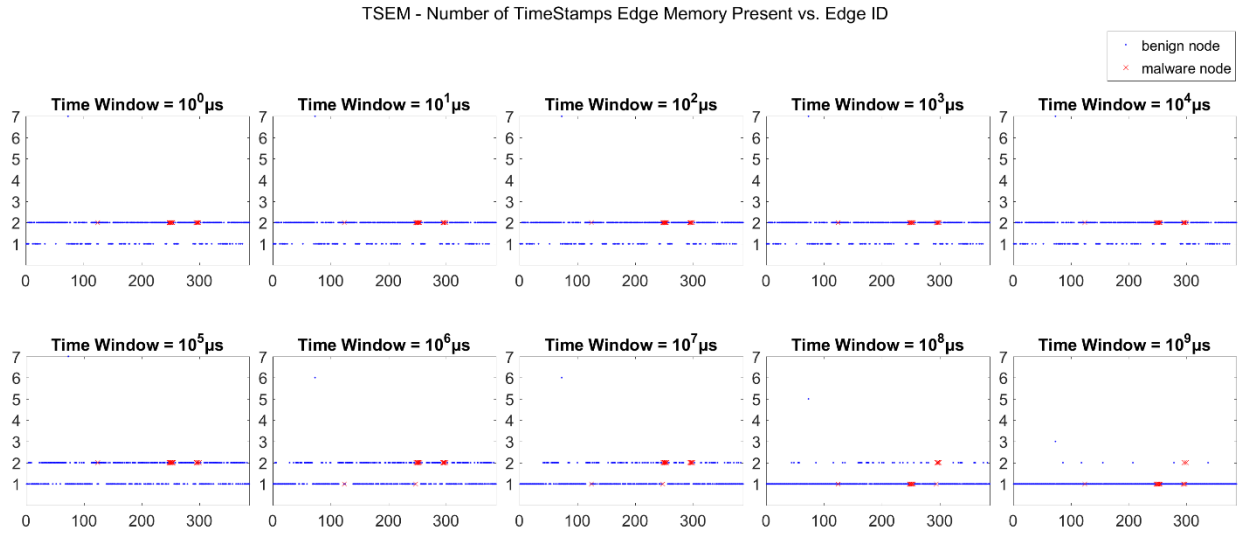
Proteus Malware - Instance 2

6) TSER



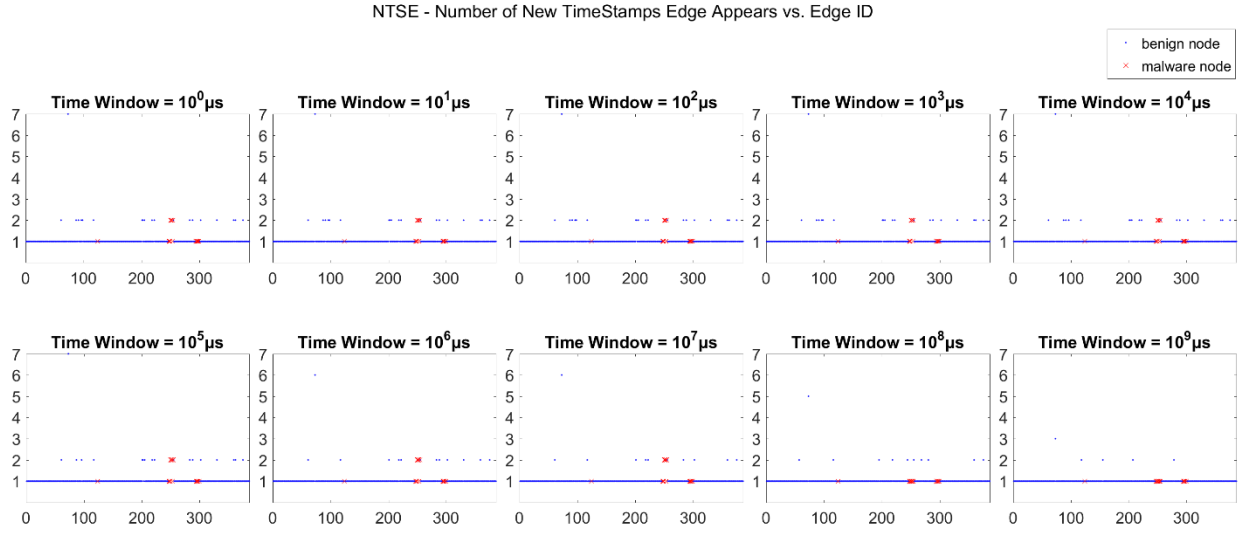
Proteus Malware - Instance 2

7) TSEM



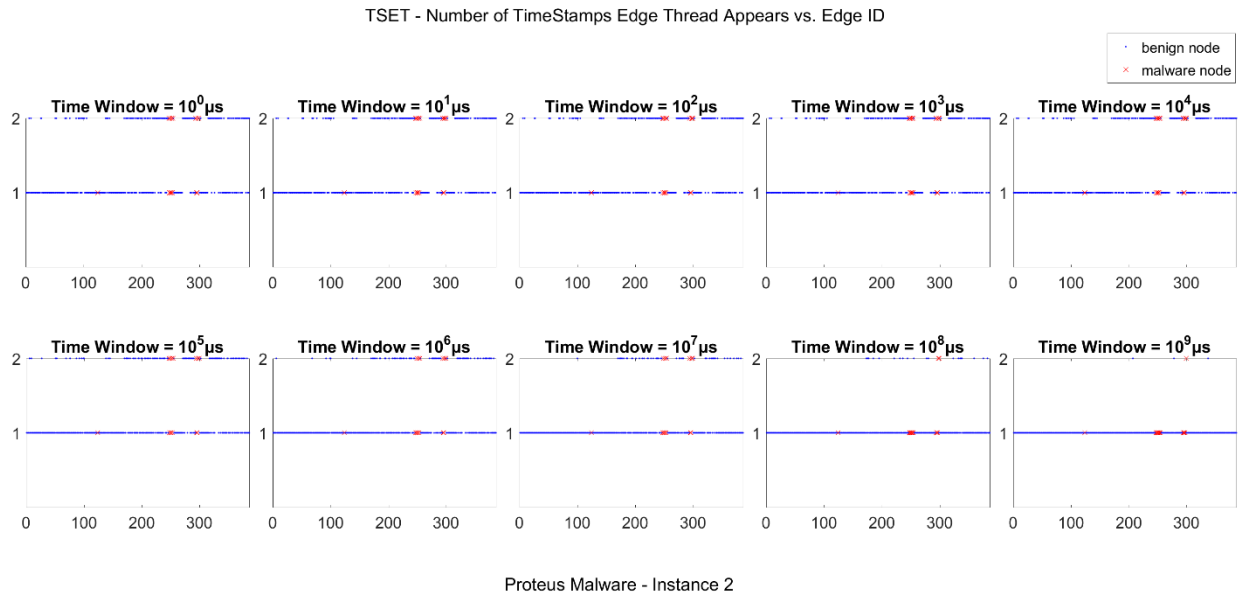
Proteus Malware - Instance 2

8) NTSE



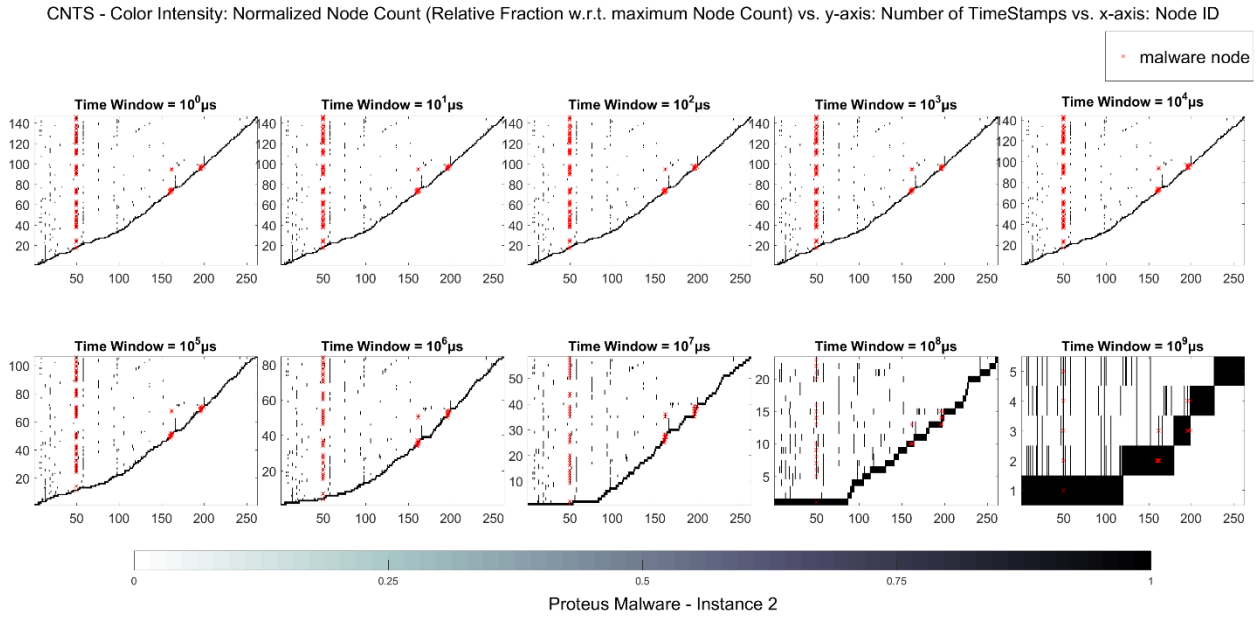
Proteus Malware - Instance 2

9) TSET

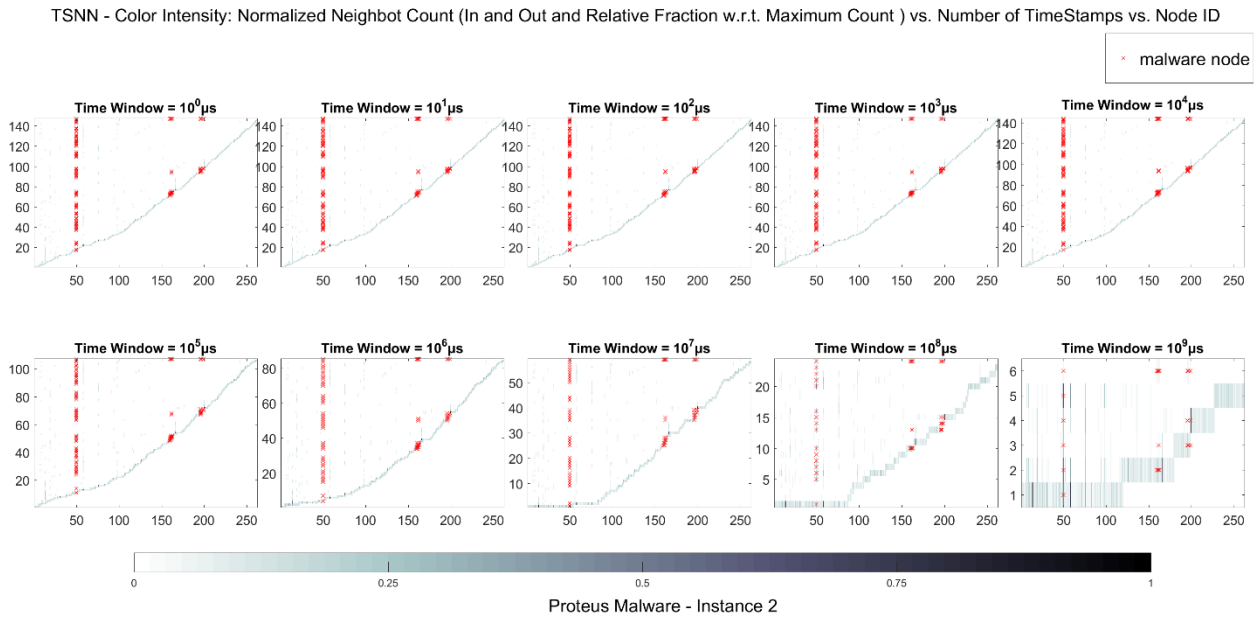


Time Graph Node Based Features

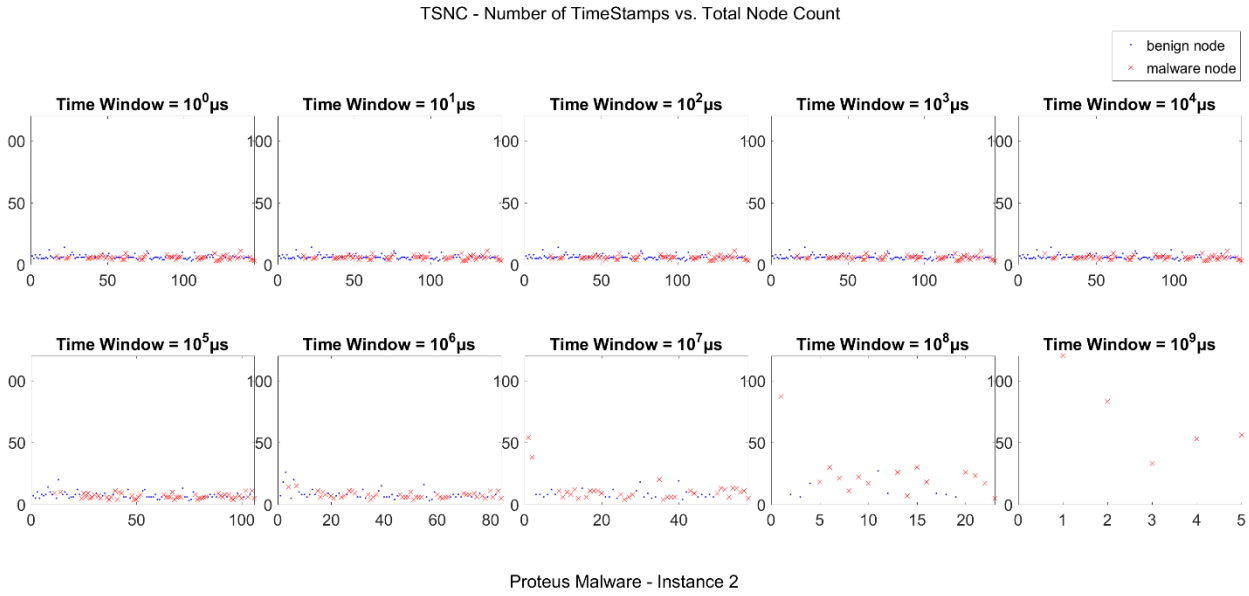
10) CNTS



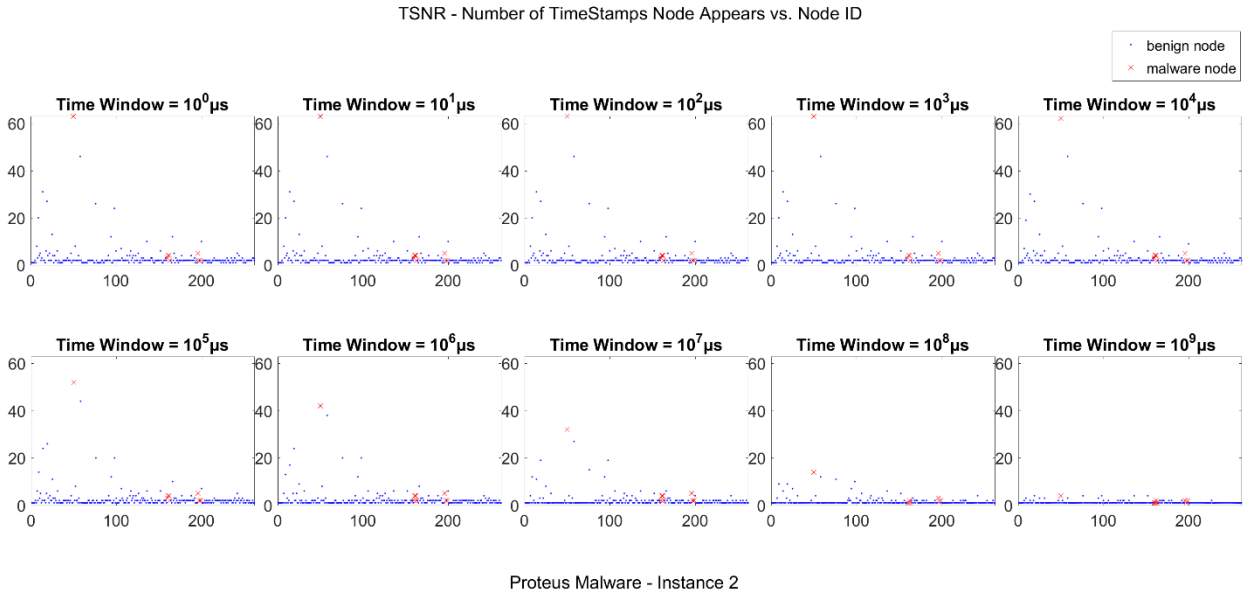
11) TSNN



12) TSNC



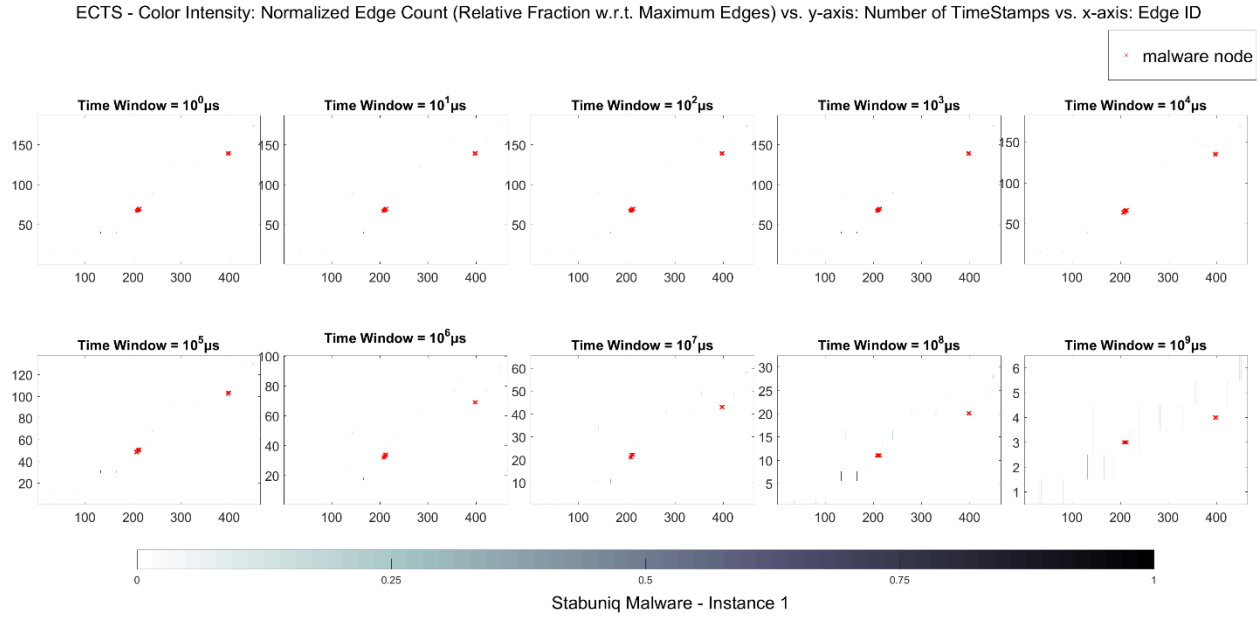
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Proteus Malware - Instance 2

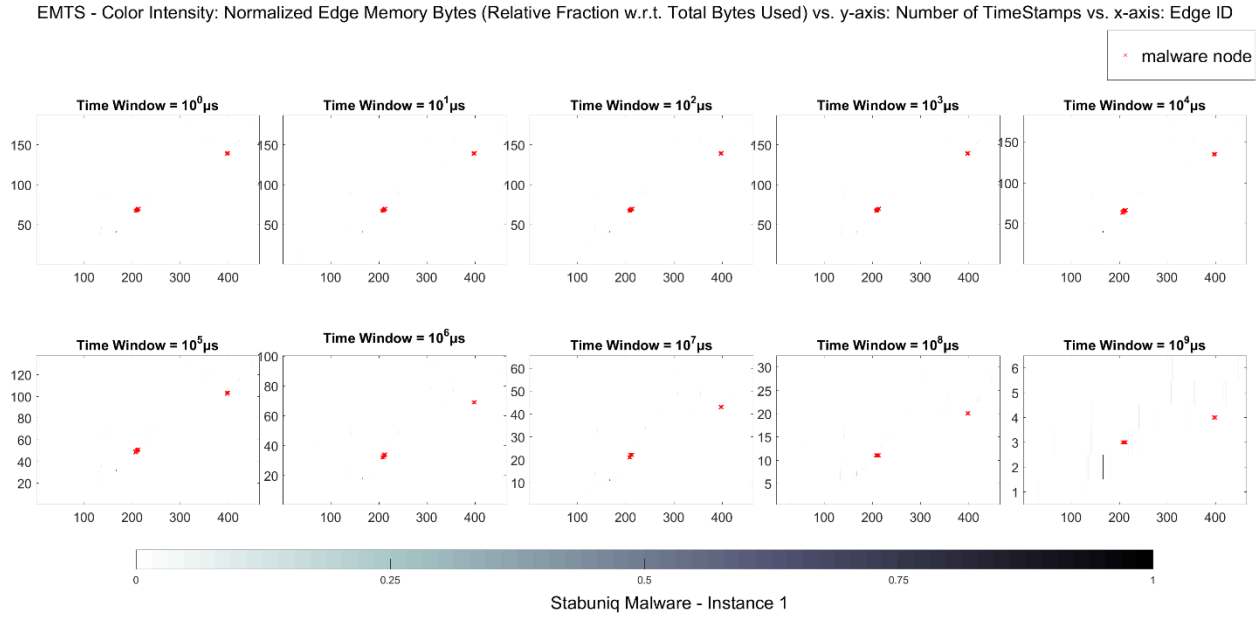
7.1.15 Stabuniq Malware – Instance 1

Time Graph Edge Based Features

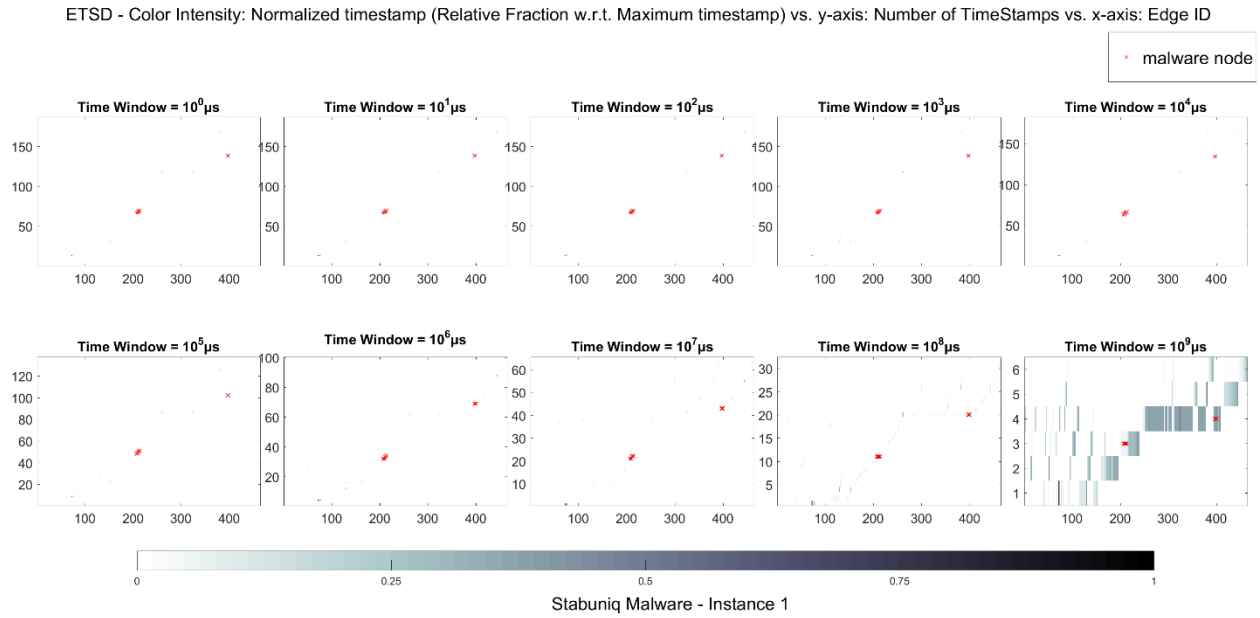
1) ECTS



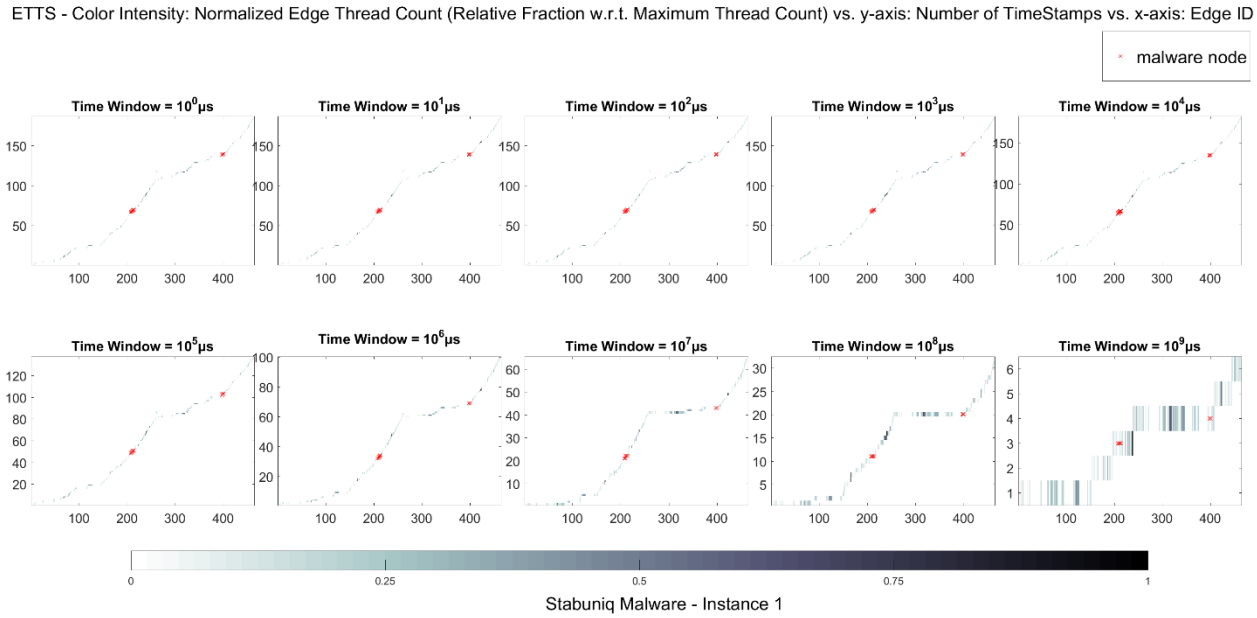
2) EMTS



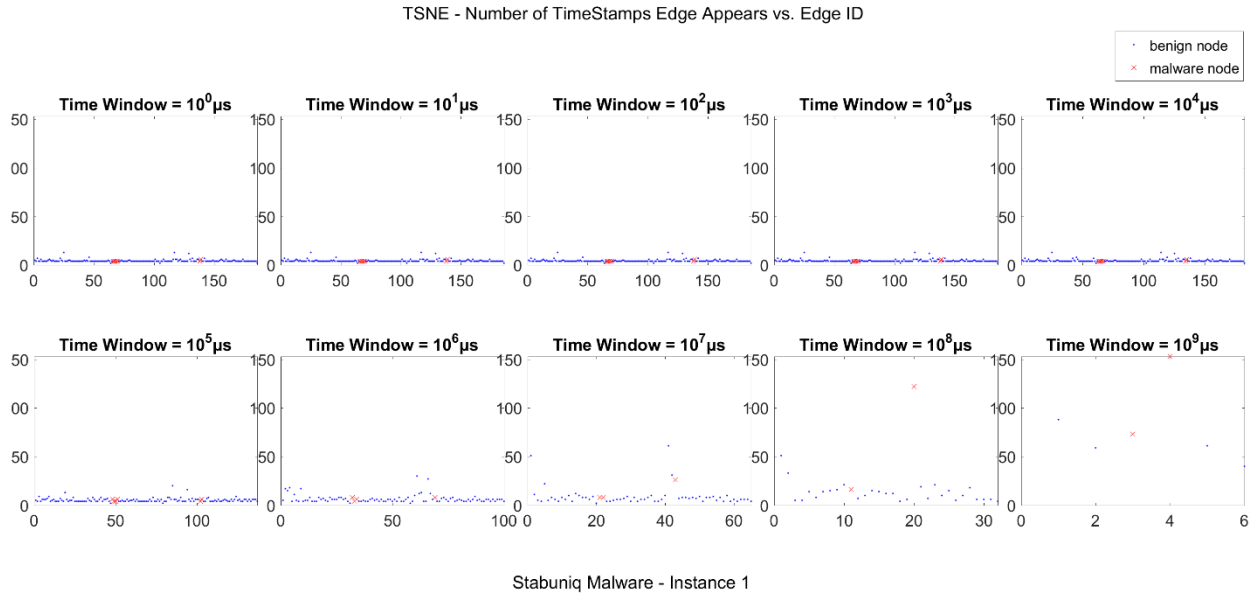
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Stabuniq Malware - Instance 1

4) ETTS

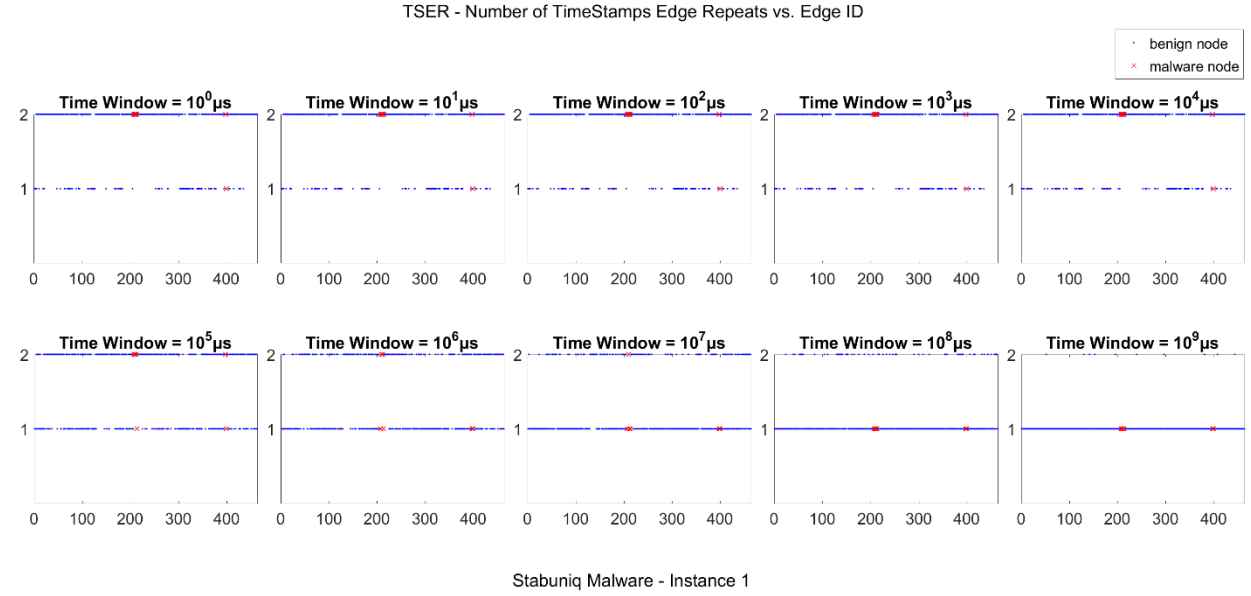

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Stabuniq Malware - Instance 1

5) TSNE



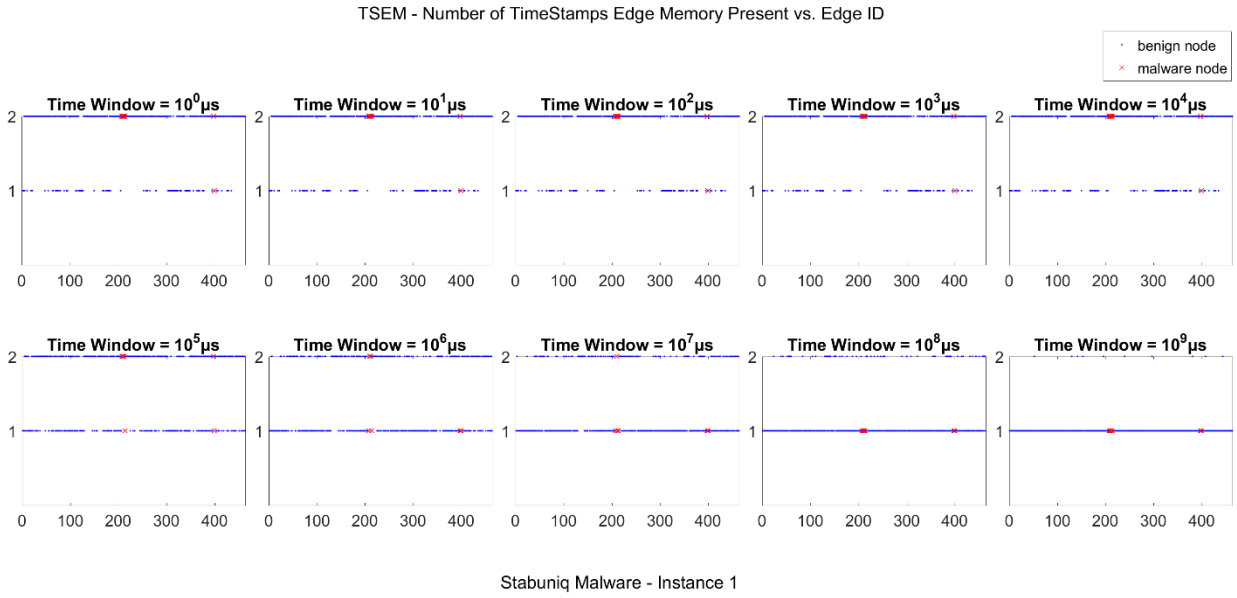
Stabuniq Malware - Instance 1

6) TSER

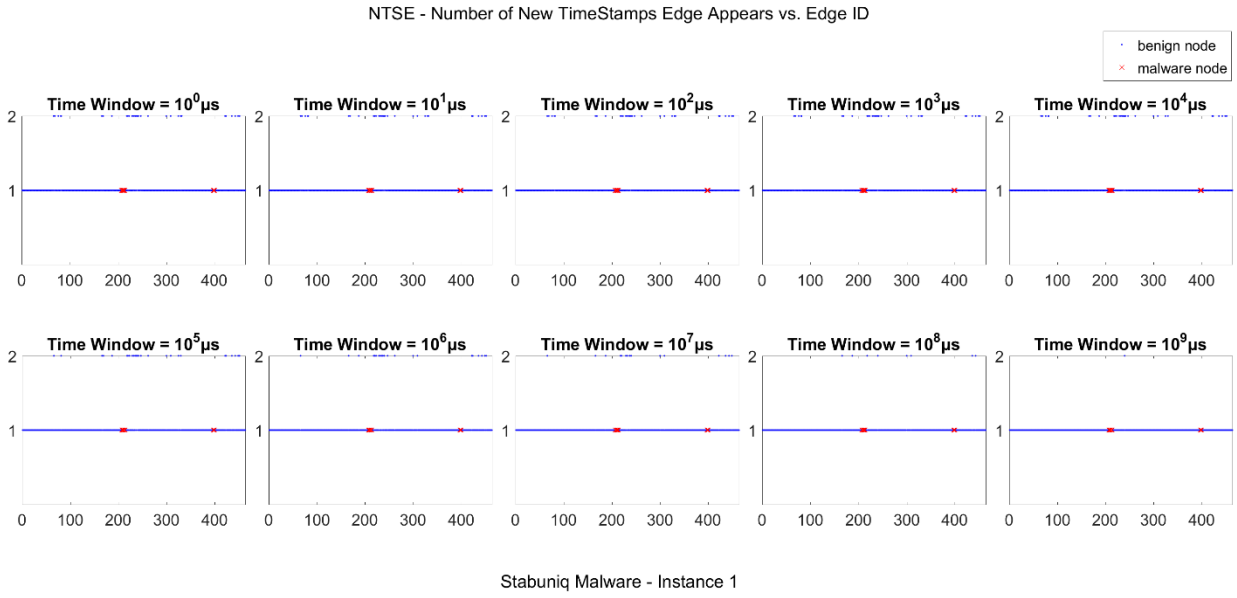


Stabuniq Malware - Instance 1

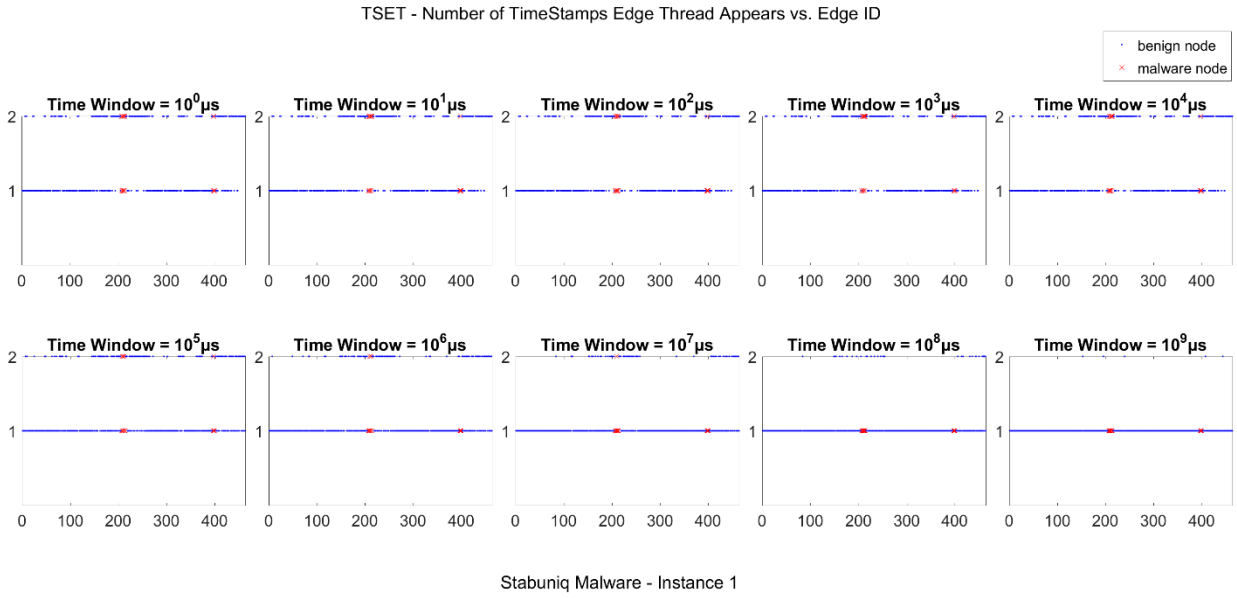
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Stabuniq Malware - Instance 1

8) NTSE

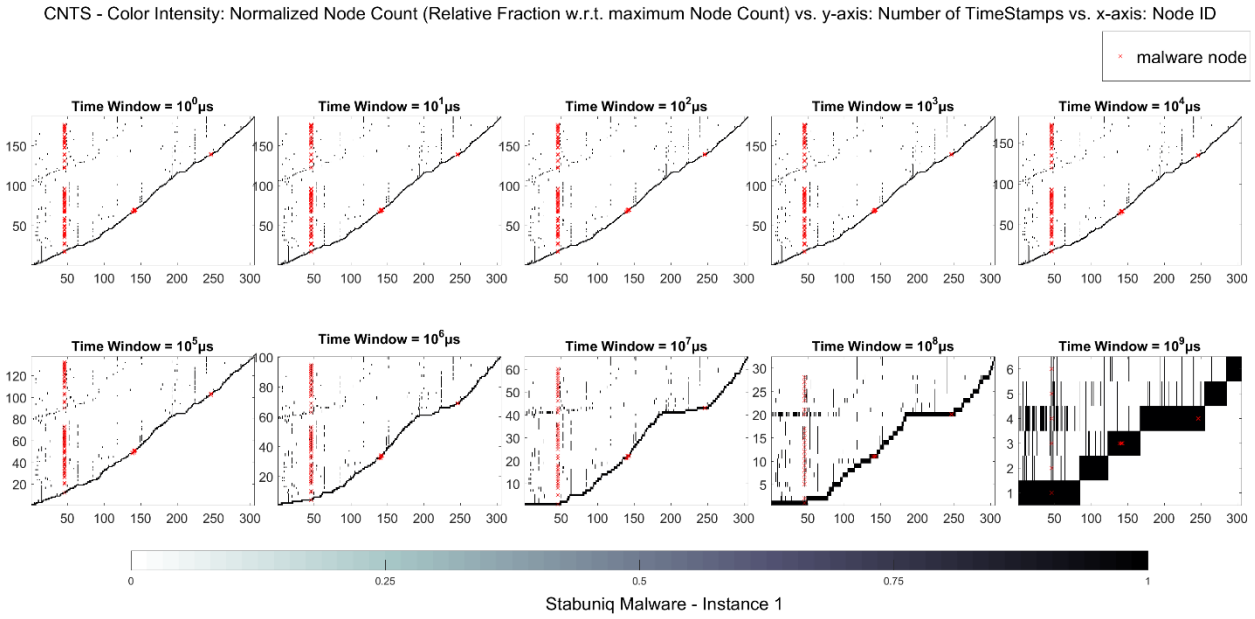

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Stabuniq Malware - Instance 1

9) TSET

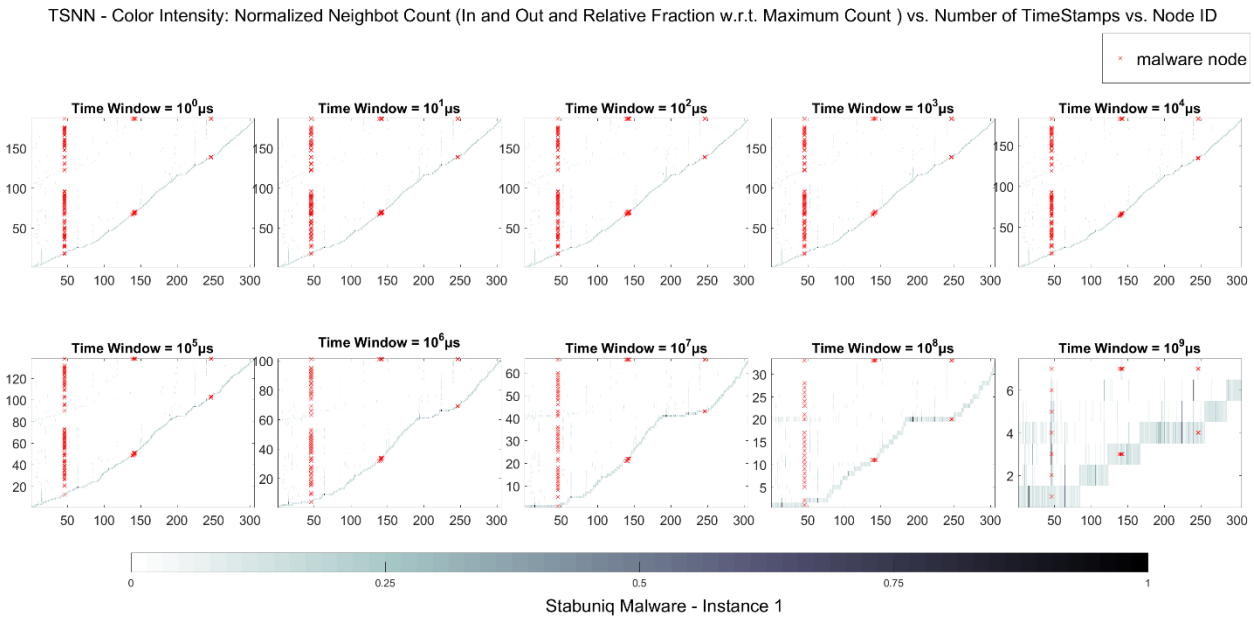


Time Graph Node Based Features

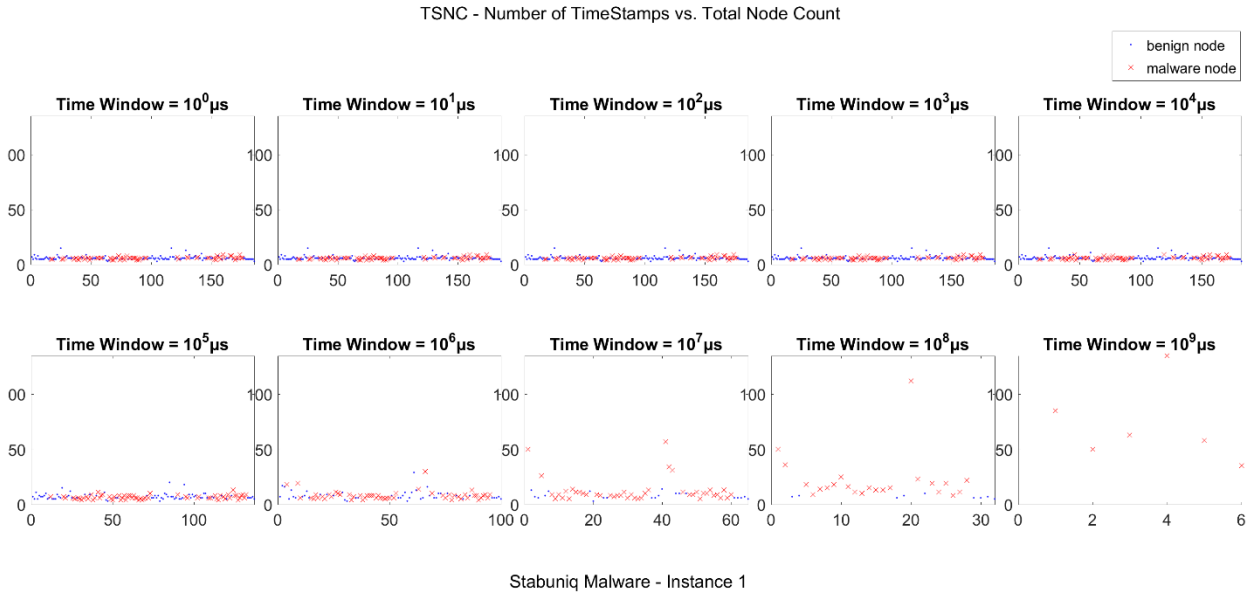
10) CNTS



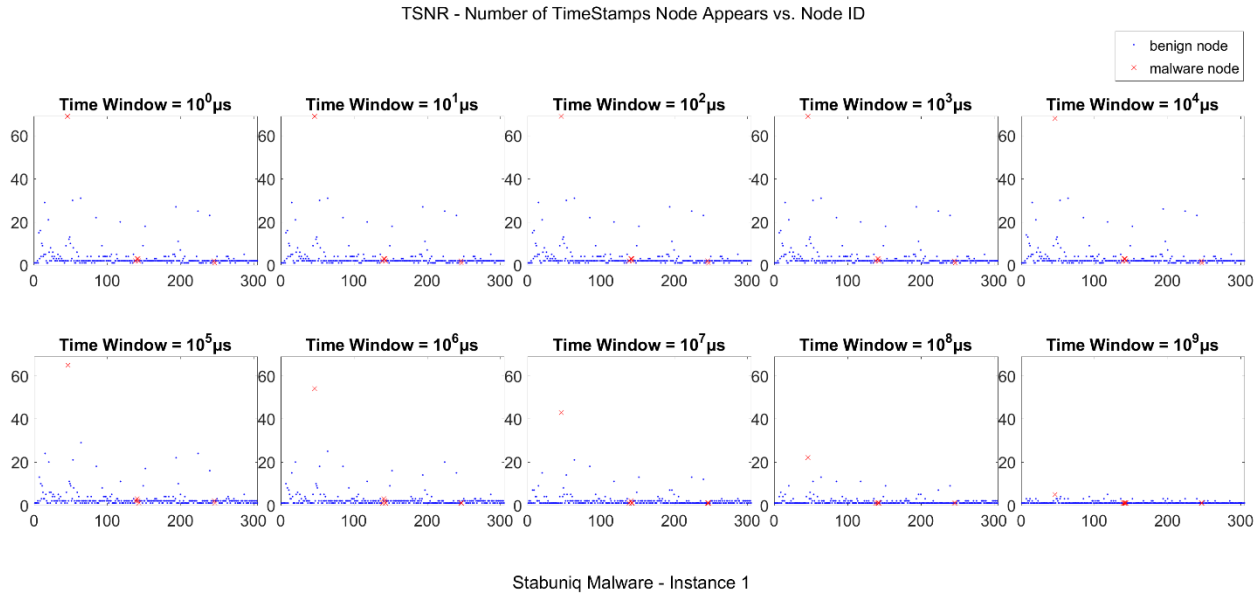
11) TSNN



12) TSNC



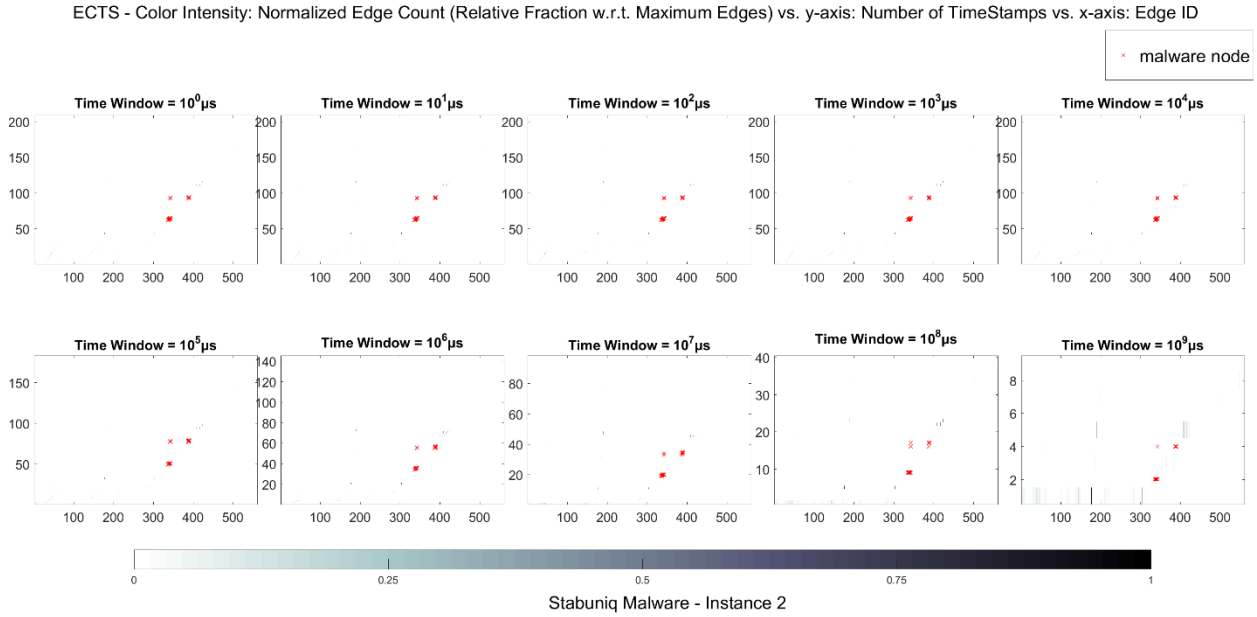
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
20
40
60
0
100
200
300
Stabuniq Malware - Instance 1

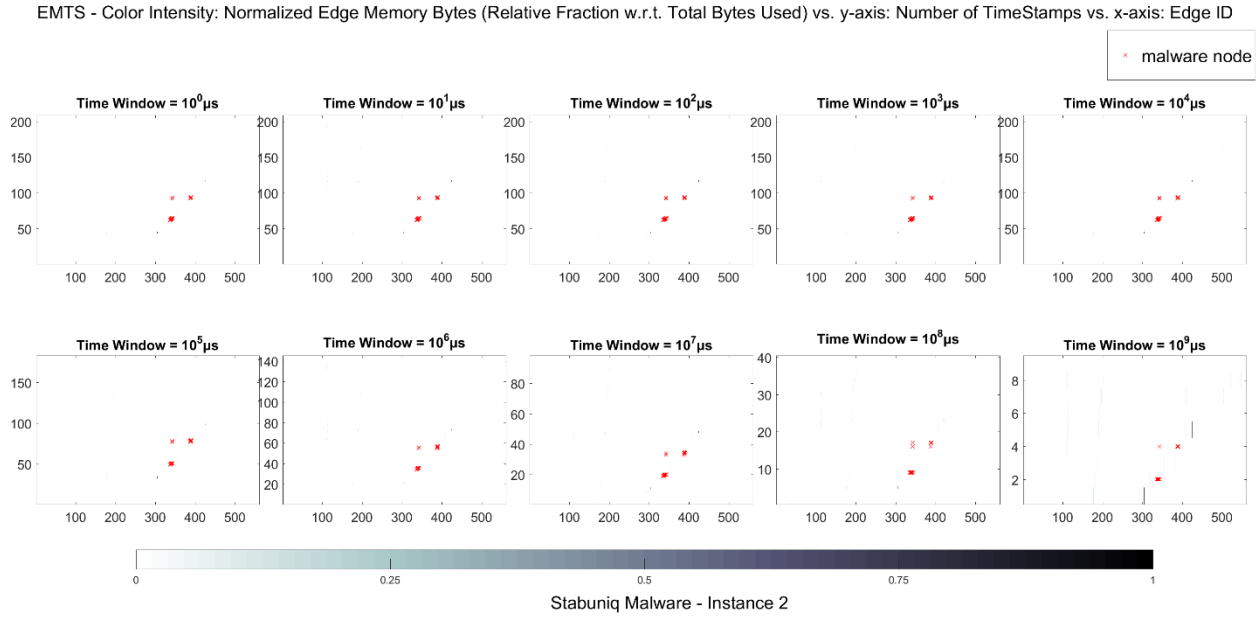
7.1.16 Stabuniq Malware – Instance 2

Time Graph Edge Based Features

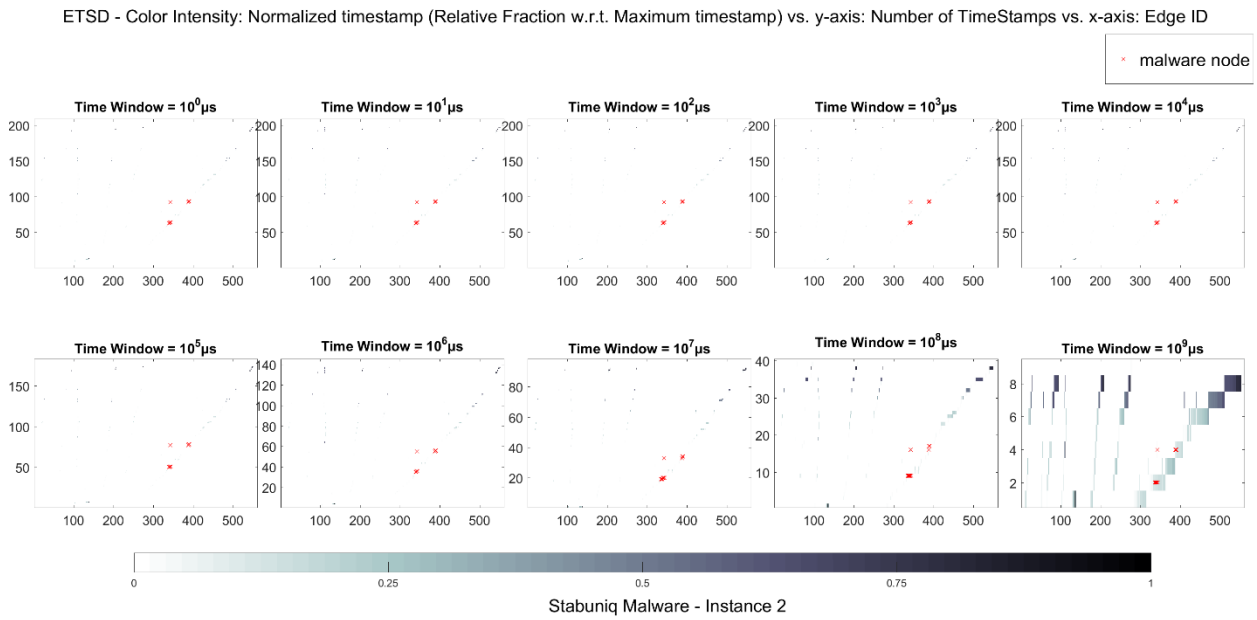
1) ECTS



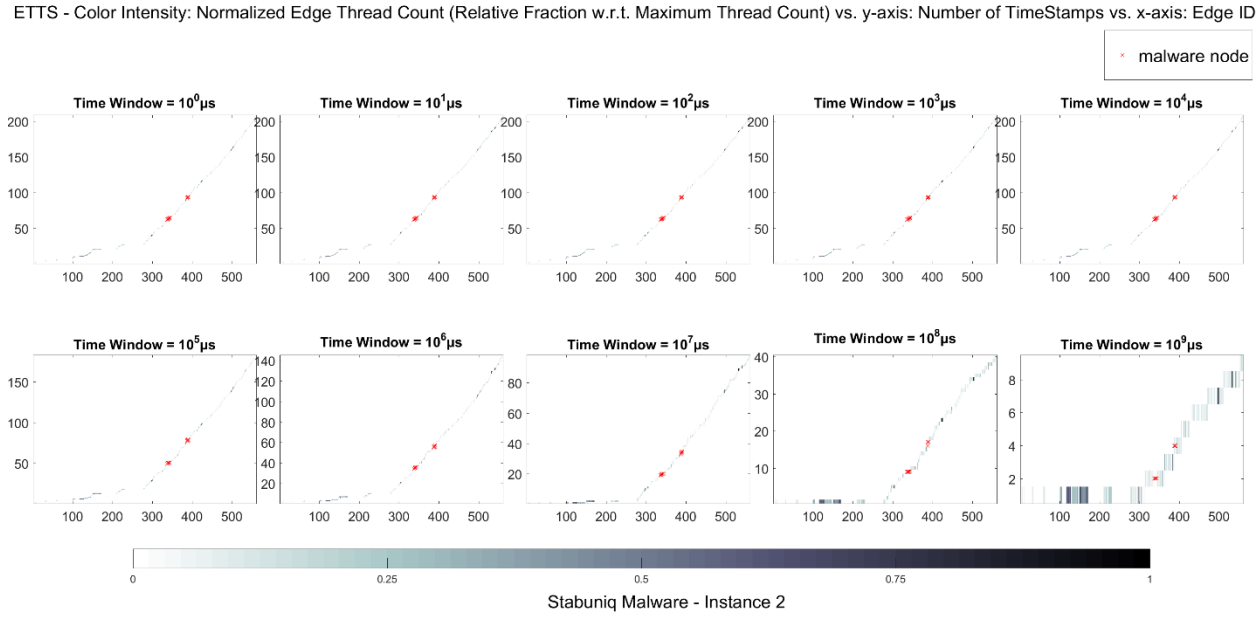
2) EMTS



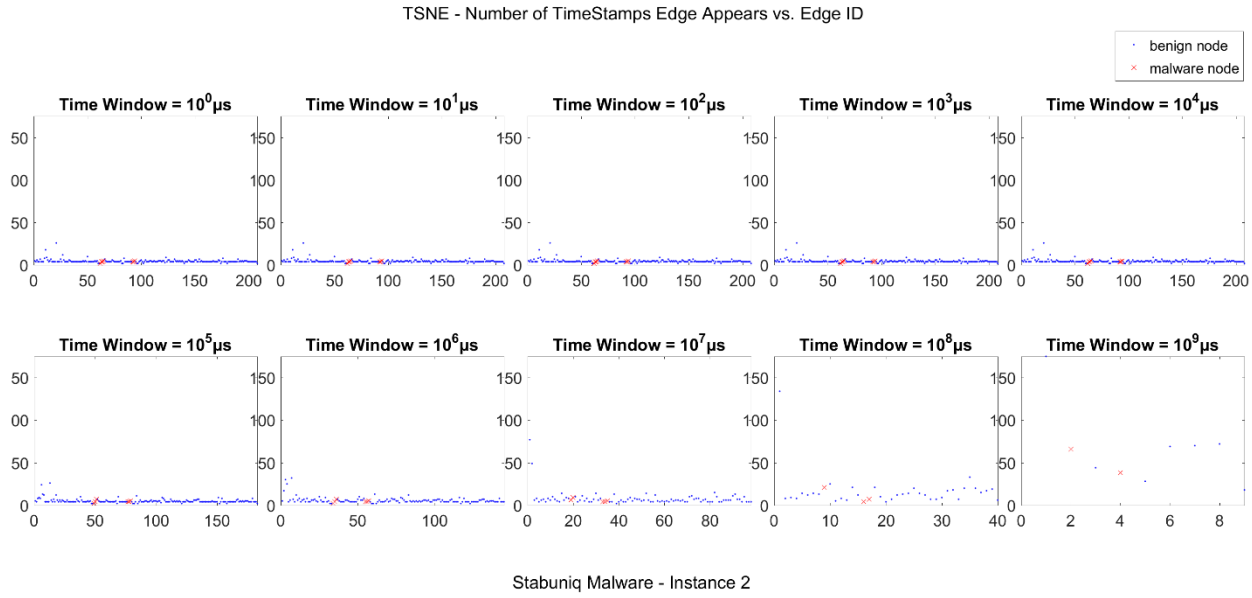
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Stabuniq Malware - Instance 2

4) ETTS

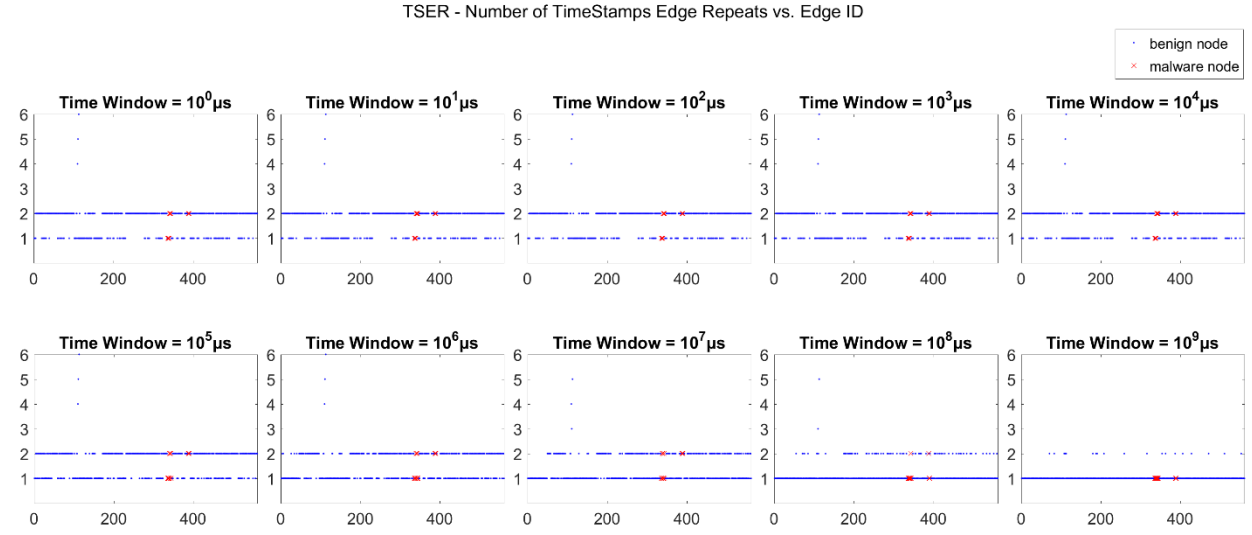

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Stabuniq Malware - Instance 2

5) TSNE



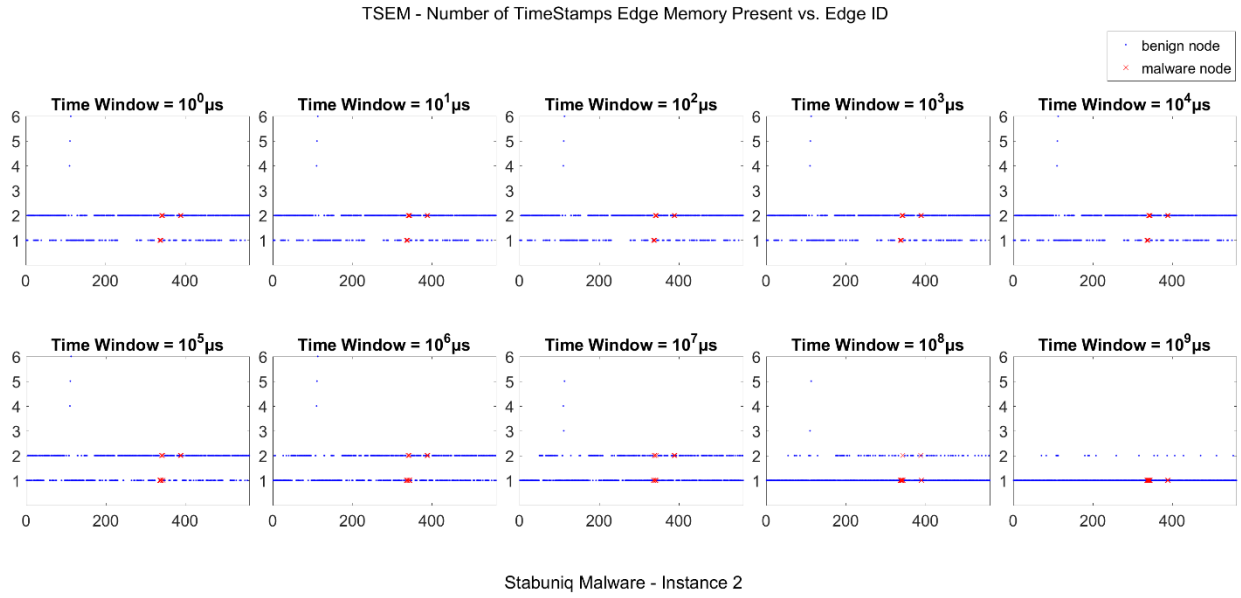
Stabuniq Malware - Instance 2

6) TSER

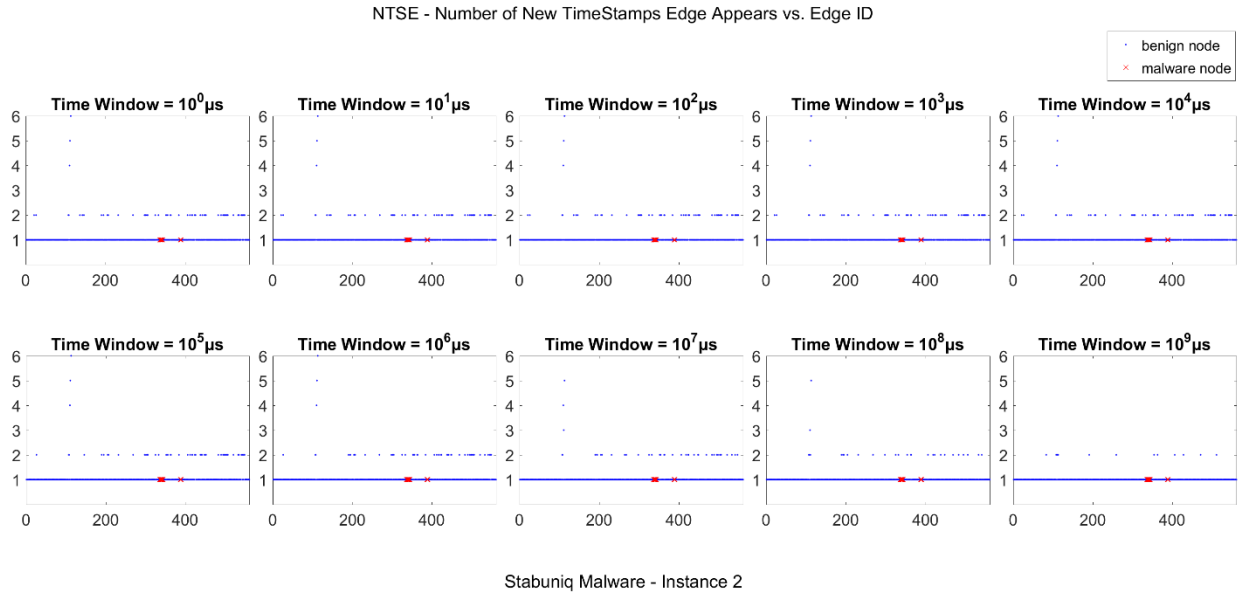


Stabuniq Malware - Instance 2

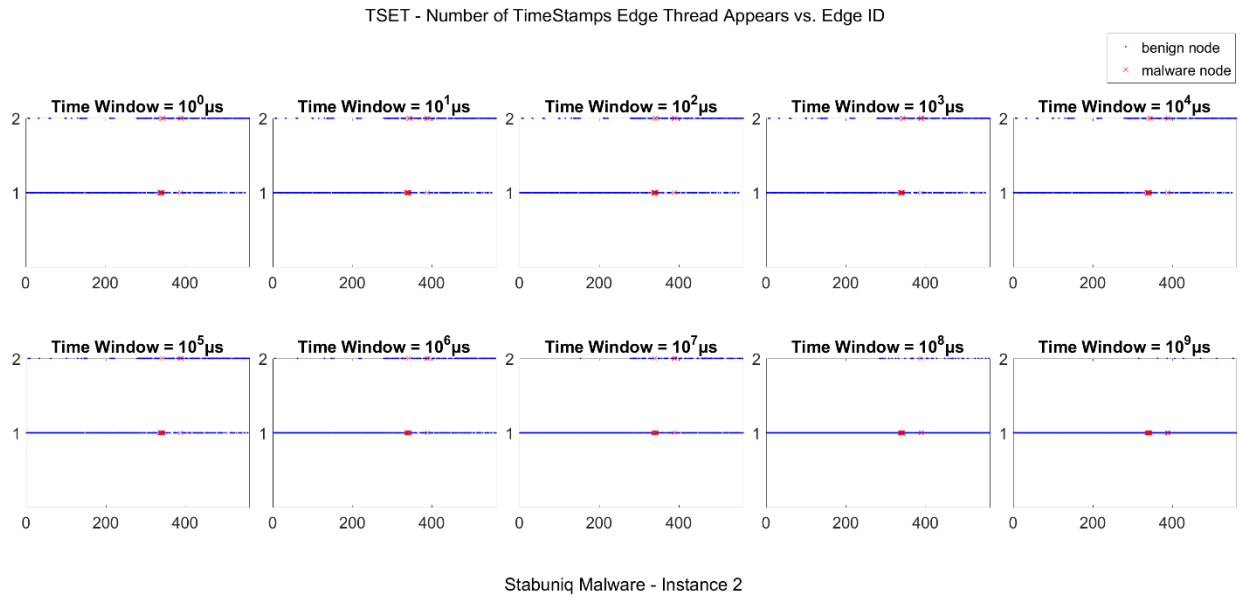
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Stabuniq Malware - Instance 2

8) NTSE

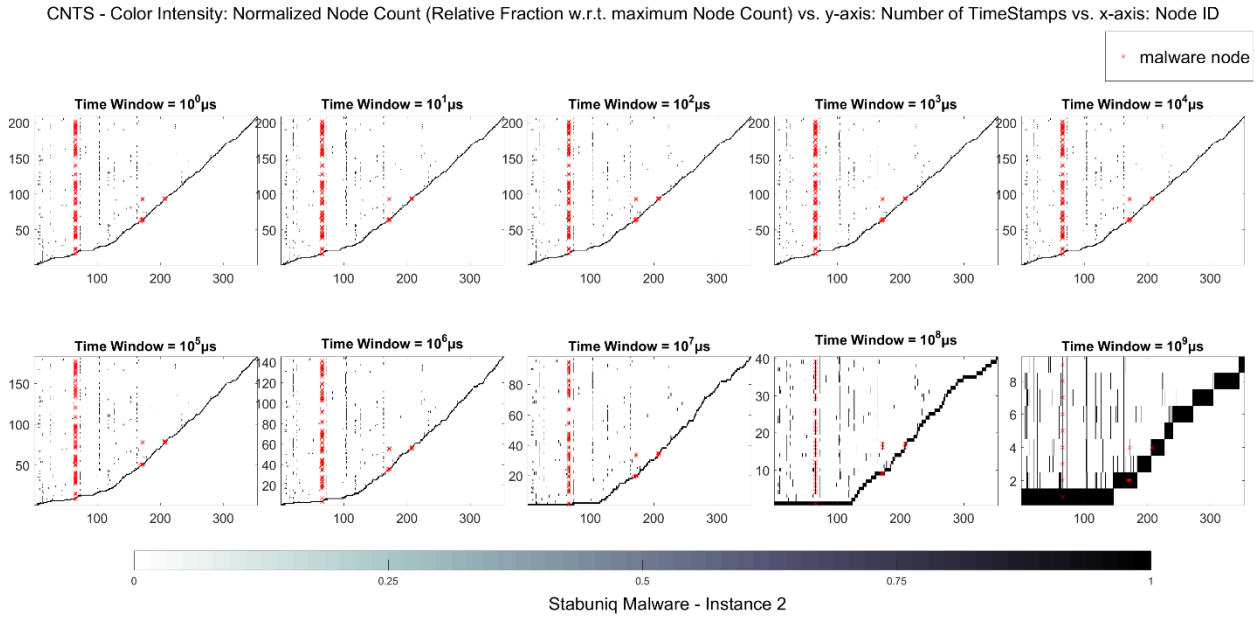

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Stabuniq Malware - Instance 2

9) TSET

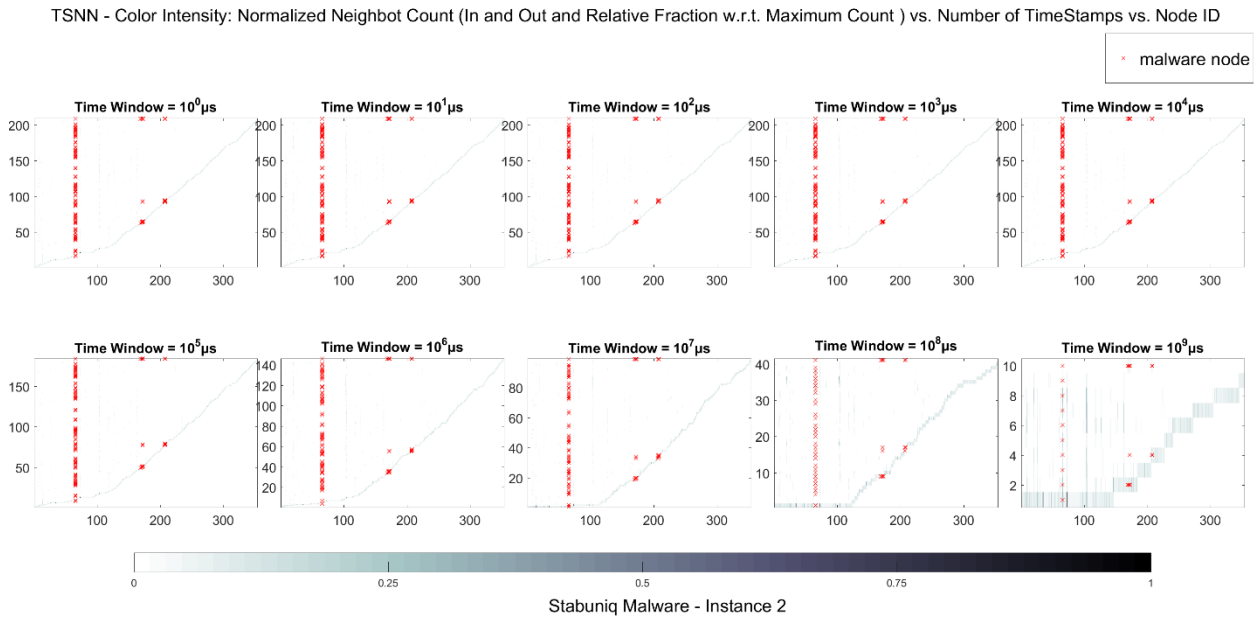


Time Graph Node Based Features

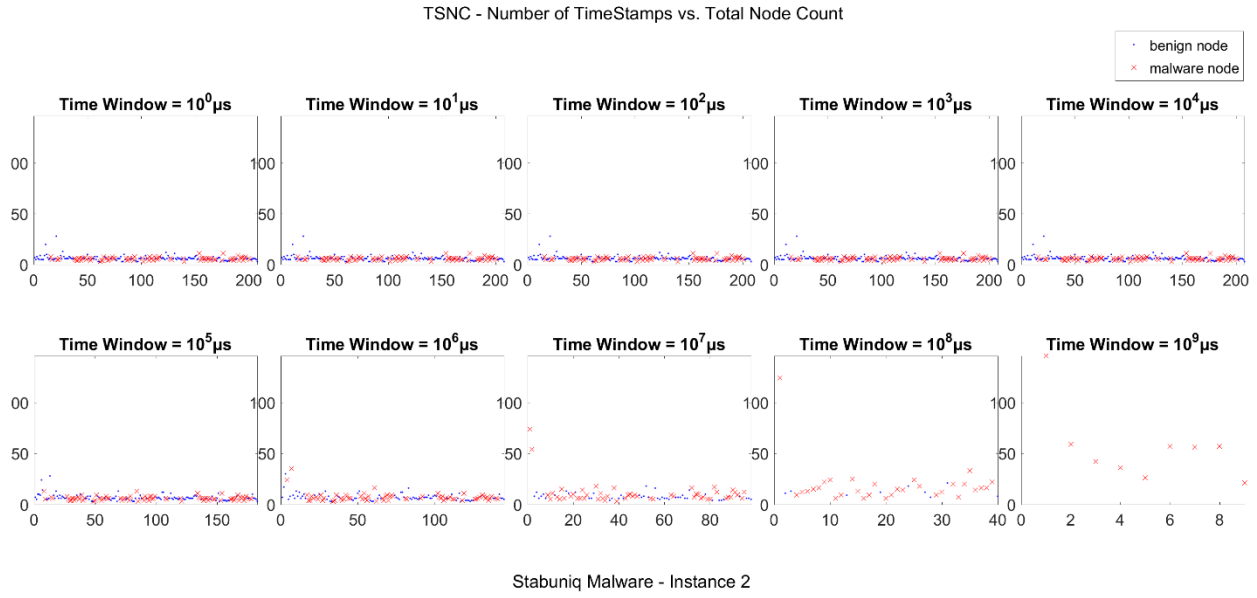
10) CNTS



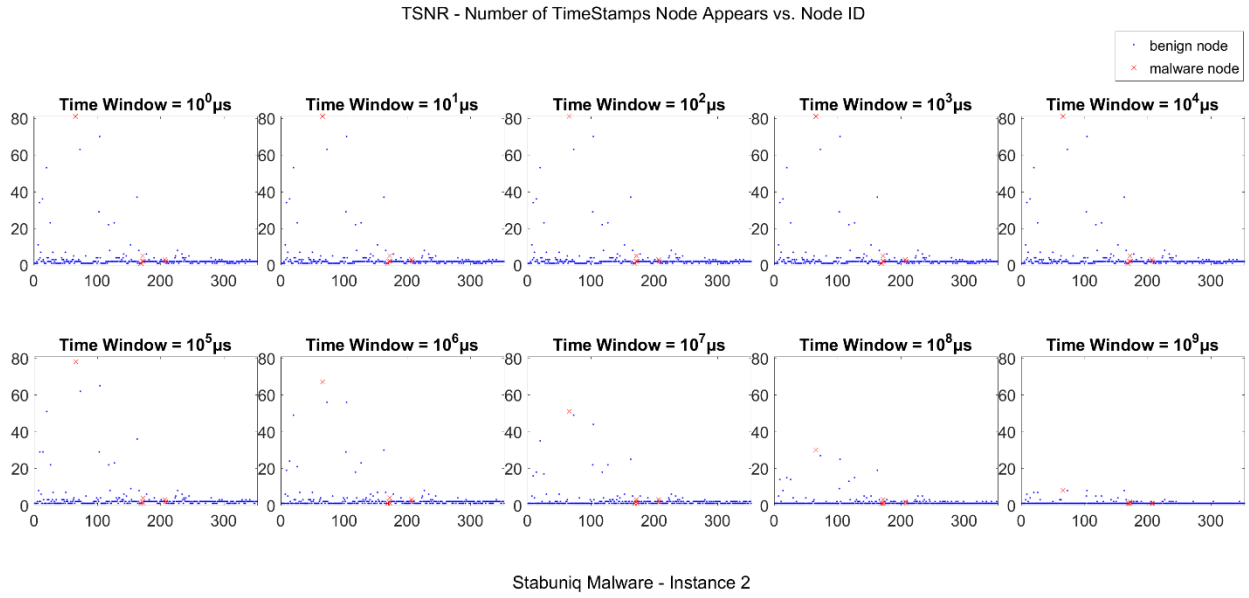
11) TSNN



12) TSNC



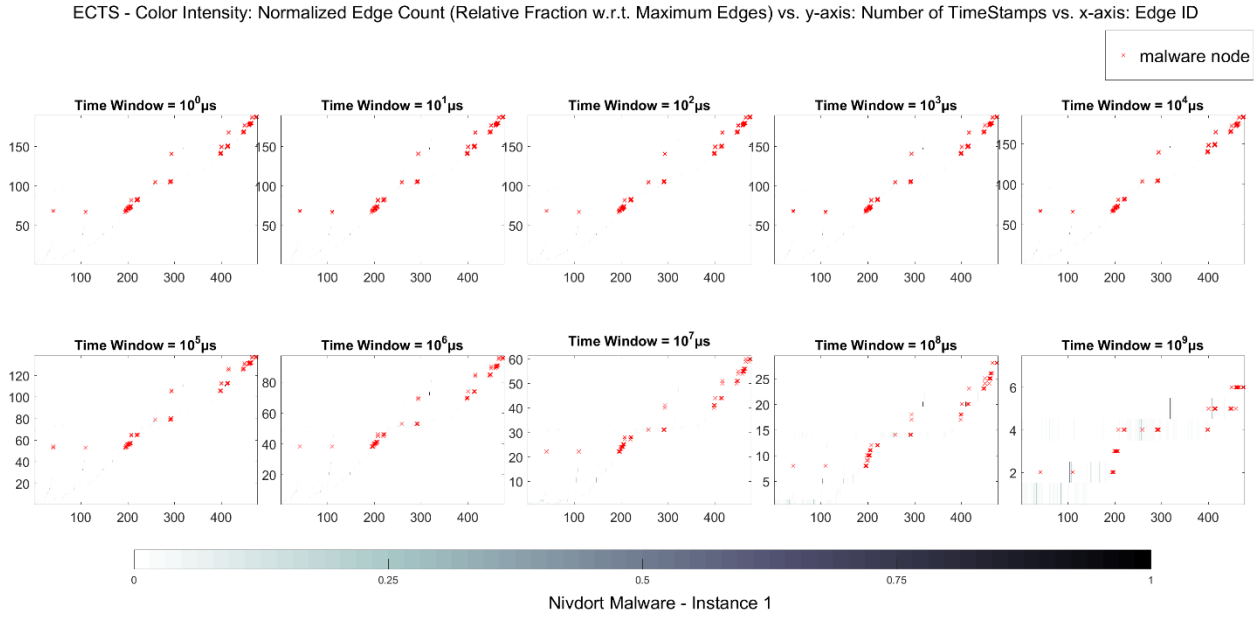
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Stabuniq Malware - Instance 2

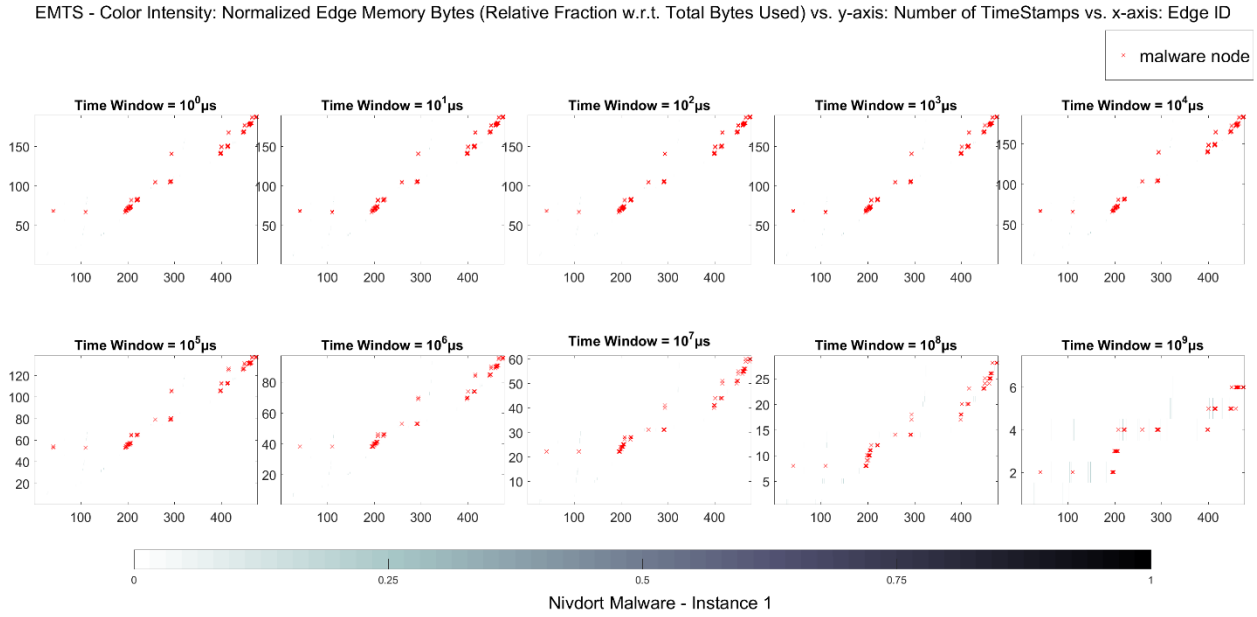
7.1.17 Nivdort Malware – Instance 1

Time Graph Edge Based Features

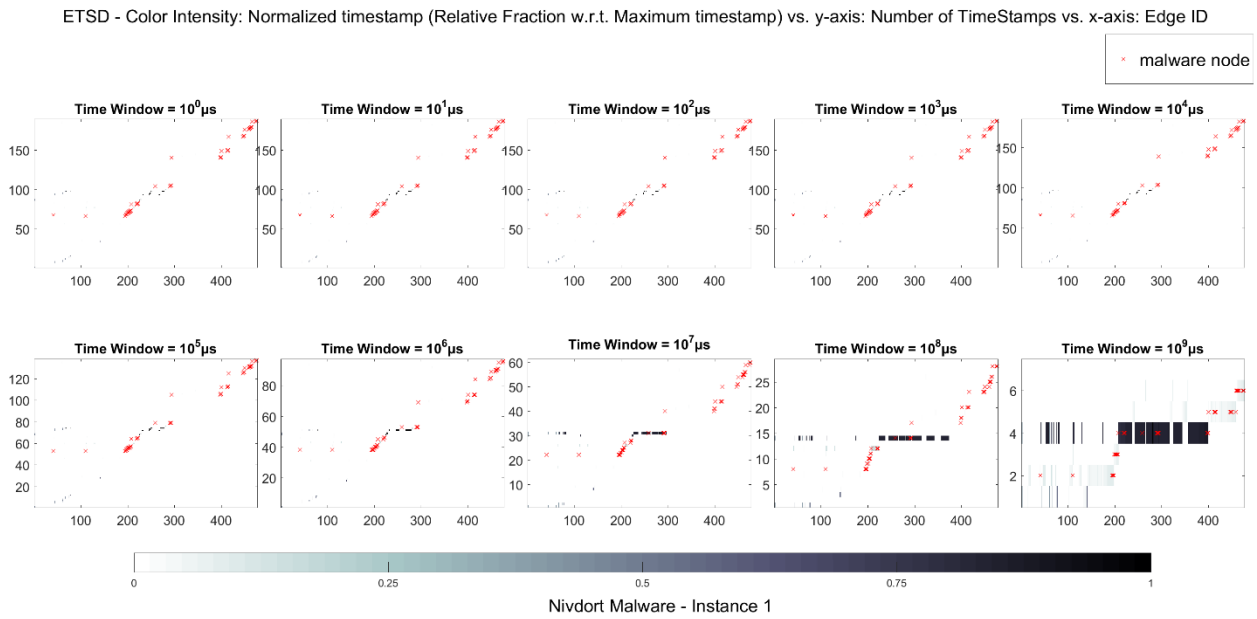
1) ECTS



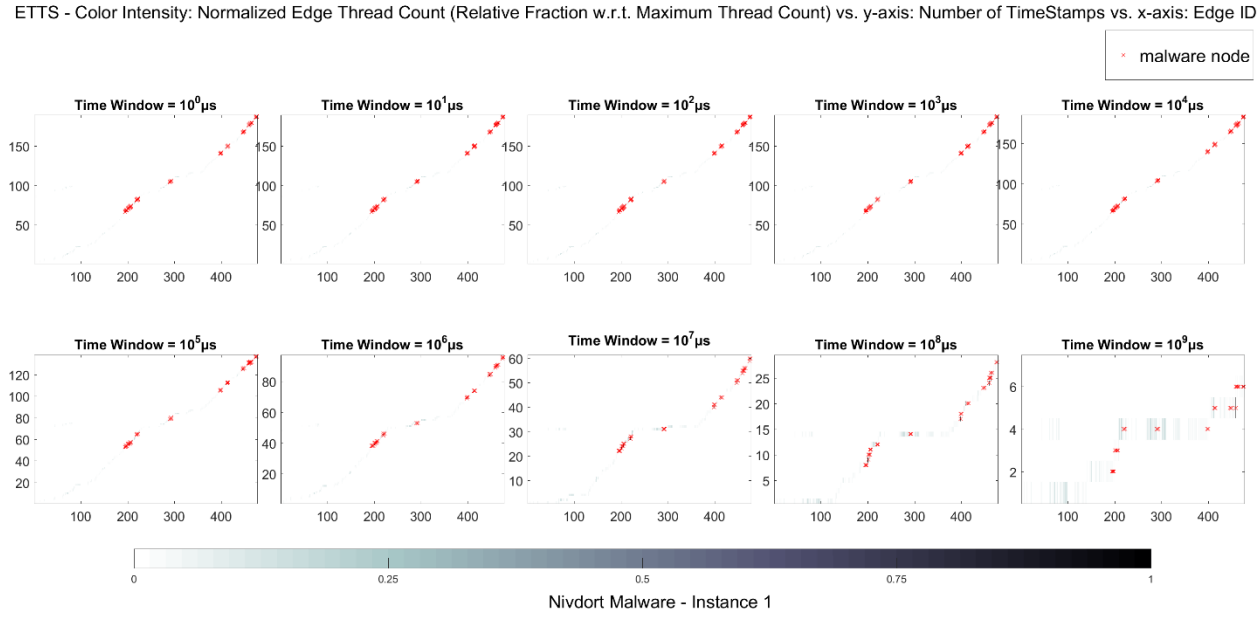
2) EMTS



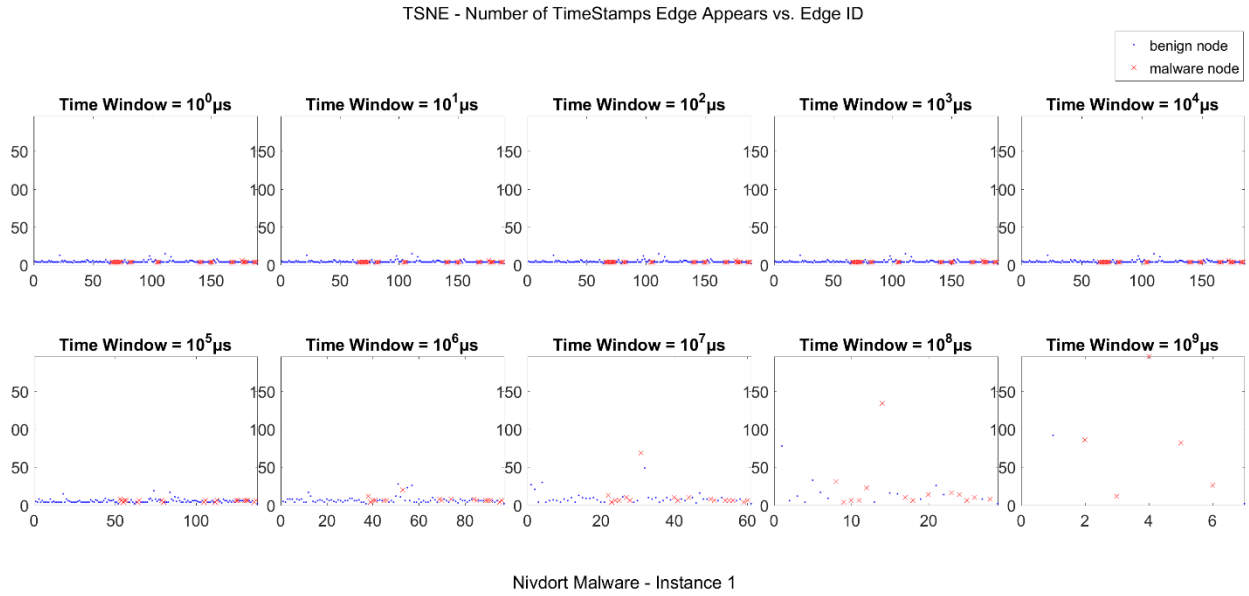
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Nivdort Malware - Instance 1

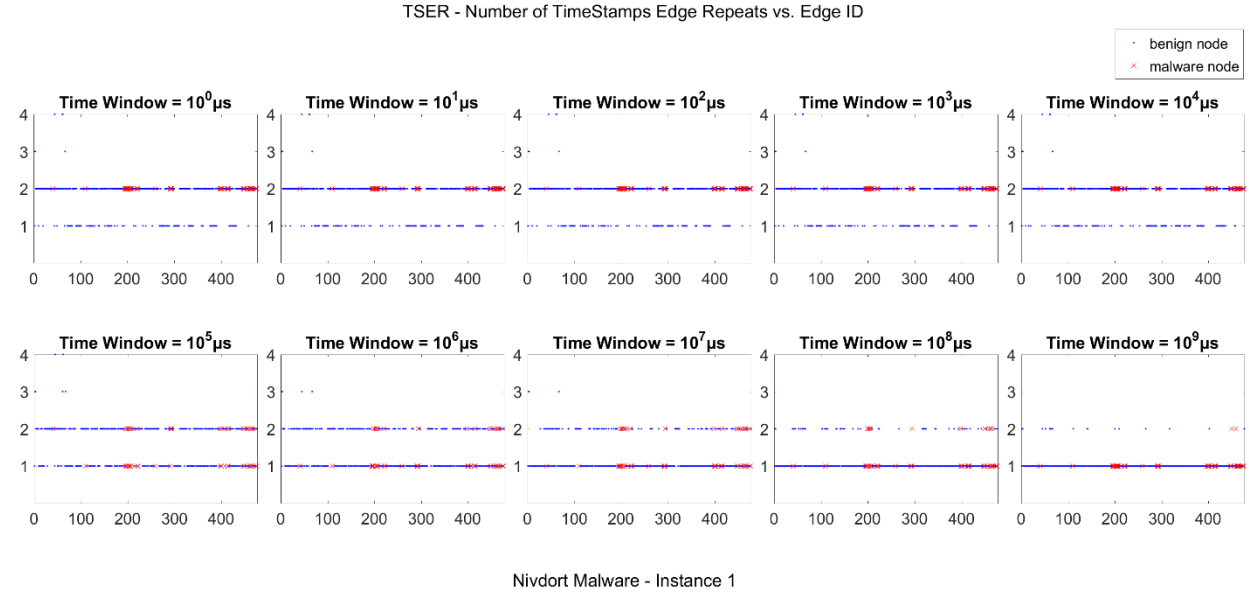
4) ETTS


ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Nivdort Malware - Instance 1

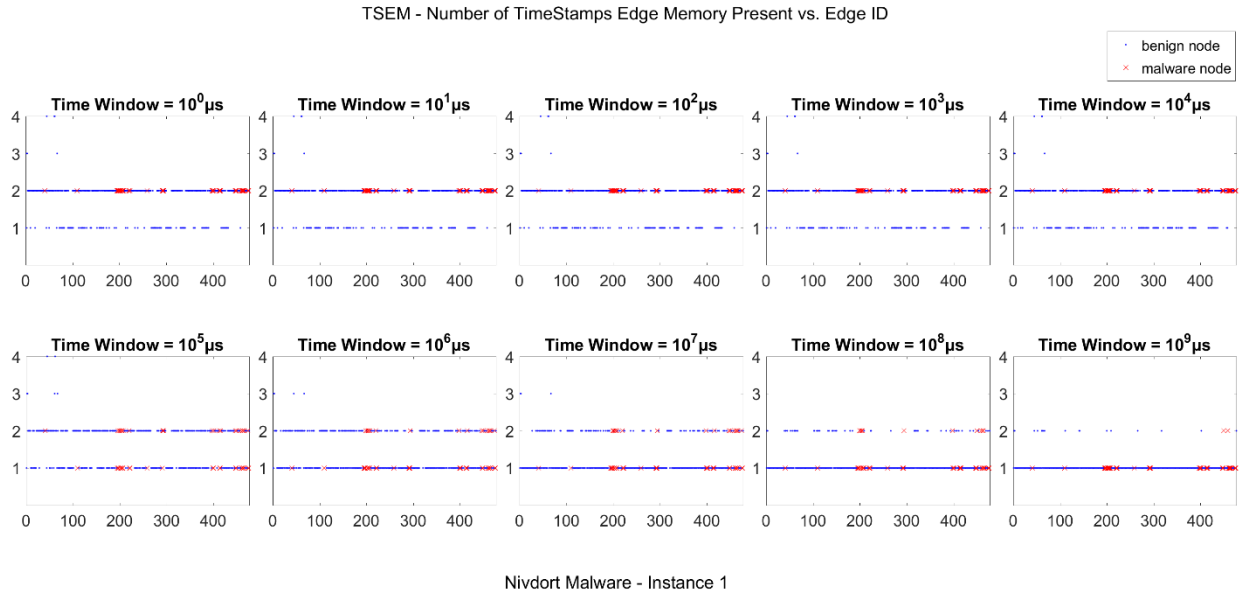
5) TSNE


TSNE - Number of TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Nivdort Malware - Instance 1

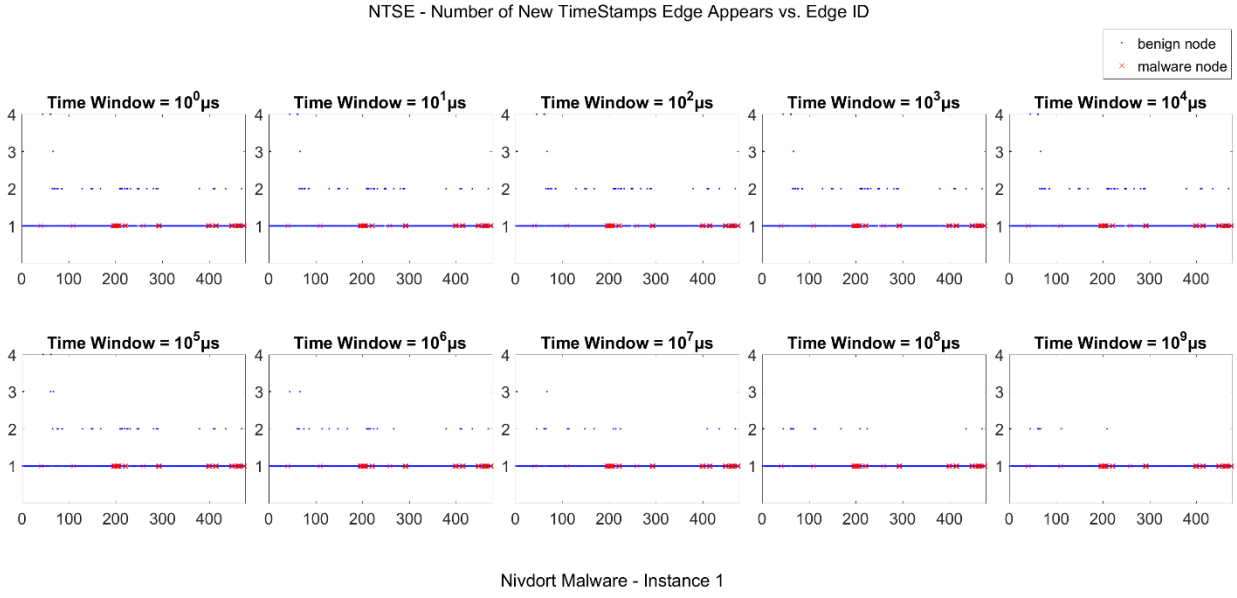
6) TSER


TSER - Number of TimeStamps Edge Repeats vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Nivdort Malware - Instance 1

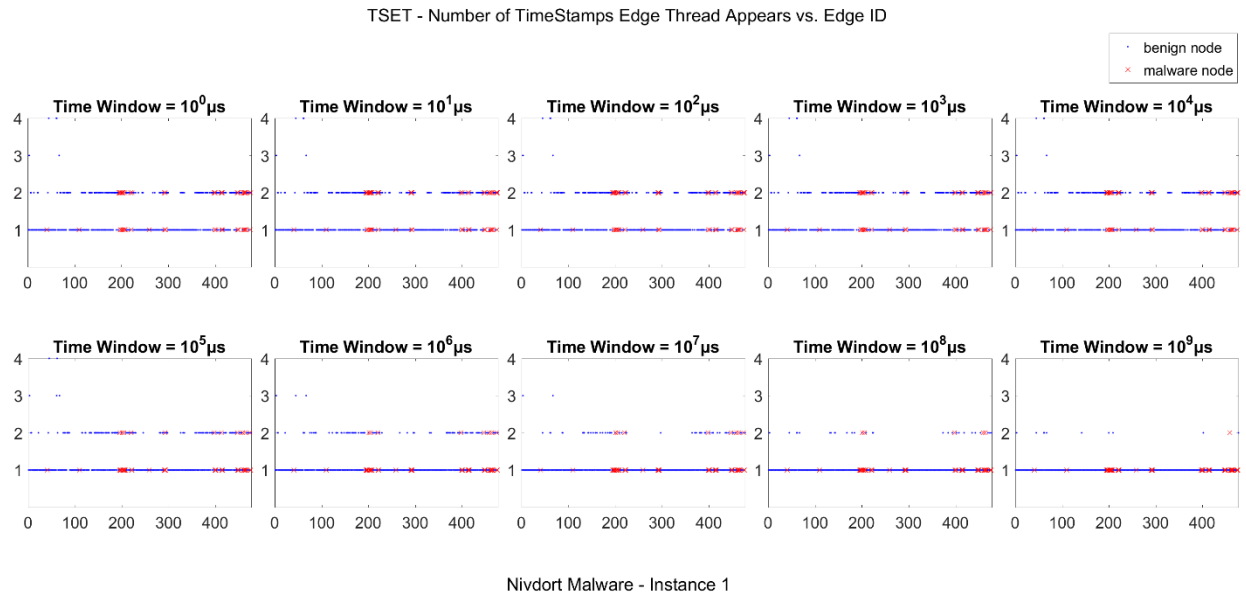
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Nivdort Malware - Instance 1

8) NTSE

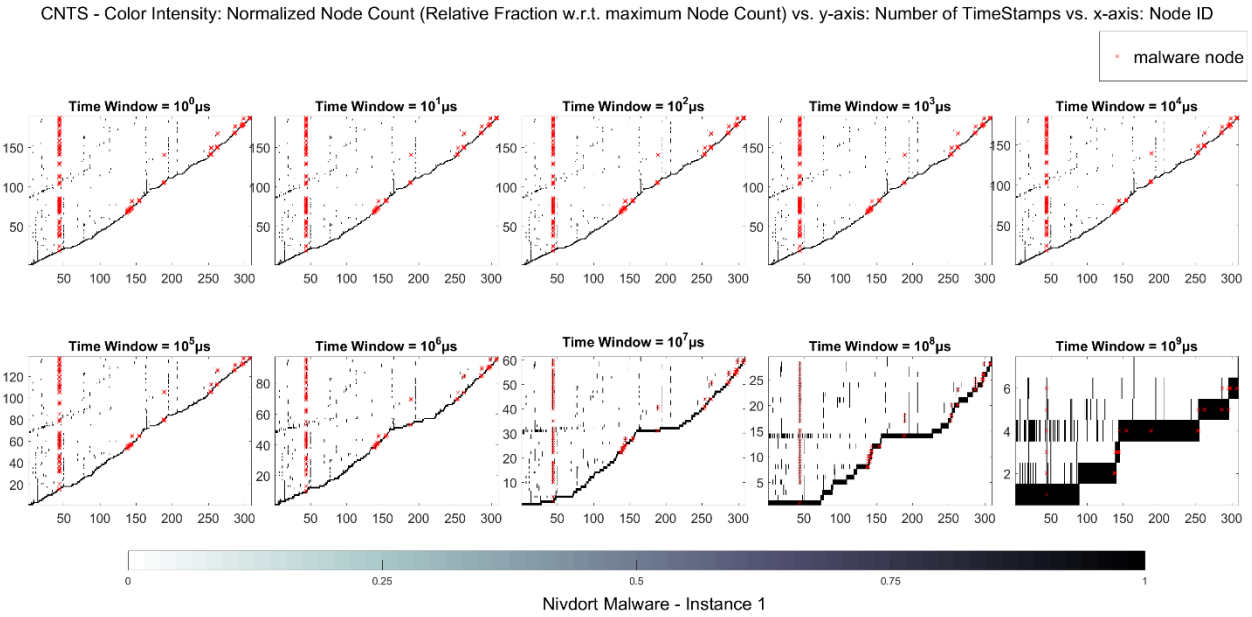

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Nivdort Malware - Instance 1

9) TSET

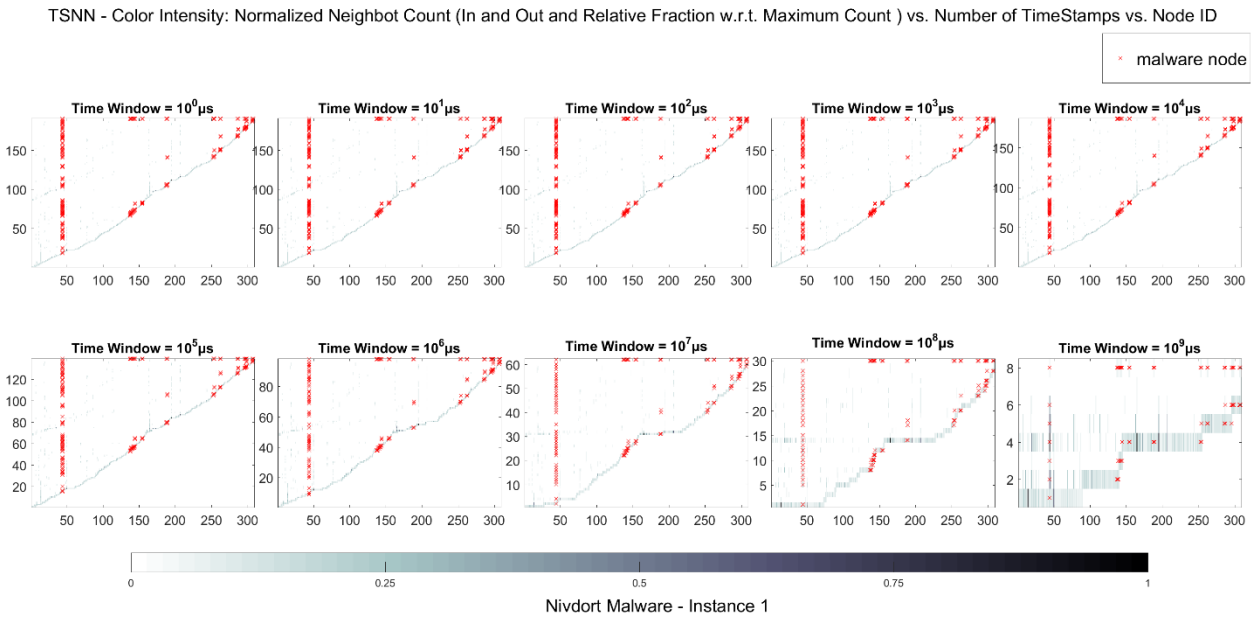


Time Graph Node Based Features

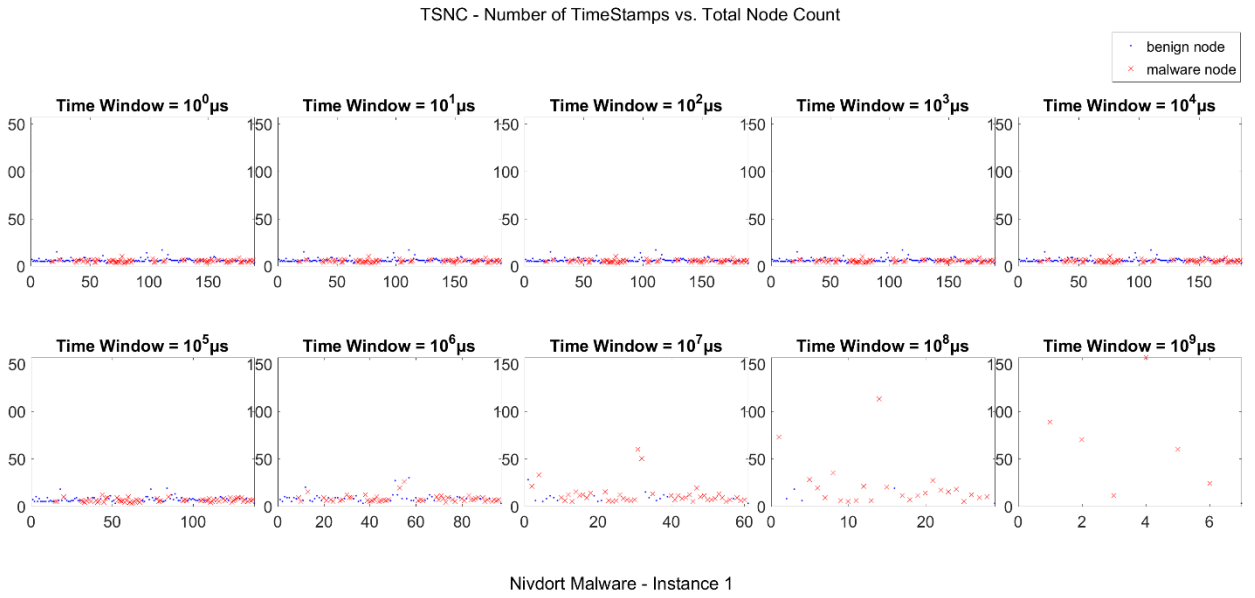
10) CNTS



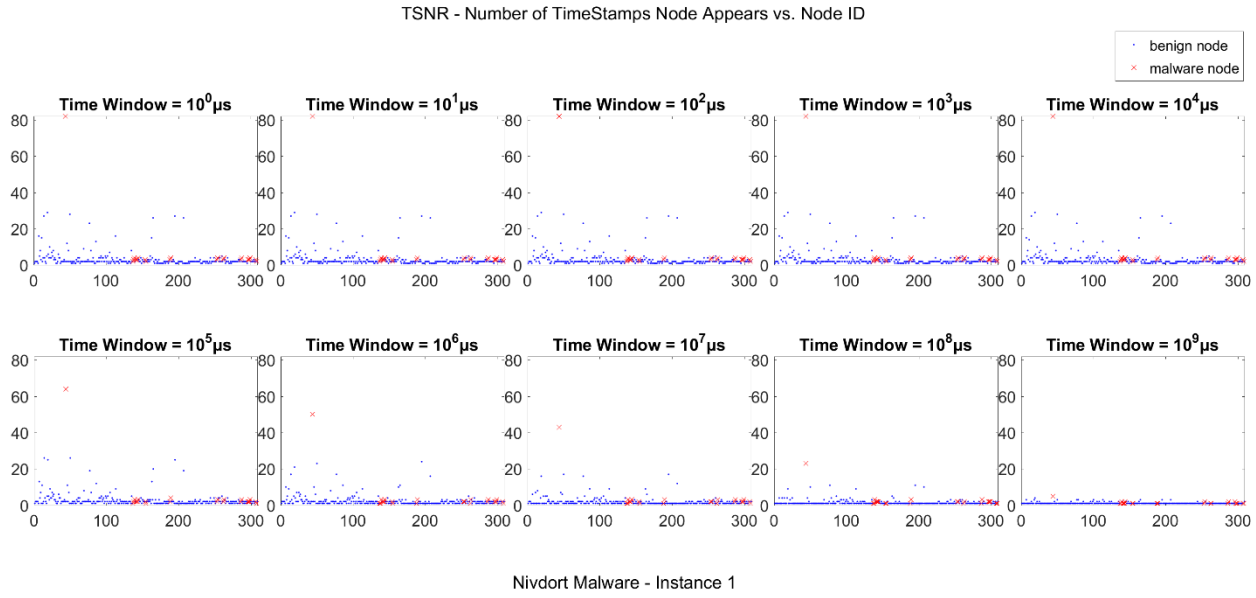
11) TSNN



12) TSNC



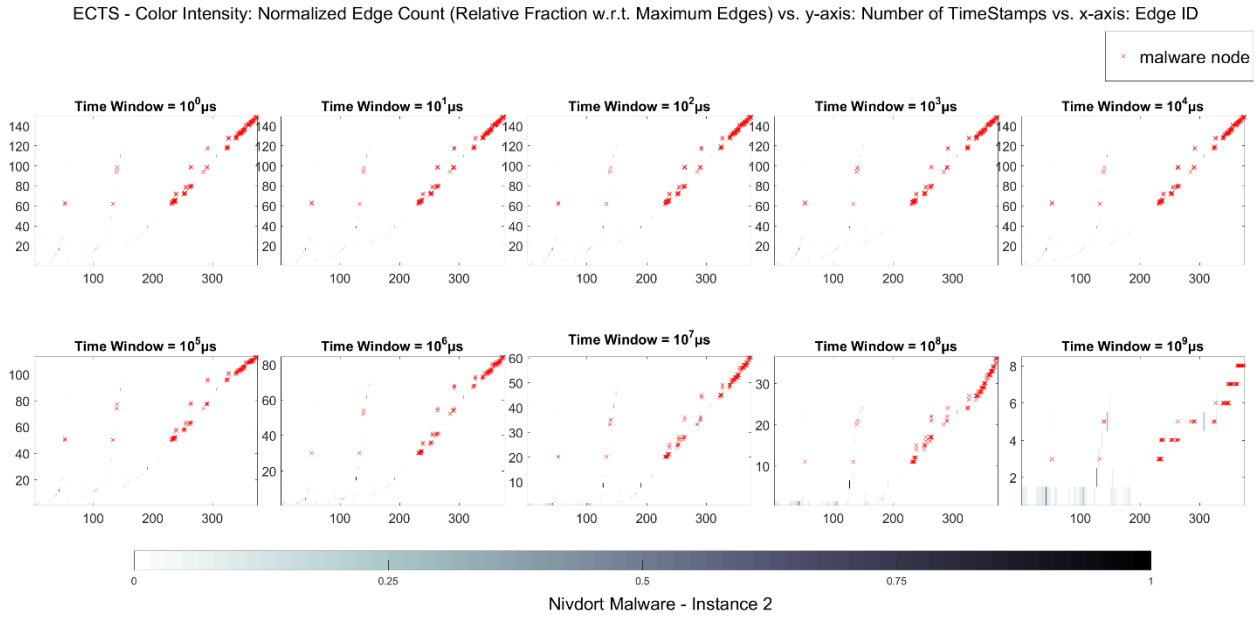
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Nivdort Malware - Instance 1

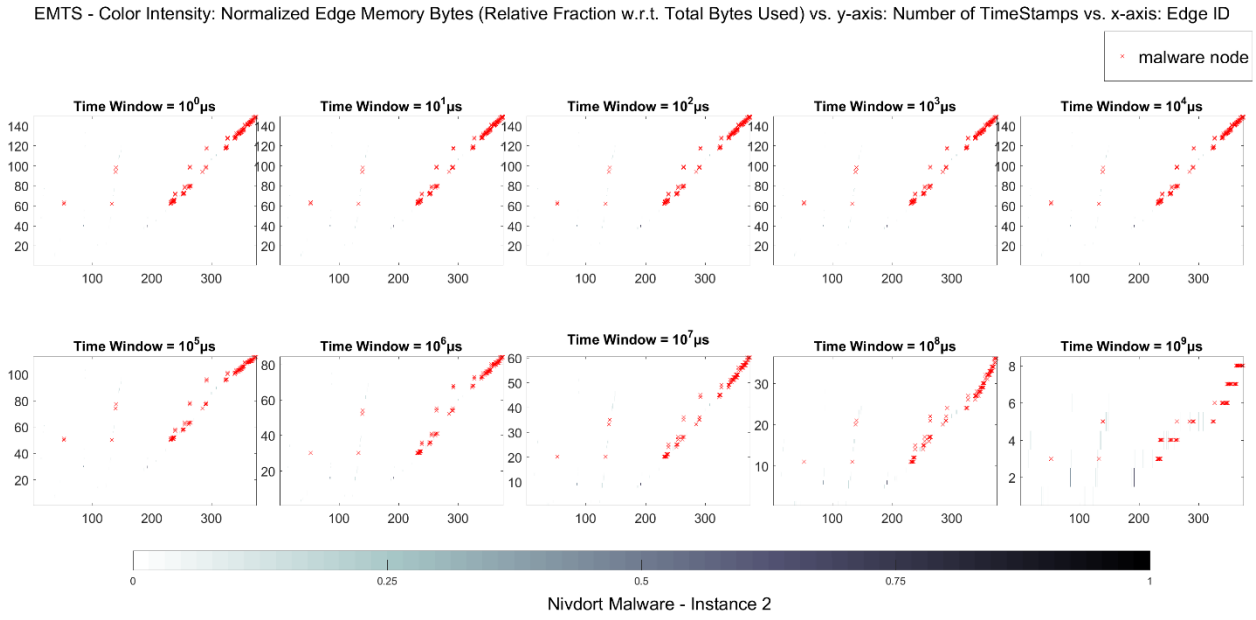
7.1.18 Nivdort Malware – Instance 2

Time Graph Edge Based Features

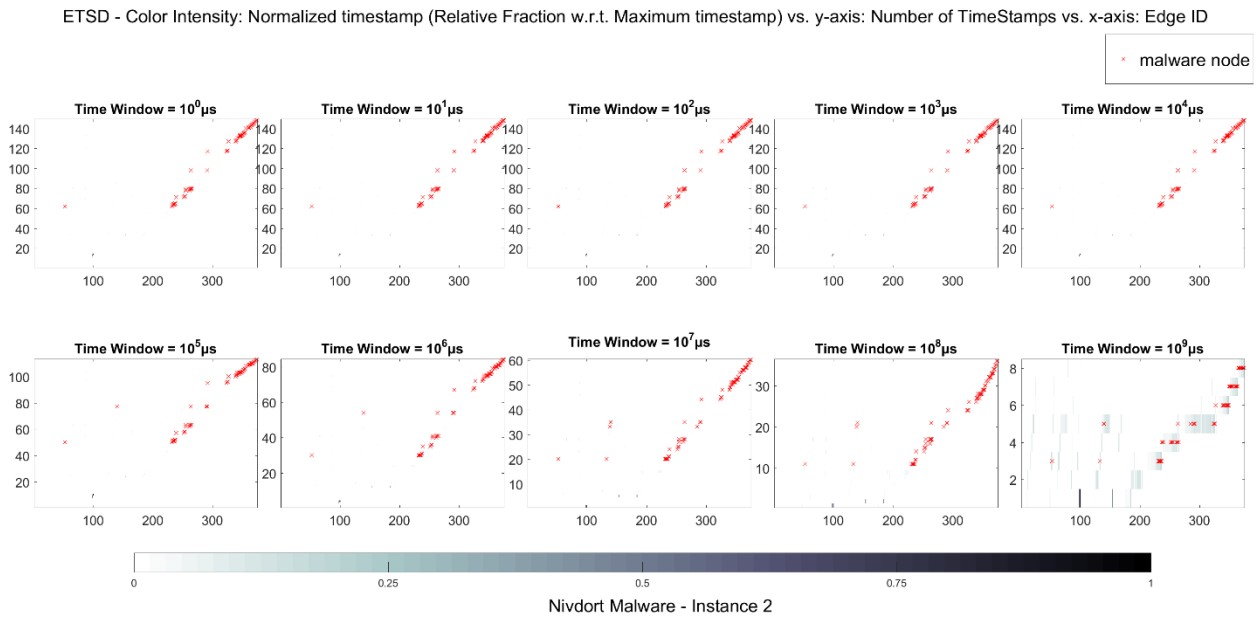
1) ECTS



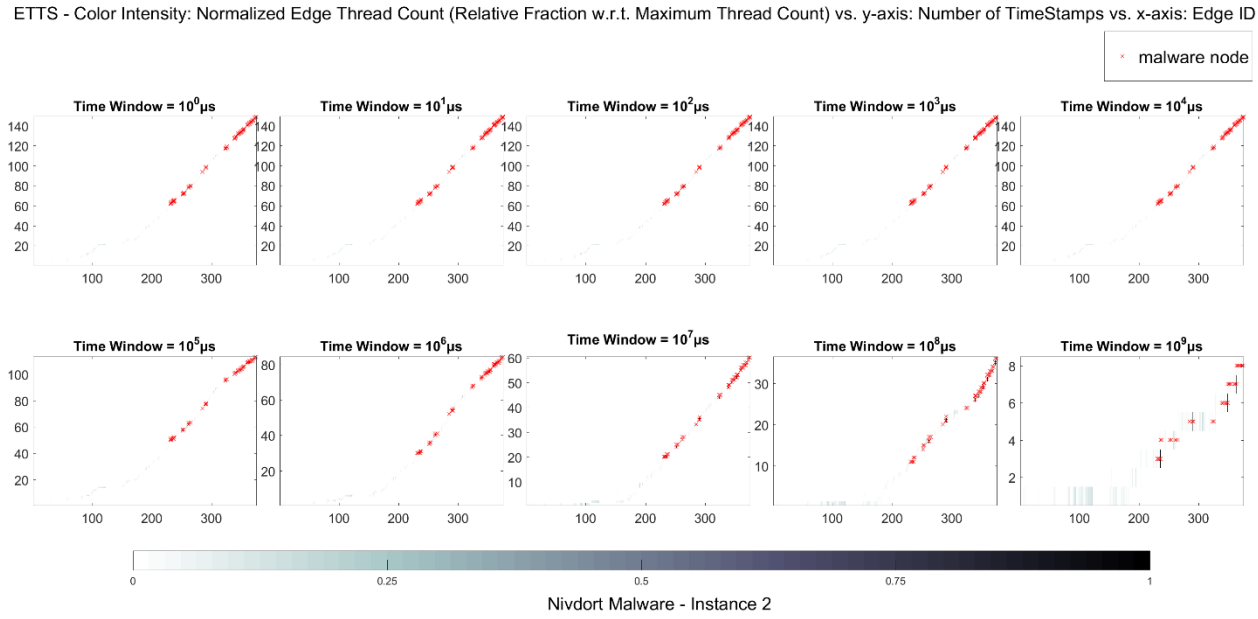
2) EMTS



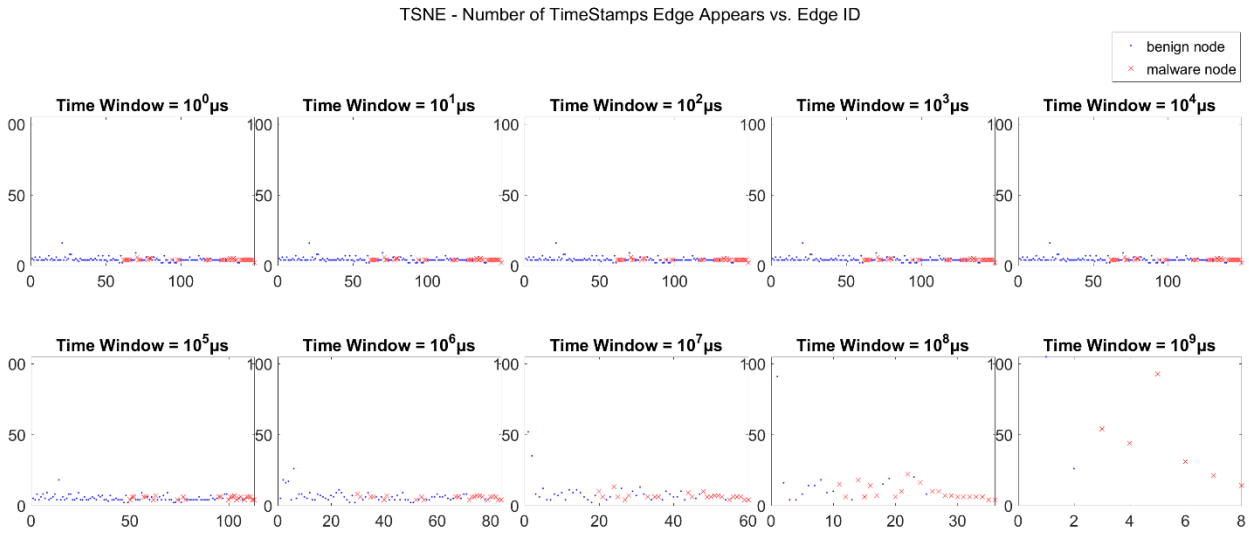
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Nivdort Malware - Instance 2

4) ETTS

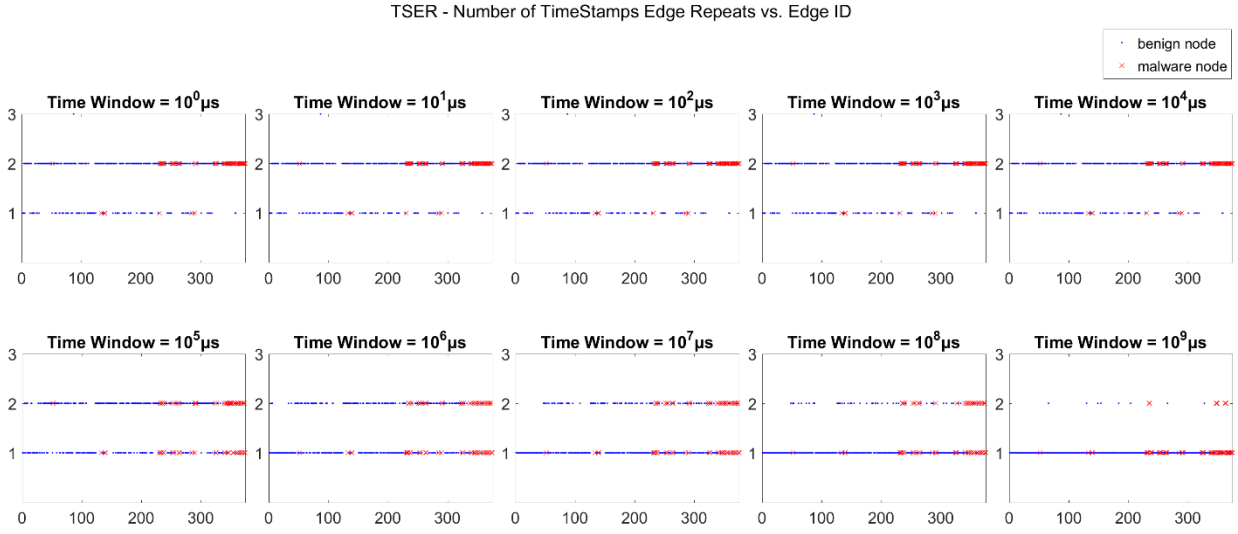

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Nivdort Malware - Instance 2

5) TSNE



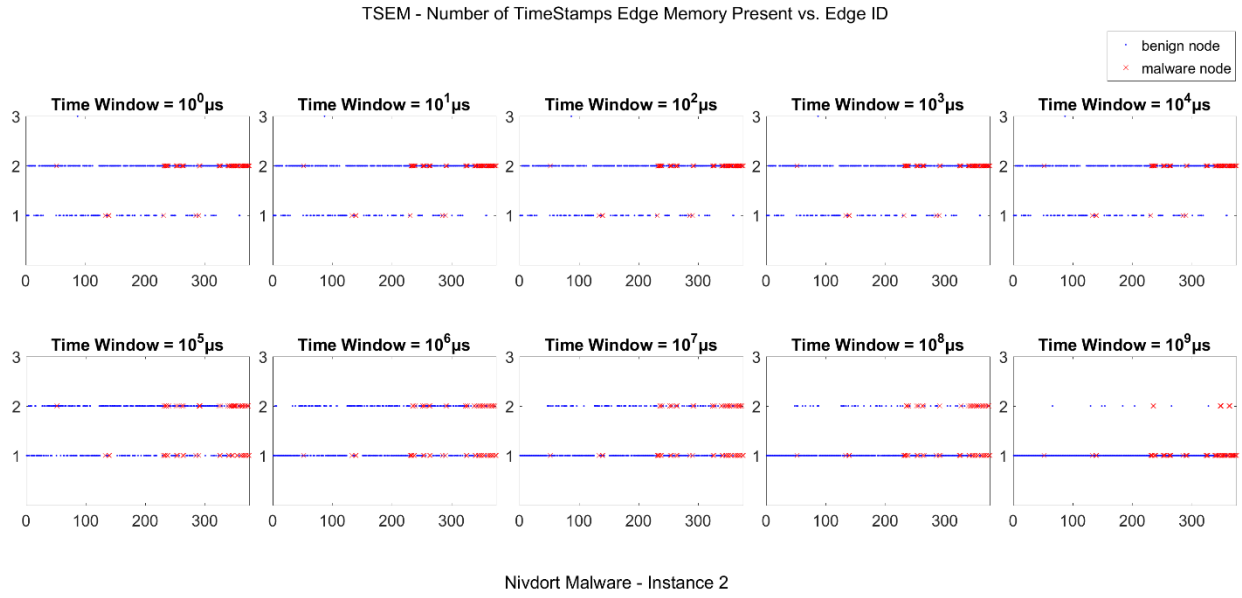
Nivdort Malware - Instance 2

6) TSER

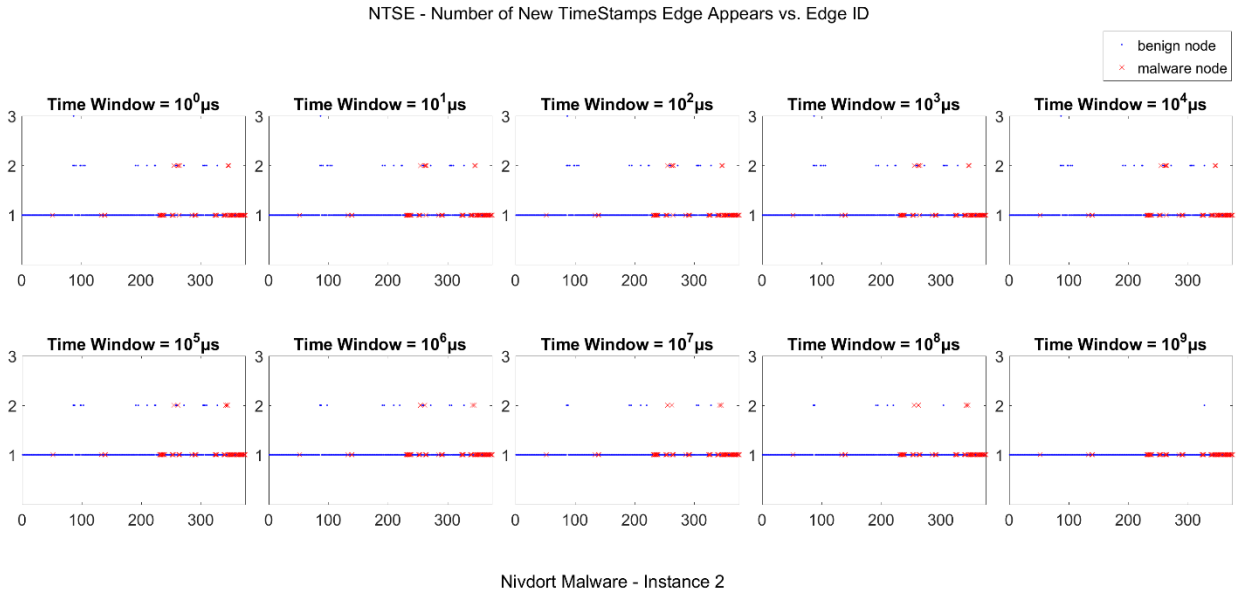


Nivdort Malware - Instance 2

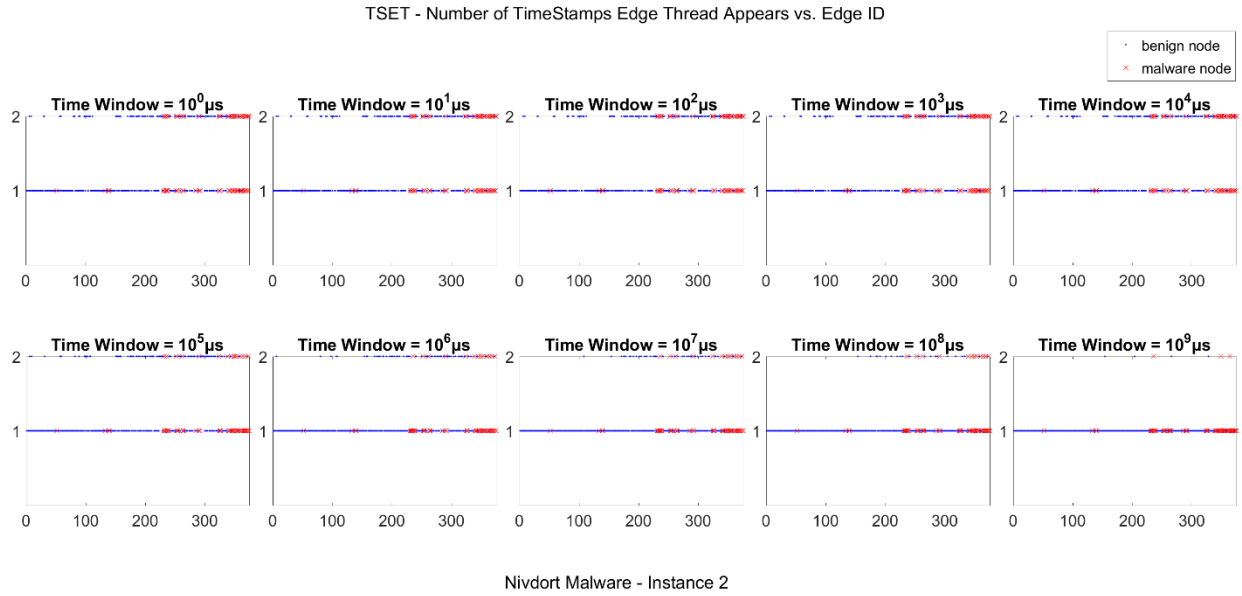
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Nivdort Malware - Instance 2

8) NTSE

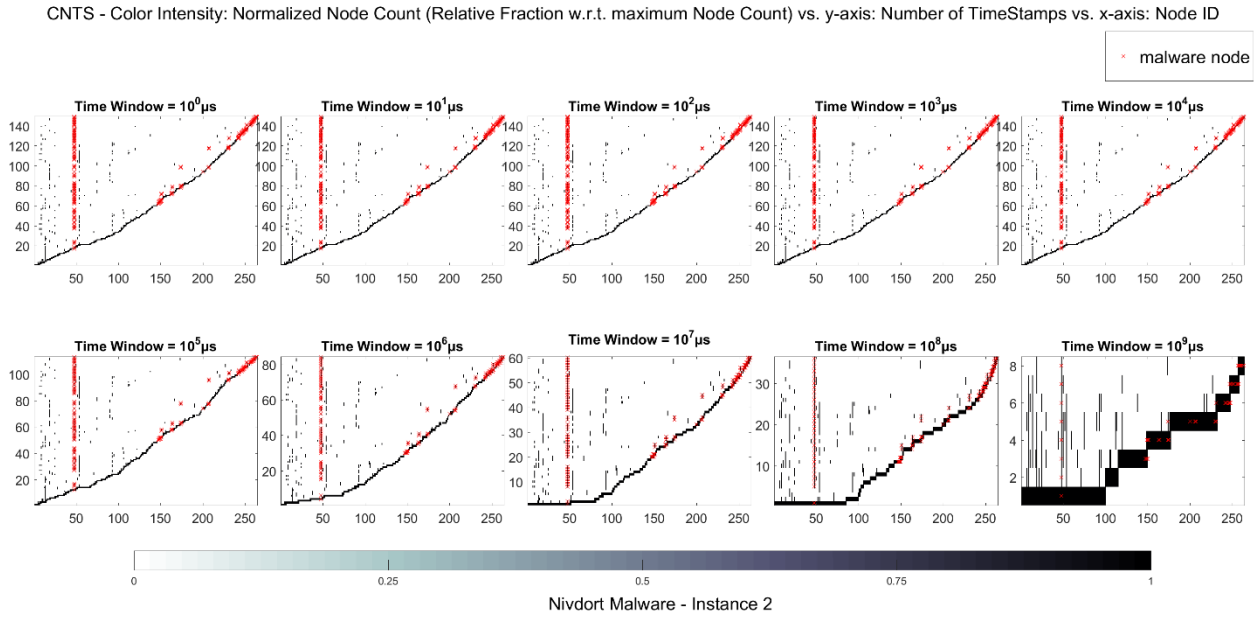

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Nivdort Malware - Instance 2

9) TSET

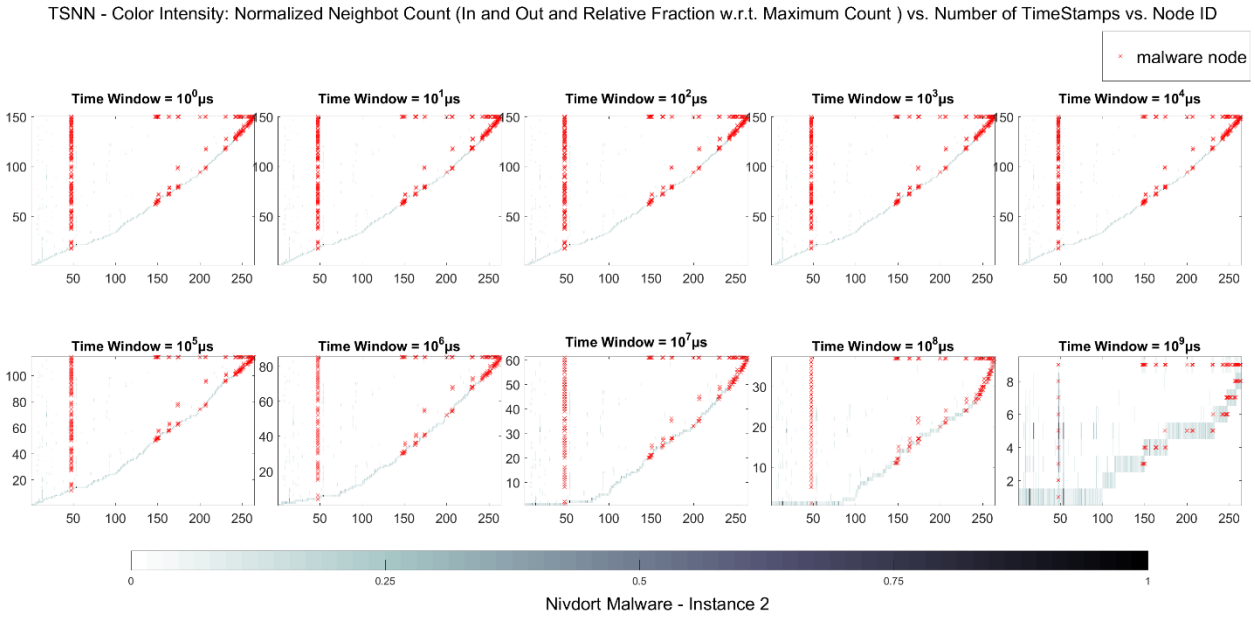


Time Graph Node Based Features

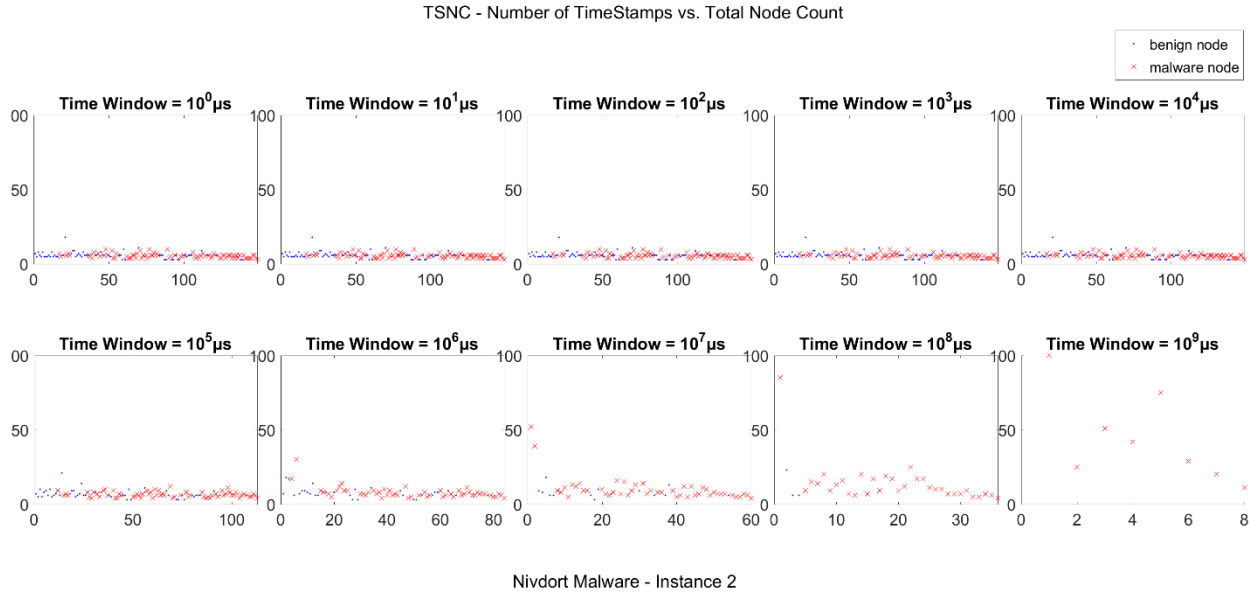
10) CNTS



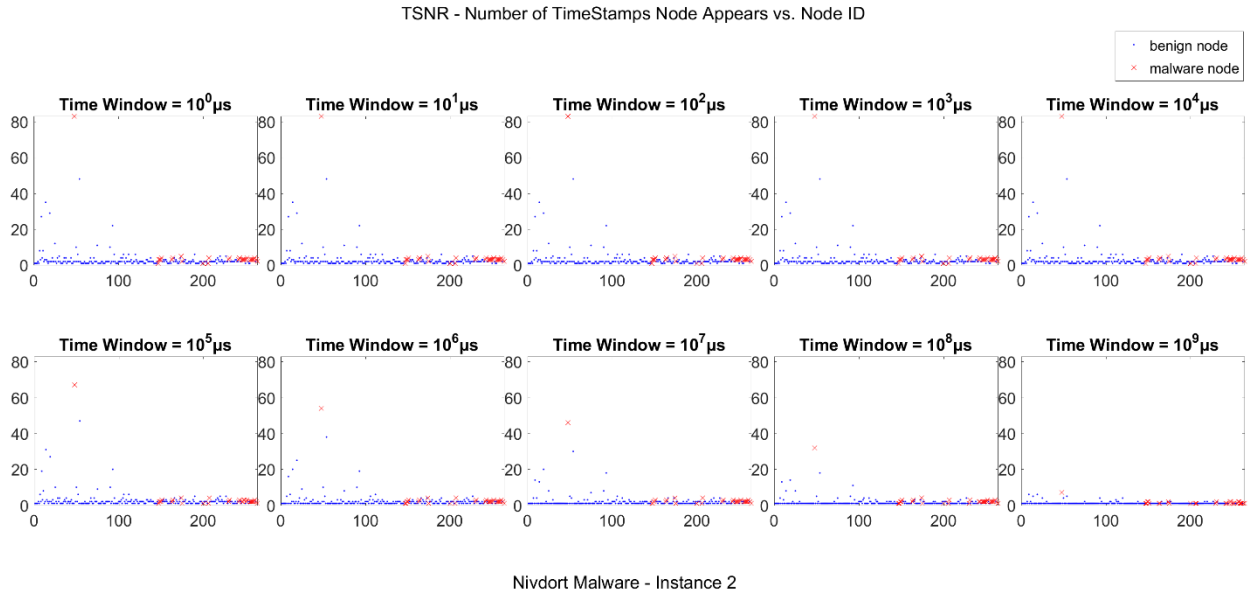
11) TSNN



12) TSNC



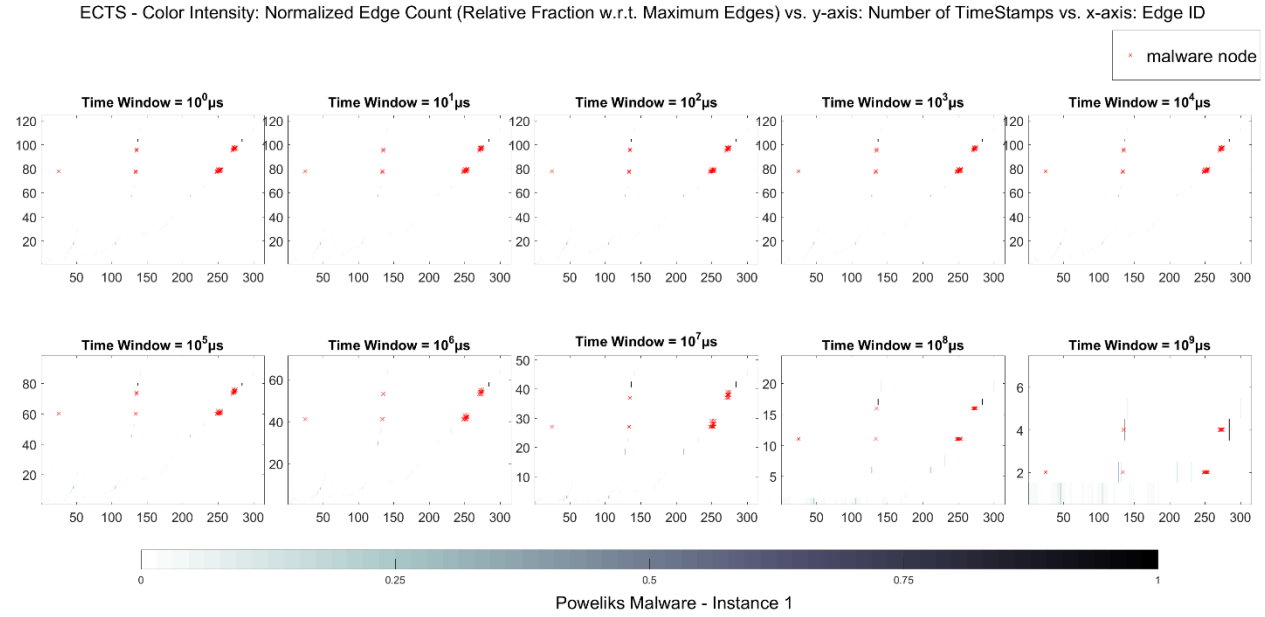
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Nivdort Malware - Instance 2

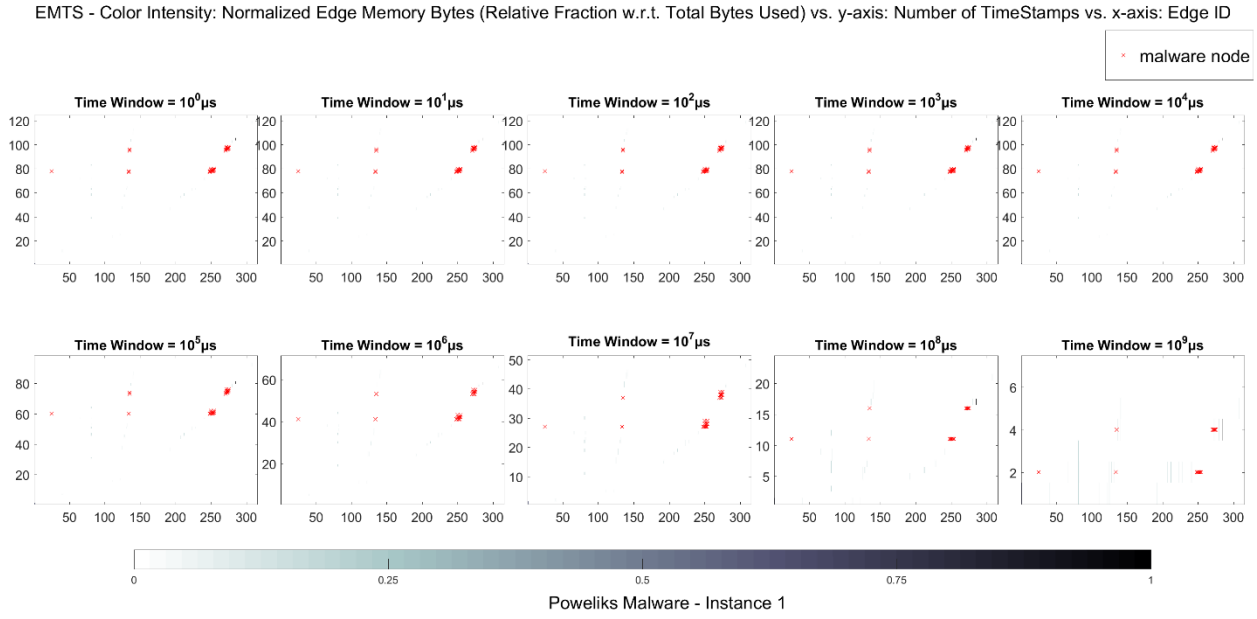
7.1.19 Poweliks Malware – Instance 1

Time Graph Edge Based Features

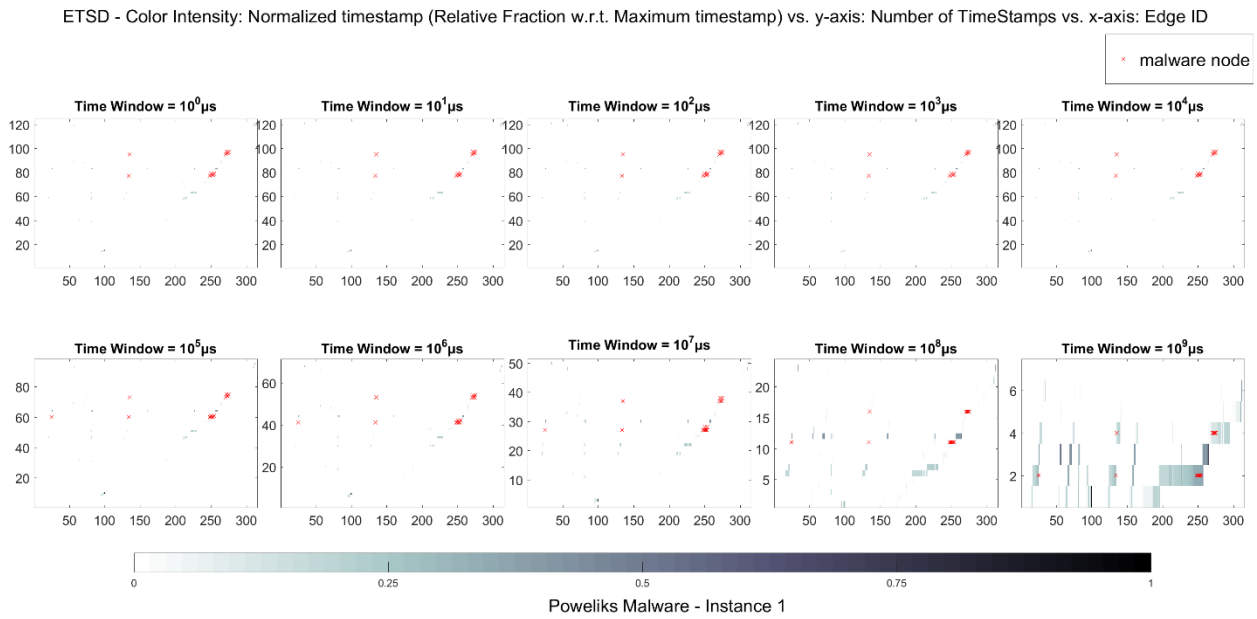
1) ECTS



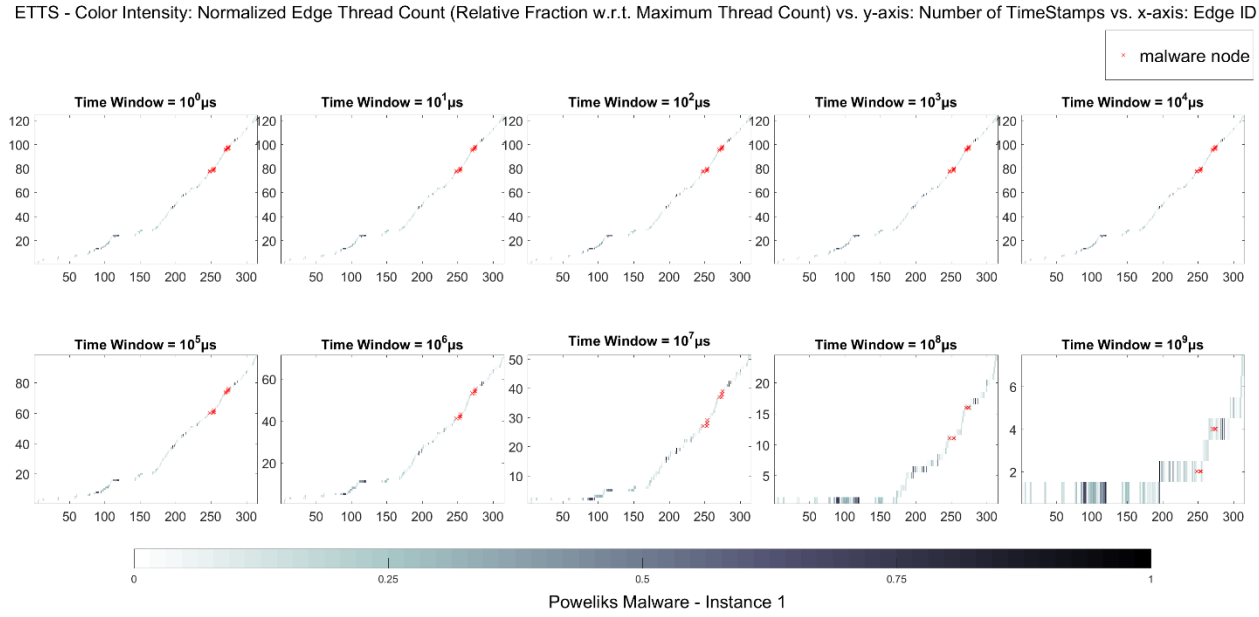
2) EMTS



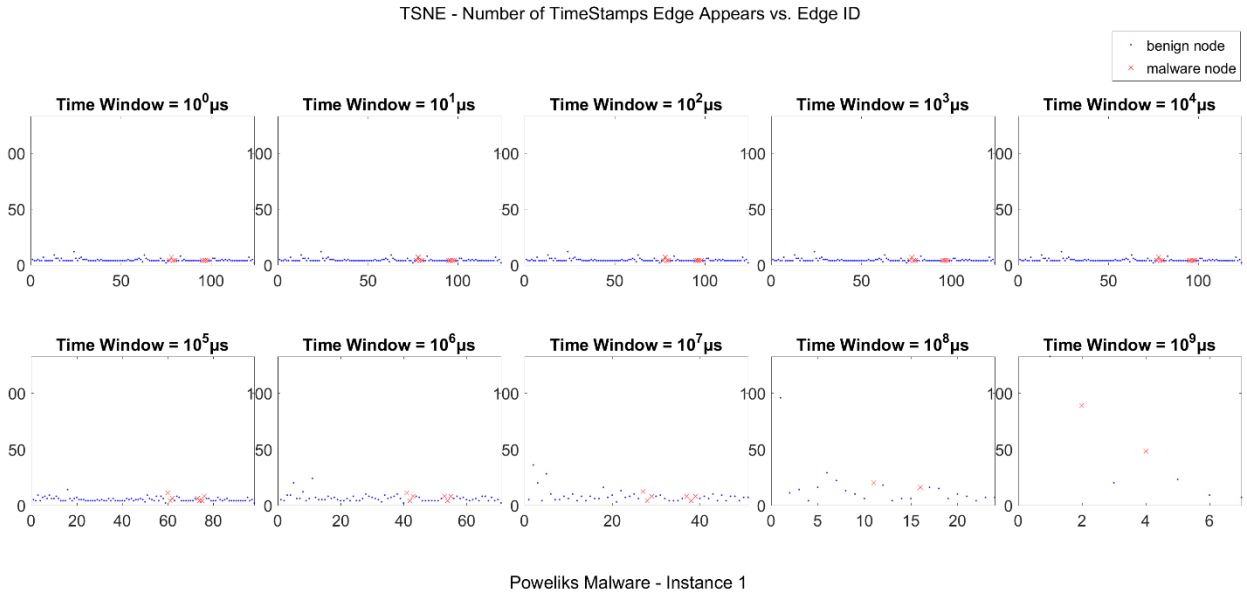
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Poweliks Malware - Instance 1

4) ETTS

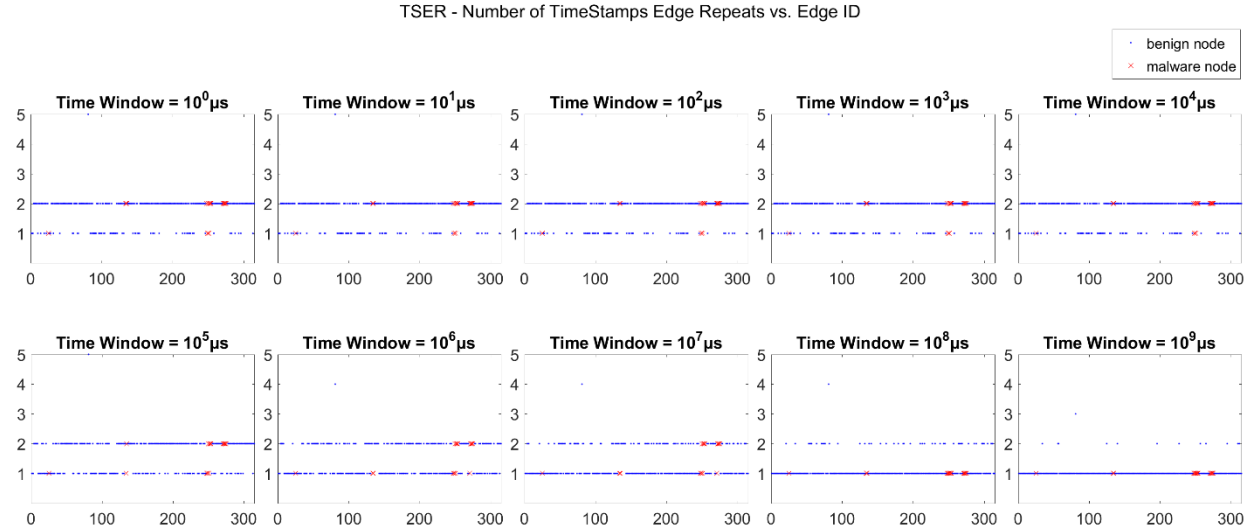

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Poweliks Malware - Instance 1

5) TSNE



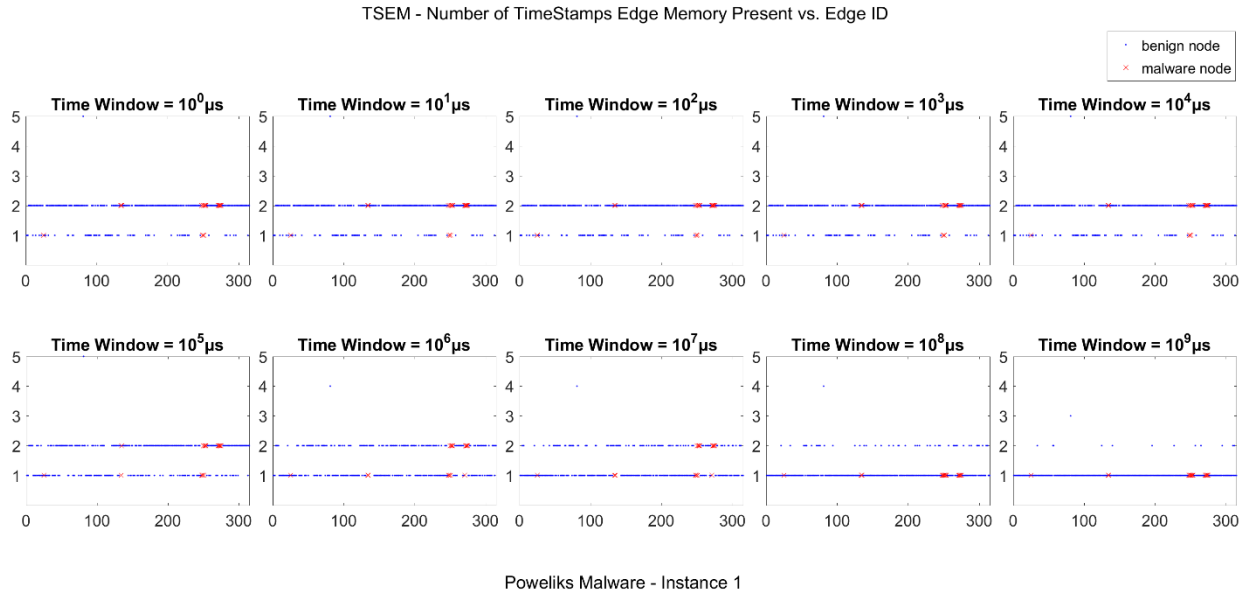
Poweliks Malware - Instance 1

6) TSER

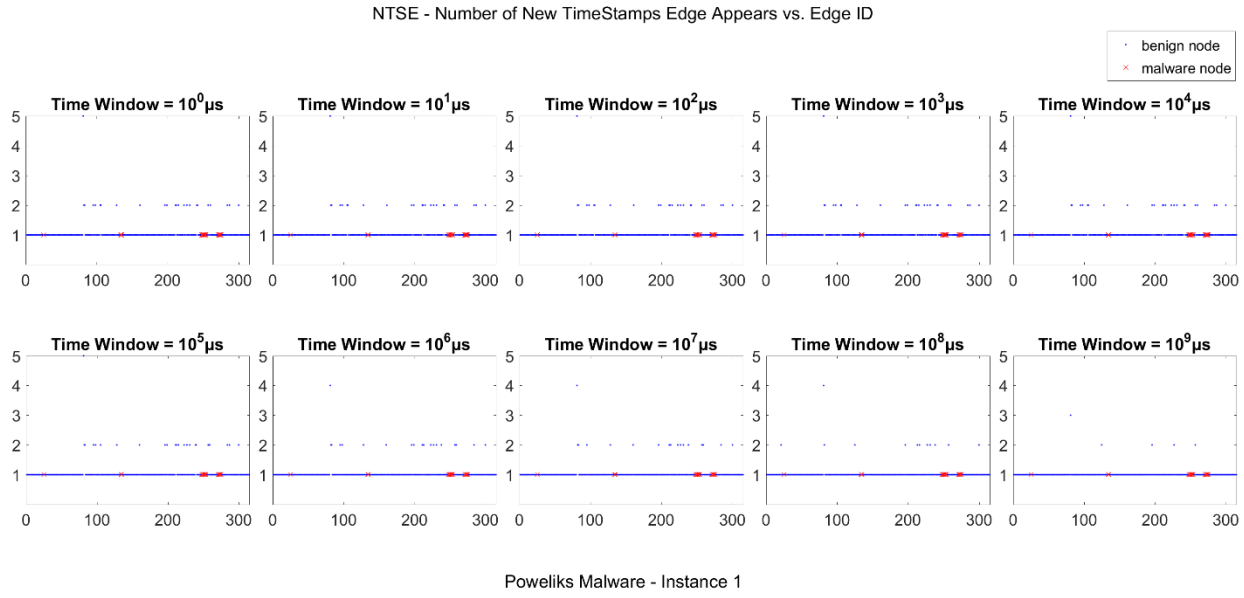


Poweliks Malware - Instance 1

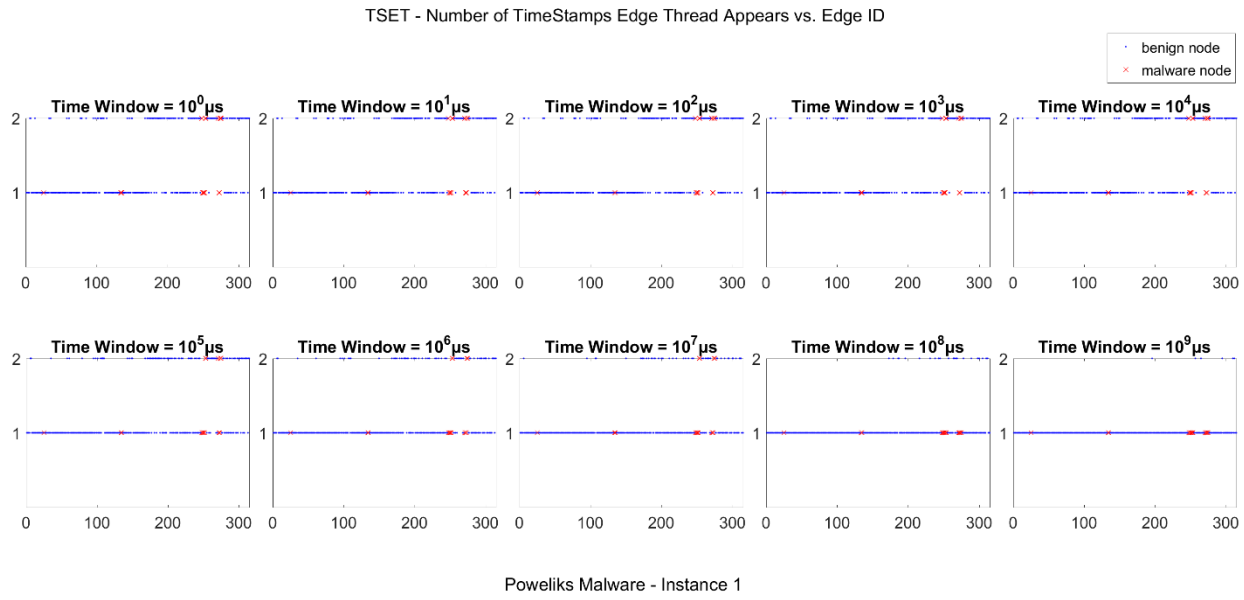
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Poweliks Malware - Instance 1

8) NTSE

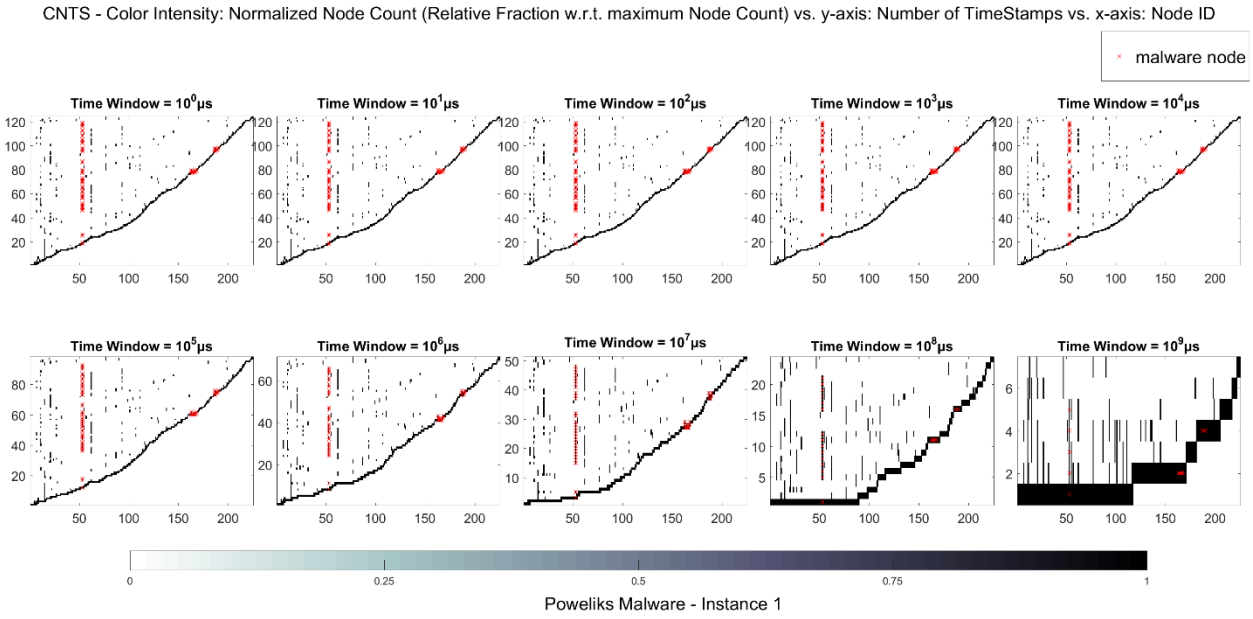

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Poweliks Malware - Instance 1

9) TSET

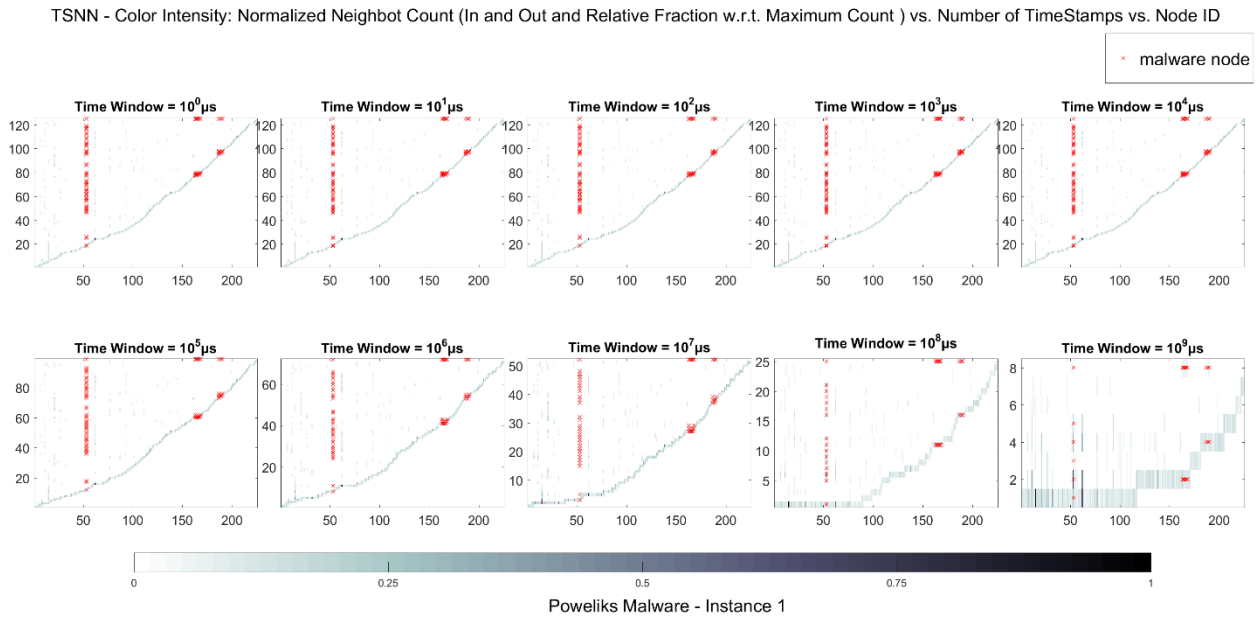


Time Graph Node Based Features

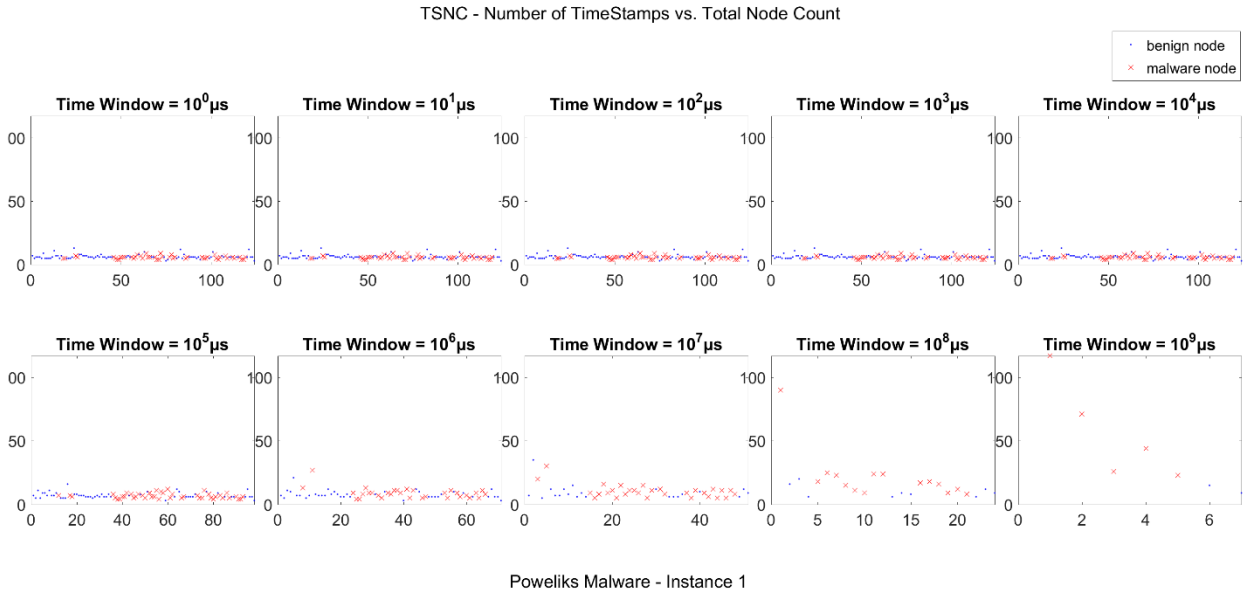
10) CNTS



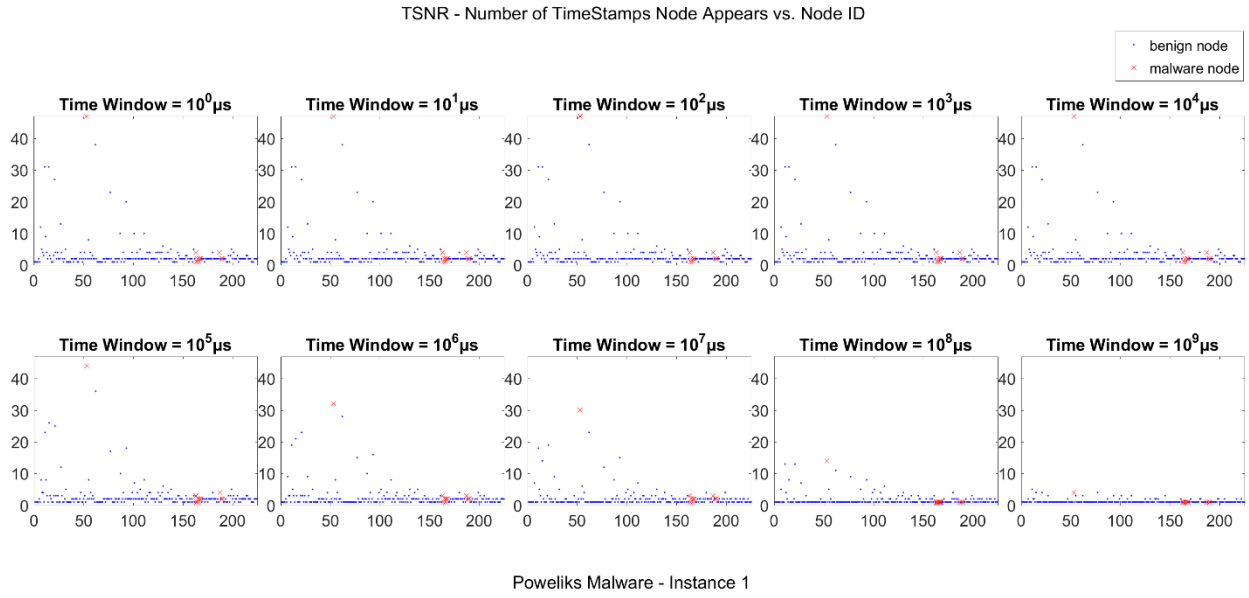
11) TSNN



12) TSNC



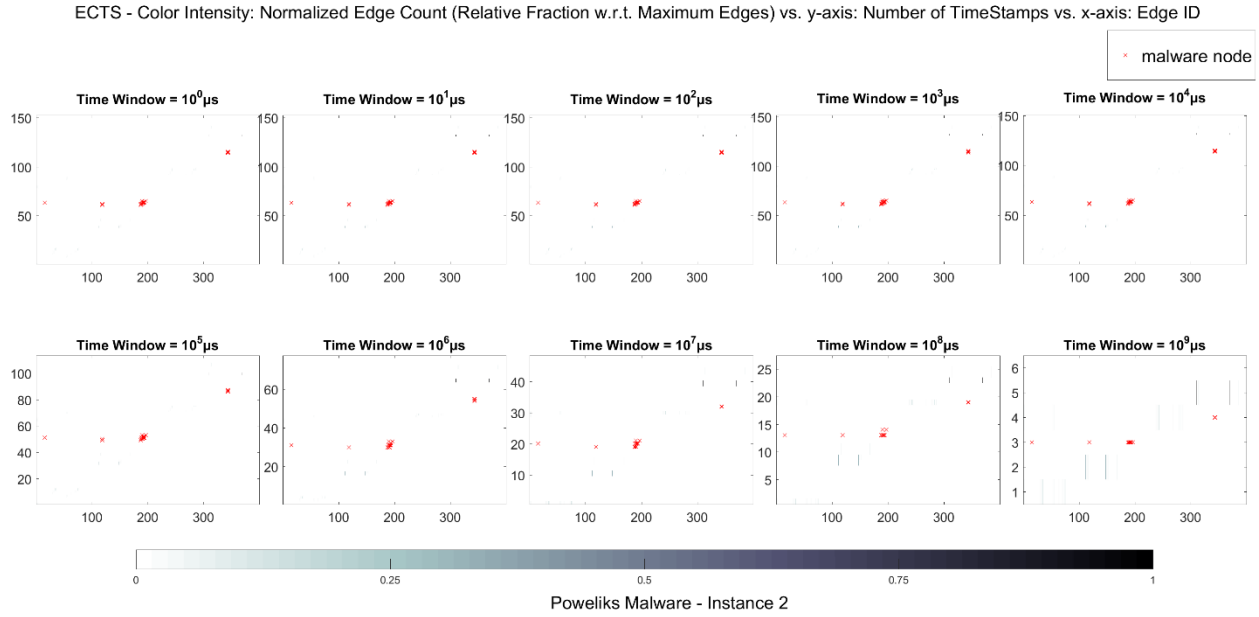
13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Poweliks Malware - Instance 1

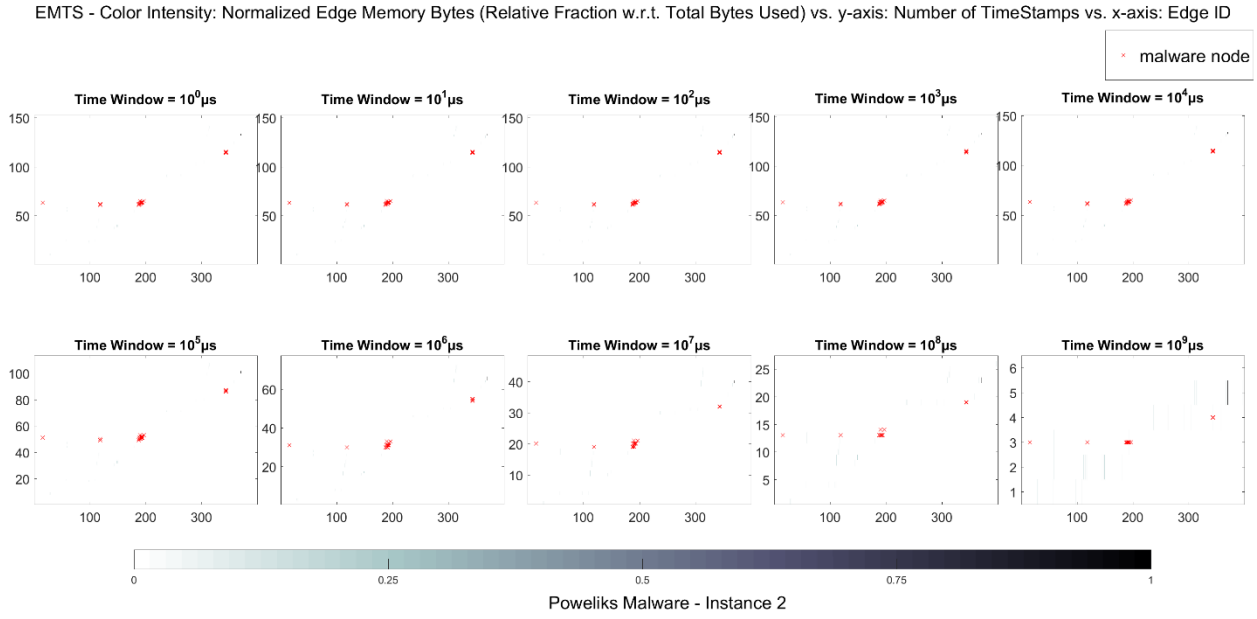
7.1.20 Poweliks Malware – Instance 2

Time Graph Edge Based Features

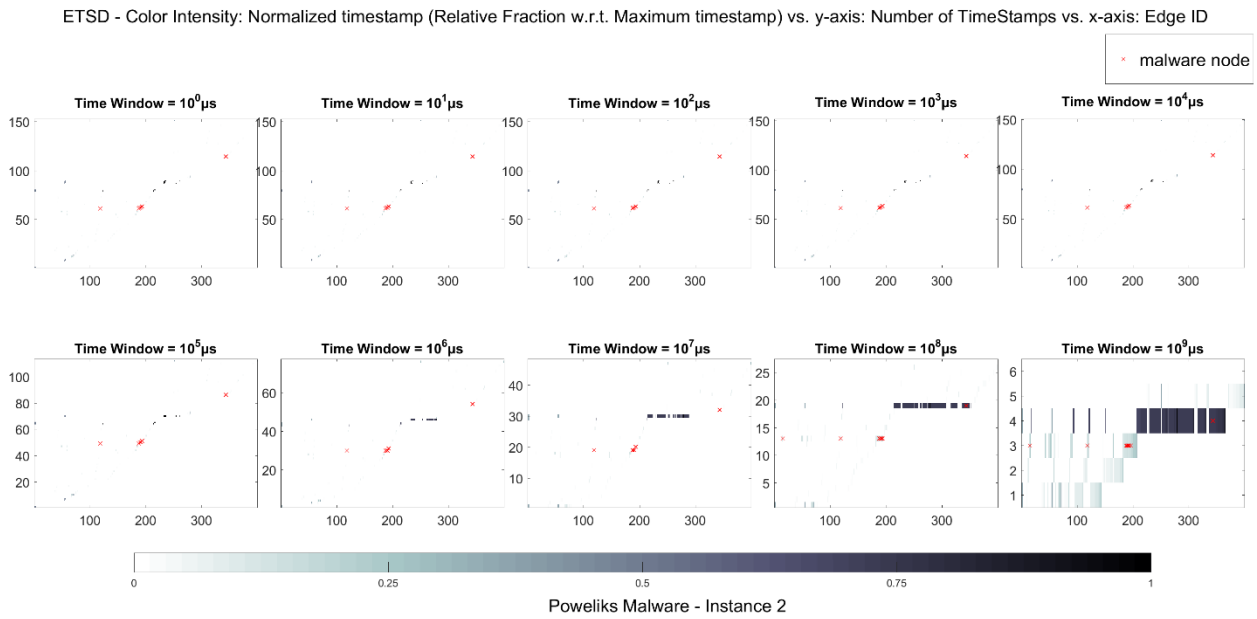
1) ECTS



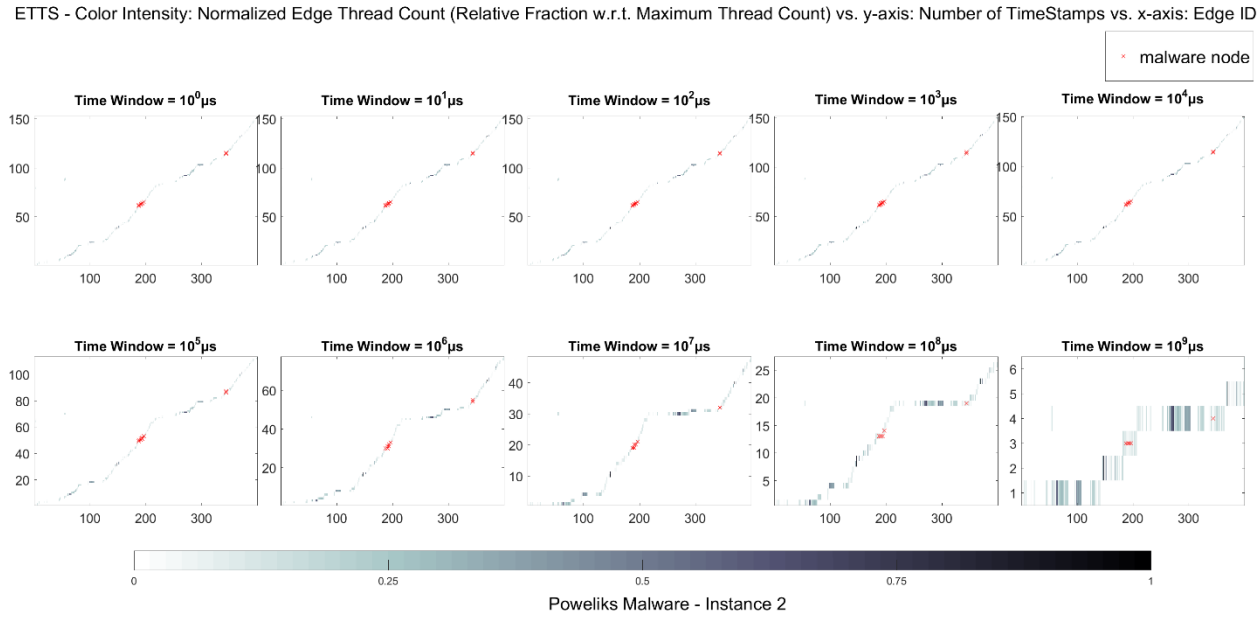
2) EMTS



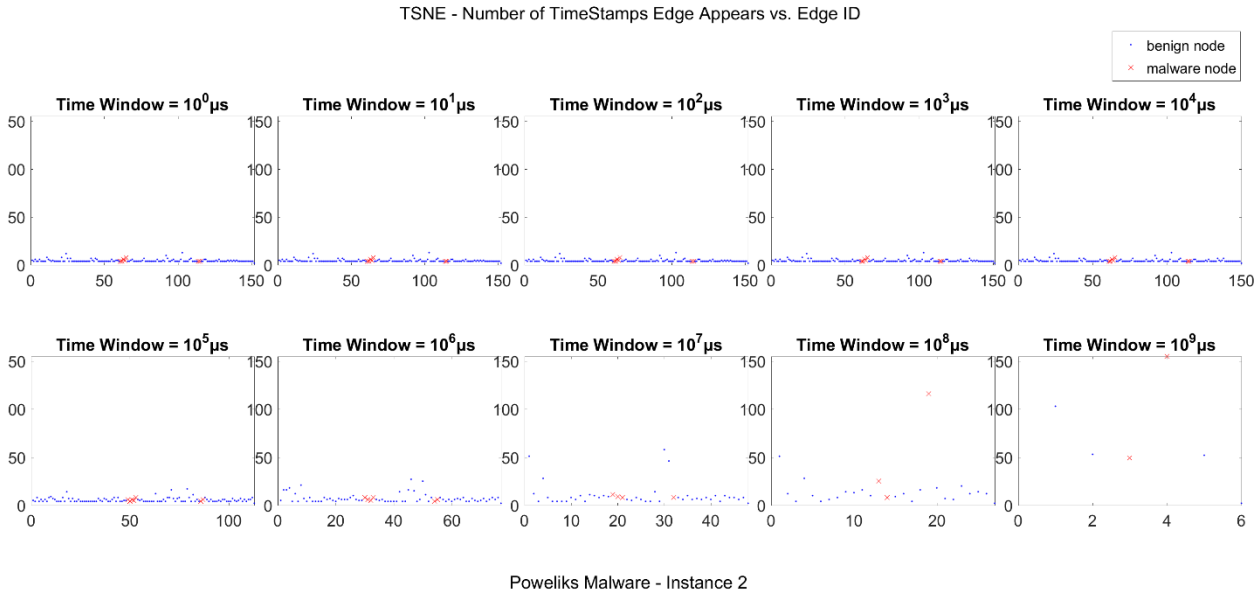
3) ETSD


ETSD - Color Intensity: Normalized timestamp (Relative Fraction w.r.t. Maximum timestamp) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Poweliks Malware - Instance 2

4) ETTS

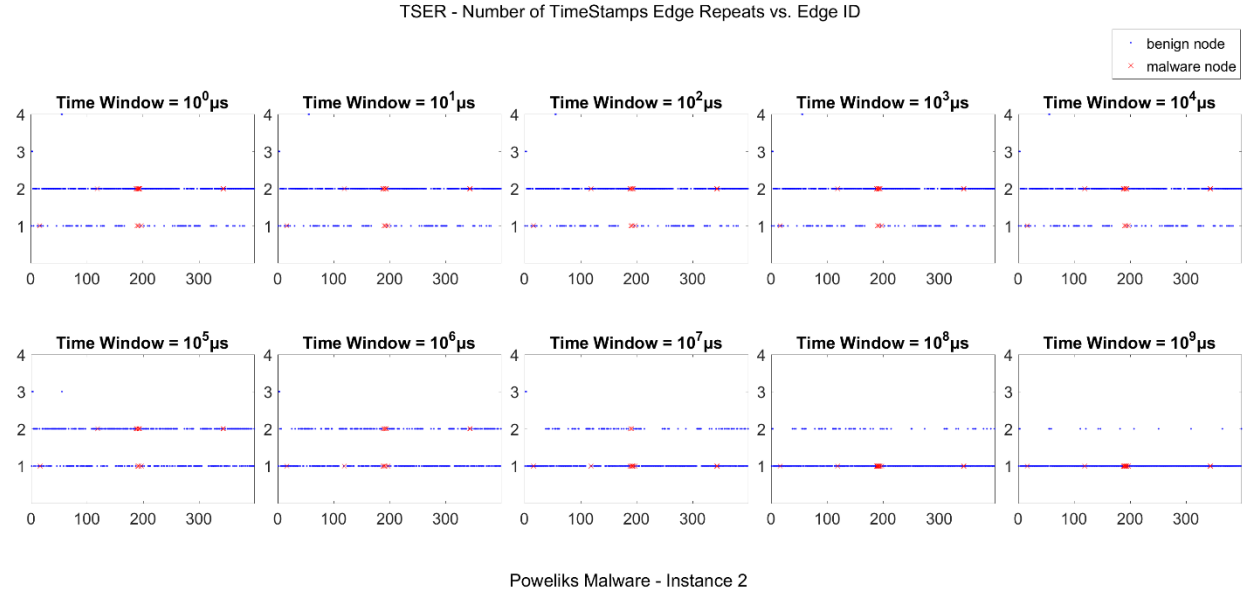

ETTS - Color Intensity: Normalized Edge Thread Count (Relative Fraction w.r.t. Maximum Thread Count) vs. y-axis: Number of TimeStamps vs. x-axis: Edge ID
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
0
0.25
0.5
0.75
1
Poweliks Malware - Instance 2

5) TSNE



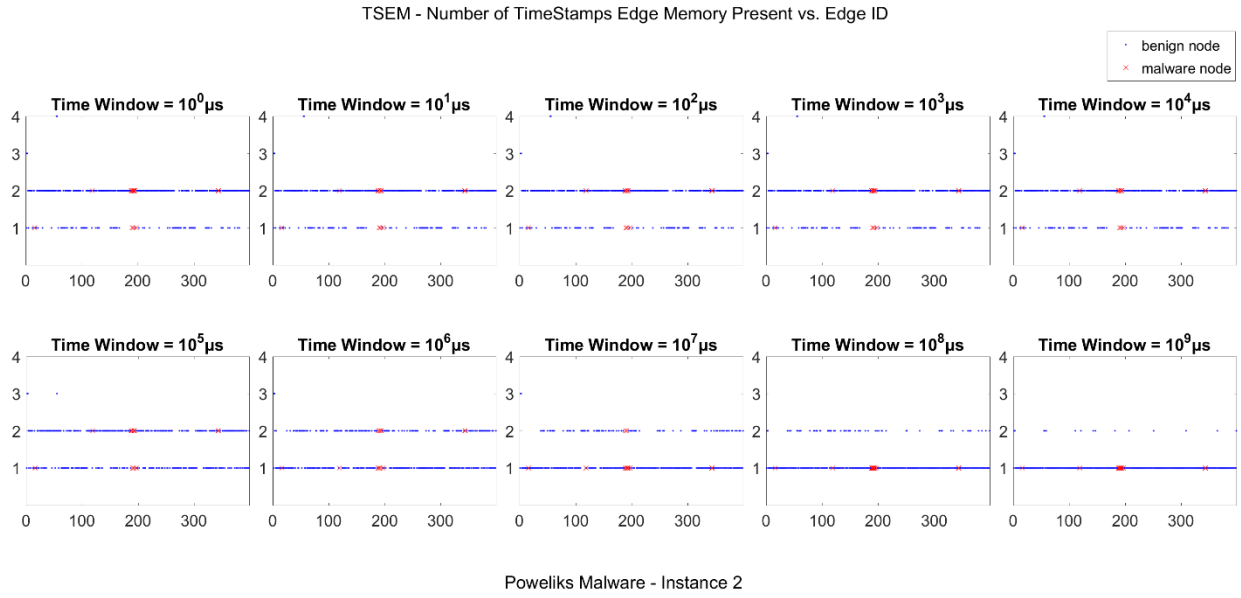
Poweliks Malware - Instance 2

6) TSER

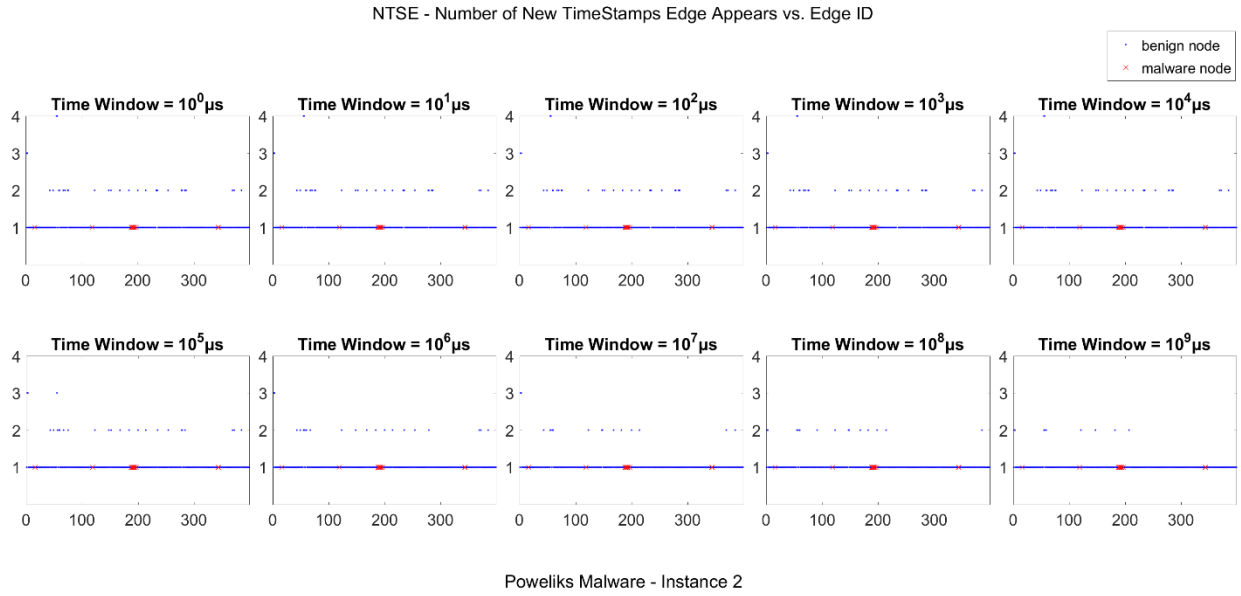


Poweliks Malware - Instance 2

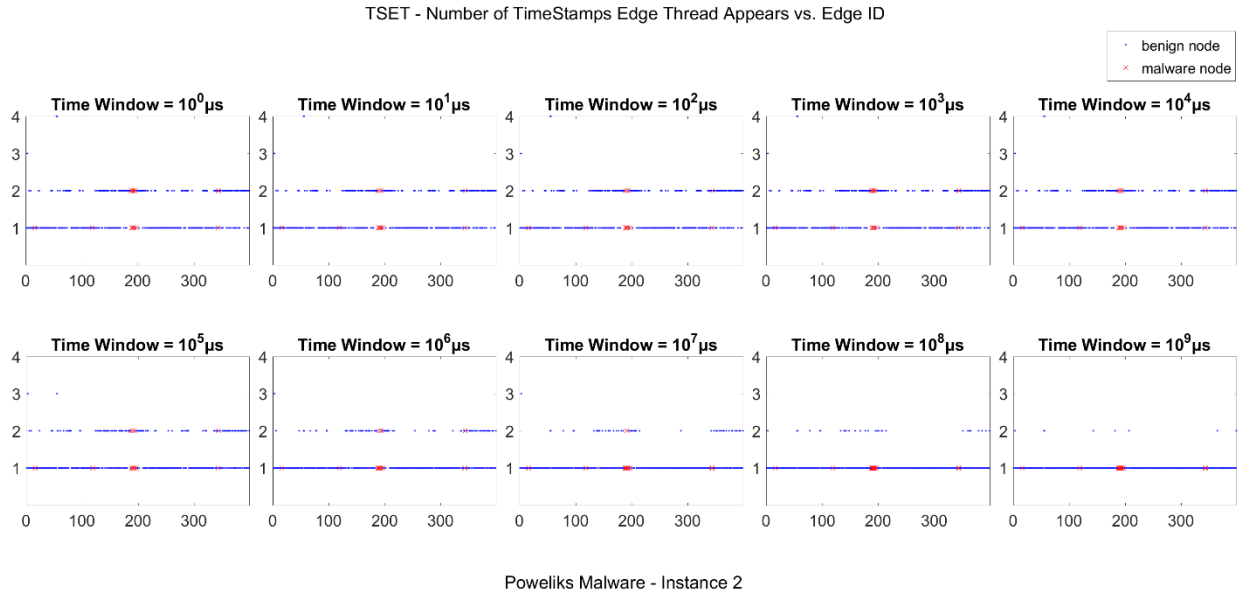
7) TSEM


TSEM - Number of TimeStamps Edge Memory Present vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Poweliks Malware - Instance 2

8) NTSE

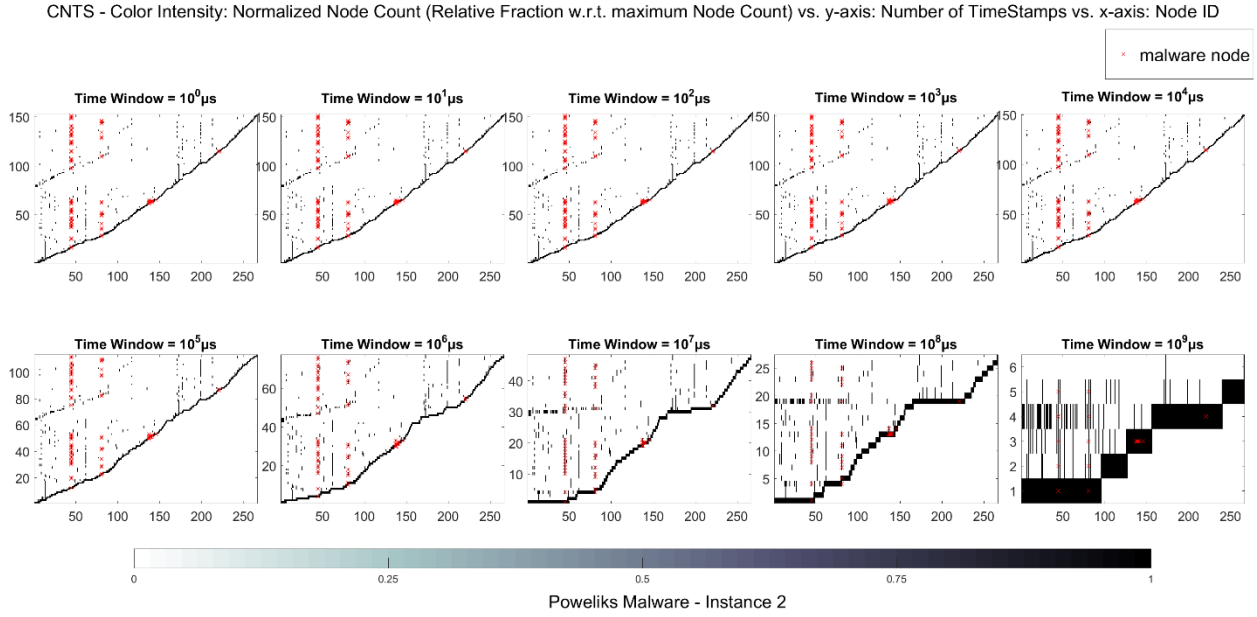

NTSE - Number of New TimeStamps Edge Appears vs. Edge ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Poweliks Malware - Instance 2

9) TSET

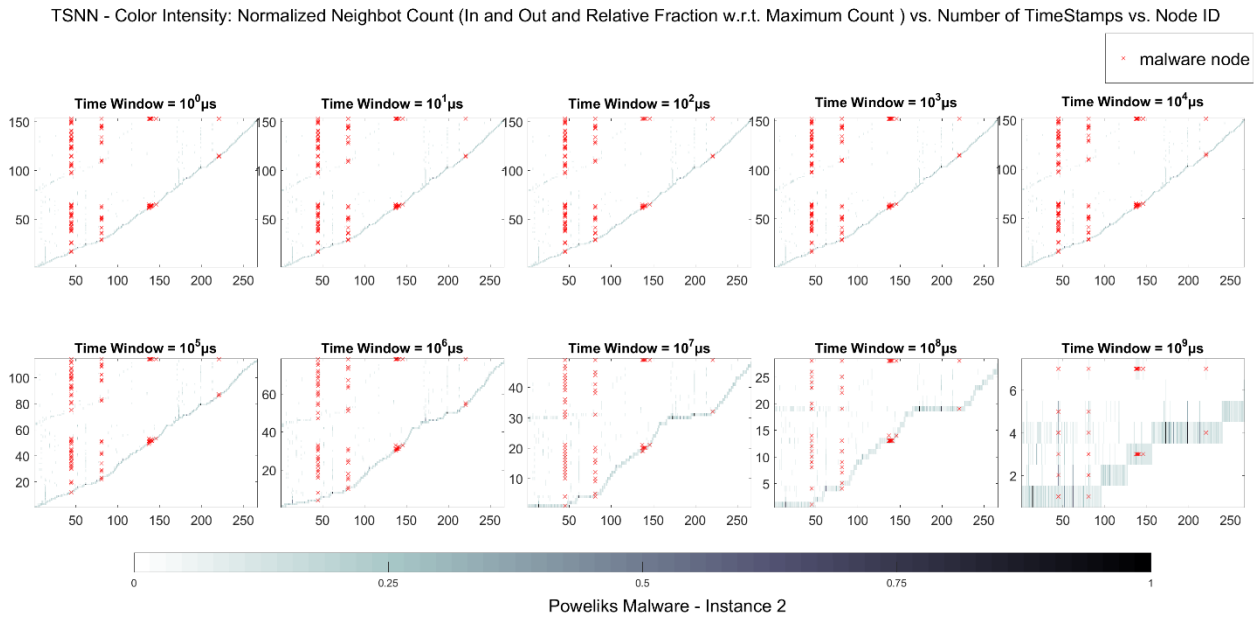


Time Graph Node Based Features

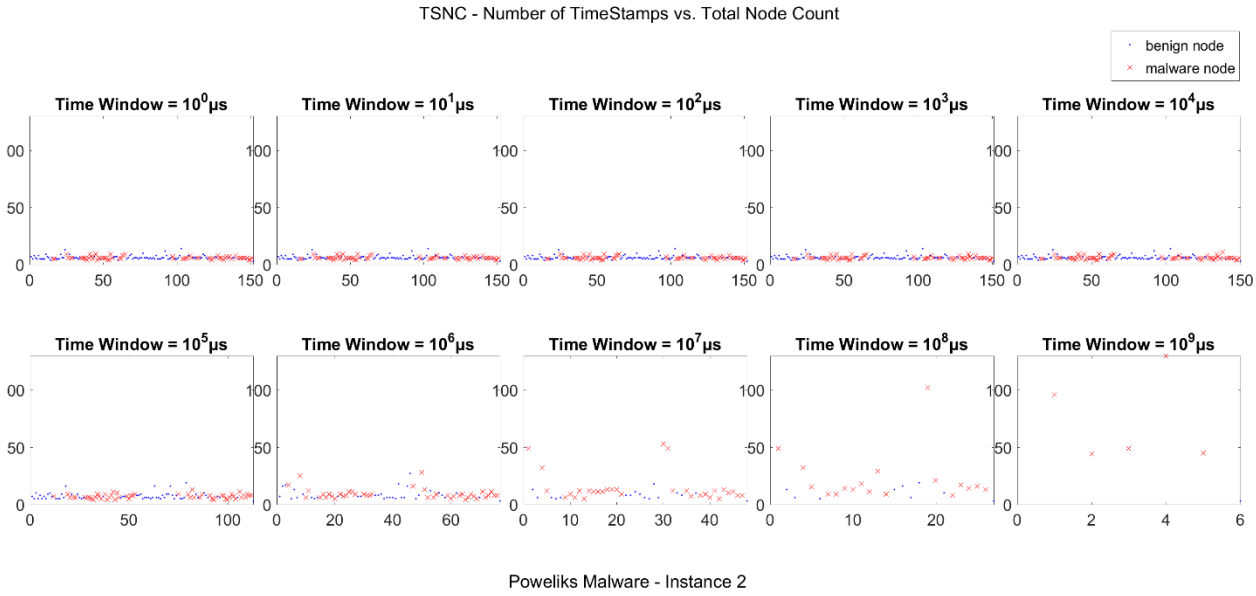
10) CNTS



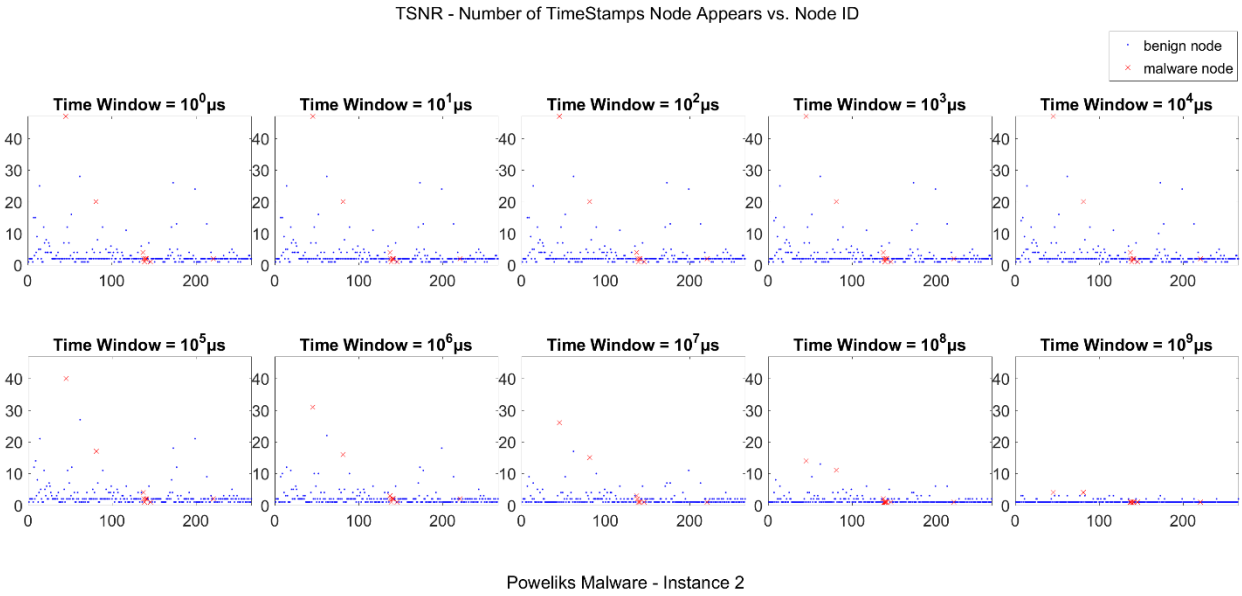
11) TSNN



12) TSNC



13) TSNR


TSNR - Number of TimeStamps Node Appears vs. Node ID
benign node
malware node
Time Window = 10^0µs
Time Window = 10^1µs
Time Window = 10^2µs
Time Window = 10^3µs
Time Window = 10^4µs
Time Window = 10^5µs
Time Window = 10^6µs
Time Window = 10^7µs
Time Window = 10^8µs
Time Window = 10^9µs
Poweliks Malware - Instance 2

7.2 Process Tree Data – Graph Attributes of All Malware Instance Data Set (Nodes and Edges)

In this subsection, node and edge process tree information is provided. Node IDs and names are enumerated in the table for each malware. Similarly, edge ID and names are enumerated for each malware. Node and edge IDs are represented as a tuple of either process ID and process name or module name and module path.

7.2.1 Zeus Malware – Instance 1

Table 95: Zeus Malware Instance 1 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'356,svchost.exe'
6	'364,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'412,XXX'
9	'424,csrss.exe'
10	'404,wininit.exe'
11	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'504,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'528,lsm.exe'
17	'520,lsass.exe'
18	'wkscli.dll,C:Windowssystem32wkscli.dll'
19	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
20	'psbase.dll,C:Windowssystem32psbase.dll'
21	'628,svchost.exe'
22	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
23	'692,VBoxService.exe'
24	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'

25	'756,svchost.exe'
26	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
27	'860,svchost.exe'
28	'winrnr.dll,C:WindowsSystem32winrnr.dll'
29	'896,svchost.exe'
30	'credssp.dll,C:WindowsSystem32credssp.dll'
31	'924,svchost.exe'
32	'AVRT.dll,c:windowssystem32AVRT.dll'
33	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
34	'rasman.dll,C:Windowssystem32rasman.dll'
35	'HID.DLL,C:WindowsSystem32HID.DLL'
36	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
37	'dsrole.dll,C:Windowssystem32dsrole.dll'
38	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
39	'msxml3.dll,C:WindowsSystem32msxml3.dll'
40	'schannel.DLL,C:Windowssystem32schannel.DLL'
41	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
42	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
43	'1004,svchost.exe'
44	'SensApi.dll,C:Windowssystem32SensApi.dll'
45	'1228,spoolsv.exe'
46	'netutils.dll,C:WindowsSystem32netutils.dll'
47	'1256,svchost.exe'
48	'1380,svchost.exe'
49	'1424,FoxitConnectedPDFService.exe'
50	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
51	'1876,svchost.exe'
52	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
53	'1152,dwm.exe'
54	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
55	'1128,taskhost.exe'
56	'midimap.dll,C:Windowssystem32midimap.dll'
57	'1096,XXX'
58	'1340,explorer.exe'
59	'MLANG.dll,C:Windowssystem32MLANG.dll'
60	thumbcache.dll,C:Windowssystem32humbcache.dll'
61	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
62	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
63	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
64	tquery.dll,C:Windowssystem32query.dll'
65	'Normaliz.dll,C:Windowssystem32Normaliz.dll'

66	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
67	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
68	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
69	'2124,VBoxTray.exe'
70	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
71	'2132,MySQLNotifier.exe'
72	'2144,XXX'
73	'2296,jusched.exe'
74	'2440,WmiPrvSE.exe'
75	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
76	'2596,SearchIndexer.exe'
77	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
78	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
79	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
80	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
81	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
82	'2820,wmpnetwk.exe'
83	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
84	'provsvc.dll,C:WindowsSystem32provsvc.dll'
85	'208,sppsvc.exe'
86	'700,svchost.exe'
87	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
88	'944,XXX'
89	'2340,taskmgr.exe'
90	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
91	'2968,audiodg.exe'
92	'1280,mintty.exe'
93	'apphelp.dll,C:Windowssystem32apphelp.dll'
94	'3008,conhost.exe'
95	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
96	'1060,XXX'
97	'2936,bash.exe'
98	'authz.dll,C:Windowssystem32authz.dll'
99	'1036,XXX'
100	'3040,driver_endpoint_netconn.exe'
101	'3920,audiodg.exe'
102	'624,notepad++.exe'
103	'3248,cmd.exe'
104	'3256,conhost.exe'
105	'3316,java.exe'
106	'3368,java.exe'

107	'3500,firefox.exe'
108	'3664,firefox.exe'
109	'3184,cmd.exe'
110	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
111	'3192,conhost.exe'
112	'3232,NETSTAT.EXE'
113	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
114	'3316,Wireshark.exe'
115	'msimtf.dll,C:Windowssystem32msimtf.dll'
116	'3276,dumpcap.exe'
117	'3320,conhost.exe'
118	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
119	'4100,FoxitReader.exe'
120	'4328,SearchProtocolHost.exe'
121	'4340,SearchFilterHost.exe'
122	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
123	'4832,mintty.exe'
124	'4868,conhost.exe'
125	'4888,XXX'
126	'4900,bash.exe'
127	'4720,SearchProtocolHost.exe'
128	'4764,SearchFilterHost.exe'
129	'OffFilt.dll,C:Windowssystem32OffFilt.dll'
130	'5660,dllhost.exe'
131	'5272,SearchProtocolHost.exe'
132	'profapi.dll,C:Windowssystem32profapi.dll'
133	'VERSION.dll,C:Windowssystem32VERSION.dll'
134	'5344,SearchFilterHost.exe'
135	'SXS.DLL,C:Windowssystem32SXS.DLL'
136	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
137	'5156,firefox.exe'
138	'5452,firefox.exe'
139	'6192,dllhost.exe'
140	'6404,dllhost.exe'
141	'6540,dllhost.exe'
142	'6764,dllhost.exe'
143	'6904,dllhost.exe'
144	'IDStore.dll,C:WindowsSystem32IDStore.dll'
145	'6940,dllhost.exe'
146	'6972,zsb.exe'
147	'7156,consent.exe'

148	'7036,notepad.exe'
149	'6336,dllhost.exe'
150	'6300,dllhost.exe'
151	**'6480,bot.exe'**
152	**'6484,xusa.exe'**
153	'8648,audiodg.exe'
154	'15256,audiodg.exe'
155	'18084,audiodg.exe'
156	'19844,audiodg.exe'
157	'19200,firefox.exe'
158	'19972,pingsender.exe'
159	'19984,conhost.exe'
160	'6548,WinMail.exe'
161	'CFGMGR32.dll,C:Windowssystem32CFGMGR32.dll'
162	'6872,taskhost.exe'
163	'6184,dllhost.exe'
164	'7280,cmd.exe'
165	'7288,conhost.exe'
166	'7412,java.exe'
167	'7576,java.exe'
168	'7584,conhost.exe'
169	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
170	'7668,cmd.exe'
171	'7676,conhost.exe'
172	'7780,java.exe'
173	'7896,firefox.exe'
174	'8064,firefox.exe'
175	'7748,cmd.exe'
176	'7404,conhost.exe'
177	'8208,NETSTAT.EXE'
178	'8296,notepad++.exe'
179	'8336,Wireshark.exe'
180	'8396,gspawn-win64-helper.exe'
181	'8408,androiddump.exe'
182	'8472,dumpcap.exe'
183	'8480,conhost.exe'
184	'8888,FoxitReader.exe'
185	'9060,SearchProtocolHost.exe'
186	'9100,SearchFilterHost.exe'
187	'8616,mintty.exe'
188	'8640,conhost.exe'

189	'8728,XXX'
190	'8716,bash.exe'
191	'9800,java.exe'
192	'9808,conhost.exe'
193	'9928,pingsender.exe'
194	'9940,conhost.exe'
195	'10036,iexplore.exe'
196	'10096,iexplore.exe'
197	'9920,SearchProtocolHost.exe'
198	'9988,SearchFilterHost.exe'
199	'9952,iexplore.exe'
200	'9976,slui.exe'
201	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
202	'10588,iexplore.exe'
203	'10660,SearchProtocolHost.exe'
204	'10736,SearchFilterHost.exe'
205	'10496,SearchProtocolHost.exe'
206	'11204,SearchFilterHost.exe'
207	'11908,dllhost.exe'
208	'11944,dllhost.exe'
209	'11980,iexplore.exe'
210	'npmproxy.dll,C:WindowsSystem32npmproxy.dll'
211	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
212	'12032,iexplore.exe'
213	'12172,iexplore.exe'
214	'msfeeds.dll,C:Windowssystem32msfeeds.dll'
215	'Secur32.dll,C:WindowsSystem32Secur32.dll'
216	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
217	'slc.dll,C:Windowssystem32slc.dll'
218	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
219	'wer.dll,C:Windowssystem32wer.dll'
220	'12224,iexplore.exe'
221	'WINSPOOL.DRV,C:WindowsSystem32WINSPOOL.DRV'
222	'msimg32.dll,C:Windowssystem32msimg32.dll'
223	'vgx.dll,C:Program FilesCommon FilesMicrosoft SharedVGXvgx.dll'
224	'T2EMBED.DLL,C:Windowssystem32T2EMBED.DLL'
225	'11772,iexplore.exe'
226	'Dxtmsft.dll,C:WindowsSystem32Dxtmsft.dll'
227	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
228	'12316,SearchProtocolHost.exe'
229	'12348,SearchFilterHost.exe'

230	'11584,SearchFilterHost.exe'
231	'13488,WmiPrvSE.exe'
232	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
233	'13668,iexplore.exe'
234	'13724,iexplore.exe'
235	'13908,SearchProtocolHost.exe'
236	'13928,SearchFilterHost.exe'
237	'13376,SearchProtocolHost.exe'
238	'13412,SearchFilterHost.exe'
239	'15012,dllhost.exe'
240	'15228,calc.exe'
241	'oleacc.dll,C:Windowssystem32oleacc.dll'
242	'8692,dllhost.exe'
243	'15316,notepad++.exe'
244	'15480,iexplore.exe'
245	'15684,SearchProtocolHost.exe'
246	'15704,SearchFilterHost.exe'
247	'16652,firefox.exe'
248	'16820,firefox.exe'
249	'17336,dllhost.exe'
250	'17160,mip.exe'
251	'mshwgst.dll,C:Program FilesCommon FilesMicrosoft SharedInkmshwgst.dll'
252	'mraut.DLL,C:Program FilesCommon Filesmicrosoft sharedinkmraut.DLL'
253	'17296,wisptis.exe'
254	tpcps.dll,C:Program FilesCommon FilesMicrosoft SharedInkpcps.dll'
255	'17792,mspaint.exe'
256	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
257	'SAMLIB.dll,C:Windowssystem32SAMLIB.dll'
258	'17820,svchost.exe'
259	'18048,dllhost.exe'
260	'msxml6.dll,C:WindowsSystem32msxml6.dll'
261	'18308,SearchProtocolHost.exe'
262	'18328,SearchFilterHost.exe'
263	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
264	'18400,dllhost.exe'
265	'18476,FoxitReader.exe'
266	'18780,StikyNot.exe'
267	'18836,SearchProtocolHost.exe'
268	'18856,SearchFilterHost.exe'
269	'18896,SearchProtocolHost.exe'
270	'18980,StikyNot.exe'

271	'19372,firefox.exe'

Table 96: Zeus Malware Instance 1 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'356,svchost.exe'	'364,csrss.exe'
5	'356,svchost.exe'	'404,wininit.exe'
6	'356,svchost.exe'	'dsrole.dll,C:Windowssystem32dsrole.dll'
7	'356,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
8	'356,svchost.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
9	'356,svchost.exe'	'schannel.DLL,C:Windowssystem32schannel.DLL'
10	'356,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
11	'356,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
12	'364,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
13	'412,XXX'	'424,csrss.exe'
14	'412,XXX'	'460,winlogon.exe'
15	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
16	'424,csrss.exe'	'3008,conhost.exe'
17	'424,csrss.exe'	'3256,conhost.exe'
18	'424,csrss.exe'	'3192,conhost.exe'
19	'424,csrss.exe'	'3320,conhost.exe'
20	'424,csrss.exe'	'4868,conhost.exe'
21	'424,csrss.exe'	'19984,conhost.exe'
22	'424,csrss.exe'	'7288,conhost.exe'
23	'424,csrss.exe'	'7584,conhost.exe'
24	'424,csrss.exe'	'7676,conhost.exe'
25	'424,csrss.exe'	'7404,conhost.exe'
26	'424,csrss.exe'	'8480,conhost.exe'
27	'424,csrss.exe'	'8640,conhost.exe'
28	'424,csrss.exe'	'9808,conhost.exe'
29	'424,csrss.exe'	'9940,conhost.exe'
30	'404,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
31	'404,wininit.exe'	'504,services.exe'
32	'404,wininit.exe'	'528,lsm.exe'
33	'404,wininit.exe'	'520,lsass.exe'
34	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
35	'504,services.exe'	'356,svchost.exe'
36	'504,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
37	'504,services.exe'	'628,svchost.exe'
38	'504,services.exe'	'692,VBoxService.exe'
39	'504,services.exe'	'756,svchost.exe'
40	'504,services.exe'	'860,svchost.exe'
41	'504,services.exe'	'896,svchost.exe'
42	'504,services.exe'	'924,svchost.exe'
43	'504,services.exe'	'1004,svchost.exe'
44	'504,services.exe'	'1228,spoolsv.exe'

45	'504,services.exe'	'1256,svchost.exe'
46	'504,services.exe'	'1380,svchost.exe'
47	'504,services.exe'	'1424,FoxitConnectedPDFService.exe'
48	'504,services.exe'	'1876,svchost.exe'
49	'504,services.exe'	'1128,taskhost.exe'
50	'504,services.exe'	'2596,SearchIndexer.exe'
51	'504,services.exe'	'2820,wmpnetwk.exe'
52	'504,services.exe'	'208,sppsvc.exe'
53	'504,services.exe'	'700,svchost.exe'
54	'504,services.exe'	'6872,taskhost.exe'
55	'504,services.exe'	'17820,svchost.exe'
56	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
57	'520,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
58	'520,lsass.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
59	'520,lsass.exe'	'psbase.dll,C:Windowssystem32psbase.dll'
60	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
61	'628,svchost.exe'	'2440,WmiPrvSE.exe'
62	'628,svchost.exe'	'5660,dllhost.exe'
63	'628,svchost.exe'	'6192,dllhost.exe'
64	'628,svchost.exe'	'6404,dllhost.exe'
65	'628,svchost.exe'	'6540,dllhost.exe'
66	'628,svchost.exe'	'6764,dllhost.exe'
67	'628,svchost.exe'	'6904,dllhost.exe'
68	'628,svchost.exe'	'6940,dllhost.exe'
69	'628,svchost.exe'	'6336,dllhost.exe'
70	'628,svchost.exe'	'6300,dllhost.exe'
71	'628,svchost.exe'	'6548,WinMail.exe'
72	'628,svchost.exe'	'6184,dllhost.exe'
73	'628,svchost.exe'	'9976,slui.exe'
74	'628,svchost.exe'	'11908,dllhost.exe'
75	'628,svchost.exe'	'11944,dllhost.exe'
76	'628,svchost.exe'	'13488,WmiPrvSE.exe'
77	'628,svchost.exe'	'15012,dllhost.exe'
78	'628,svchost.exe'	'8692,dllhost.exe'
79	'628,svchost.exe'	'17336,dllhost.exe'
80	'628,svchost.exe'	'18048,dllhost.exe'
81	'628,svchost.exe'	'18400,dllhost.exe'
82	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
83	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
84	'860,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
85	'860,svchost.exe'	'2968,audiodg.exe'
86	'860,svchost.exe'	'3920,audiodg.exe'
87	'860,svchost.exe'	'8648,audiodg.exe'
88	'860,svchost.exe'	'15256,audiodg.exe'
89	'860,svchost.exe'	'18084,audiodg.exe'
90	'860,svchost.exe'	'19844,audiodg.exe'
91	'896,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
92	'896,svchost.exe'	'HID.DLL,C:WindowsSystem32HID.DLL'
93	'896,svchost.exe'	'1152,dwm.exe'
94	'896,svchost.exe'	'17296,wisptis.exe'
95	'924,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'

96	'924,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
97	'924,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
98	'924,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
99	'924,svchost.exe'	'7156,consent.exe'
100	'1004,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
101	'1004,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
102	'1228,spoolsv.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
103	'1256,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
104	'1380,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
105	'1424,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
106	'1876,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
107	'1152,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
108	'1128,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
109	'1096,XXX'	'1340,explorer.exe'
110	'1340,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
111	'1340,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
112	'1340,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
113	'1340,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
114	'1340,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
115	'1340,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
116	'1340,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
117	'1340,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
118	'1340,explorer.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
119	'1340,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
120	'1340,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
121	'1340,explorer.exe'	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
122	'1340,explorer.exe'	'2124,VBoxTray.exe'
123	'1340,explorer.exe'	'2132,MySQLNotifier.exe'
124	'1340,explorer.exe'	'1280,mintty.exe'
125	'1340,explorer.exe'	'624,notepad++.exe'
126	'1340,explorer.exe'	'3248,cmd.exe'
127	'1340,explorer.exe'	'3500,firefox.exe'
128	'1340,explorer.exe'	'3184,cmd.exe'
129	'1340,explorer.exe'	'3316,Wireshark.exe'
130	'1340,explorer.exe'	'4100,FoxitReader.exe'
131	'1340,explorer.exe'	'4832,mintty.exe'
132	'1340,explorer.exe'	'5156,firefox.exe'
133	'1340,explorer.exe'	'6972,zsb.exe'
134	**'1340,explorer.exe'**	**'6480,bot.exe'**
135	'1340,explorer.exe'	'19200,firefox.exe'
136	'1340,explorer.exe'	'7280,cmd.exe'
137	'1340,explorer.exe'	'7668,cmd.exe'
138	'1340,explorer.exe'	'7896,firefox.exe'
139	'1340,explorer.exe'	'7748,cmd.exe'
140	'1340,explorer.exe'	'8296,notepad++.exe'
141	'1340,explorer.exe'	'8336,Wireshark.exe'
142	'1340,explorer.exe'	'8888,FoxitReader.exe'
143	'1340,explorer.exe'	'8616,mintty.exe'
144	'1340,explorer.exe'	'10036,iexplore.exe'
145	'1340,explorer.exe'	'11980,iexplore.exe'
146	'1340,explorer.exe'	'12172,iexplore.exe'

147	'1340,explorer.exe'	'13668,iexplore.exe'
148	'1340,explorer.exe'	'15228,calc.exe'
149	'1340,explorer.exe'	'15316,notepad++.exe'
150	'1340,explorer.exe'	'16652,firefox.exe'
151	'1340,explorer.exe'	'17160,mip.exe'
152	'1340,explorer.exe'	'17792,mspaint.exe'
153	'1340,explorer.exe'	'18476,FoxitReader.exe'
154	'1340,explorer.exe'	'18780,StikyNot.exe'
155	'1340,explorer.exe'	'18980,StikyNot.exe'
156	'2124,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
157	'2132,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
158	'2144,XXX'	'2296,jusched.exe'
159	'2296,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
160	'2440,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
161	'2440,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
162	'2596,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
163	'2596,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
164	'2596,SearchIndexer.exe'	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
165	'2596,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
166	'2596,SearchIndexer.exe'	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
167	'2596,SearchIndexer.exe'	'4328,SearchProtocolHost.exe'
168	'2596,SearchIndexer.exe'	'4340,SearchFilterHost.exe'
169	'2596,SearchIndexer.exe'	'4720,SearchProtocolHost.exe'
170	'2596,SearchIndexer.exe'	'4764,SearchFilterHost.exe'
171	'2596,SearchIndexer.exe'	'5272,SearchProtocolHost.exe'
172	'2596,SearchIndexer.exe'	'5344,SearchFilterHost.exe'
173	'2596,SearchIndexer.exe'	'9060,SearchProtocolHost.exe'
174	'2596,SearchIndexer.exe'	'9100,SearchFilterHost.exe'
175	'2596,SearchIndexer.exe'	'9920,SearchProtocolHost.exe'
176	'2596,SearchIndexer.exe'	'9988,SearchFilterHost.exe'
177	'2596,SearchIndexer.exe'	'10660,SearchProtocolHost.exe'
178	'2596,SearchIndexer.exe'	'10736,SearchFilterHost.exe'
179	'2596,SearchIndexer.exe'	'10496,SearchProtocolHost.exe'
180	'2596,SearchIndexer.exe'	'11204,SearchFilterHost.exe'

181	'2596,SearchIndexer.exe'	'12316,SearchProtocolHost.exe'
182	'2596,SearchIndexer.exe'	'12348,SearchFilterHost.exe'
183	'2596,SearchIndexer.exe'	'11584,SearchFilterHost.exe'
184	'2596,SearchIndexer.exe'	'13908,SearchProtocolHost.exe'
185	'2596,SearchIndexer.exe'	'13928,SearchFilterHost.exe'
186	'2596,SearchIndexer.exe'	'13376,SearchProtocolHost.exe'
187	'2596,SearchIndexer.exe'	'13412,SearchFilterHost.exe'
188	'2596,SearchIndexer.exe'	'15684,SearchProtocolHost.exe'
189	'2596,SearchIndexer.exe'	'15704,SearchFilterHost.exe'
190	'2596,SearchIndexer.exe'	'18308,SearchProtocolHost.exe'
191	'2596,SearchIndexer.exe'	'18328,SearchFilterHost.exe'
192	'2596,SearchIndexer.exe'	'18836,SearchProtocolHost.exe'
193	'2596,SearchIndexer.exe'	'18856,SearchFilterHost.exe'
194	'2596,SearchIndexer.exe'	'18896,SearchProtocolHost.exe'
195	'2820,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
196	'2820,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
197	'208,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
198	'700,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
199	'944,XXX'	'2340,taskmgr.exe'
200	'2340,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
201	'1280,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
202	'3008,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
203	'1060,XXX'	'2936,bash.exe'
204	'2936,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
205	'1036,XXX'	'3040,driver_endpoint_netconn.exe'
206	'3040,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
207	'624,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
208	'3248,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
209	'3248,cmd.exe'	'3316,java.exe'
210	'3248,cmd.exe'	'3368,java.exe'
211	'3256,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
212	'3316,java.exe'	'3276,dumpcap.exe'
213	'3368,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
214	'3500,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
215	'3500,firefox.exe'	'3664,firefox.exe'
216	'3664,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
217	'3184,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
218	'3184,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'

219	'3184,cmd.exe'	'3232,NETSTAT.EXE'
220	'3192,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
221	'3232,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
222	'3232,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
223	'3316,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
224	'3316,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
225	'3276,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
226	'3320,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
227	'4100,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
228	'4328,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
229	'4340,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
230	'4832,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
231	'4868,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
232	'4888,XXX'	'4900,bash.exe'
233	'4900,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
234	'4720,SearchProtocolHost.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
235	'4764,SearchFilterHost.exe'	'OffFilt.dll,C:Windowssystem32OffFilt.dll'
236	'5660,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
237	'5272,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
238	'5272,SearchProtocolHost.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
239	'5344,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
240	'5344,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
241	'5156,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
242	'5156,firefox.exe'	'5452,firefox.exe'
243	'5452,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
244	'6192,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
245	'6404,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
246	'6540,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
247	'6764,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
248	'6904,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
249	'6940,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
250	'6972,zsb.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
251	'6972,zsb.exe'	'7036,notepad.exe'
252	'7036,notepad.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
253	'6336,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
254	'6300,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
255	**'6480,bot.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
256	**'6480,bot.exe'**	**'6484,xusa.exe'**
257	**'6484,xusa.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
258	'19200,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
259	'19200,firefox.exe'	'19972,pingsender.exe'
260	'19200,firefox.exe'	'19372,firefox.exe'
261	'6548,WinMail.exe'	'CFGMGR32.dll,C:Windowssystem32CFGMGR32.dll'
262	'6872,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'

263	'6184,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
264	'7280,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
265	'7280,cmd.exe'	'7412,java.exe'
266	'7288,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
267	'7412,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
268	'7412,java.exe'	'7576,java.exe'
269	'7576,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
270	'7584,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
271	'7668,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
272	'7668,cmd.exe'	'7780,java.exe'
273	'7676,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
274	'7780,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
275	'7780,java.exe'	'9800,java.exe'
276	'7896,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
277	'7896,firefox.exe'	'8064,firefox.exe'
278	'7896,firefox.exe'	'9928,pingsender.exe'
279	'8064,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
280	'7748,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
281	'7748,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
282	'7748,cmd.exe'	'8208,NETSTAT.EXE'
283	'7404,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
284	'8208,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
285	'8208,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
286	'8296,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
287	'8336,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
288	'8336,Wireshark.exe'	'8396,gspawn-win64-helper.exe'
289	'8336,Wireshark.exe'	'8472,dumpcap.exe'
290	'8396,gspawn-win64-helper.exe'	'8408,androiddump.exe'
291	'8472,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
292	'8480,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
293	'8888,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
294	'9060,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
295	'9060,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
296	'9100,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
297	'9100,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
298	'8616,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
299	'8640,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
300	'8728,XXX'	'8716,bash.exe'
301	'8716,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
302	'9800,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
303	'9808,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
304	'10036,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
305	'10036,iexplore.exe'	'10096,iexplore.exe'
306	'10036,iexplore.exe'	'9952,iexplore.exe'
307	'10036,iexplore.exe'	'10588,iexplore.exe'
308	'10096,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

309	'9920,SearchProtocolHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
310	'9988,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
311	'9952,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
312	'9976,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
313	'10588,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
314	'10660,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
315	'10736,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
316	'10496,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
317	'11204,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
318	'11908,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
319	'11944,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
320	'11980,iexplore.exe'	'npmproxy.dll,C:WindowsSystem32npmproxy.dll'
321	'11980,iexplore.exe'	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
322	'11980,iexplore.exe'	'12032,iexplore.exe'
323	'12032,iexplore.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
324	'12172,iexplore.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
325	'12172,iexplore.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
326	'12172,iexplore.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
327	'12172,iexplore.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
328	'12172,iexplore.exe'	'npmproxy.dll,C:WindowsSystem32npmproxy.dll'
329	'12172,iexplore.exe'	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
330	'12172,iexplore.exe'	'msfeeds.dll,C:Windowssystem32msfeeds.dll'
331	'12172,iexplore.exe'	'Secur32.dll,C:WindowsSystem32Secur32.dll'
332	'12172,iexplore.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
333	'12172,iexplore.exe'	'slc.dll,C:Windowssystem32slc.dll'
334	'12172,iexplore.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
335	'12172,iexplore.exe'	'wer.dll,C:Windowssystem32wer.dll'
336	'12172,iexplore.exe'	'12224,iexplore.exe'
337	'12172,iexplore.exe'	'11772,iexplore.exe'
338	'12224,iexplore.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
339	'12224,iexplore.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
340	'12224,iexplore.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
341	'12224,iexplore.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
342	'12224,iexplore.exe'	'WINSPOOL.DRV,C:WindowsSystem32WINSPOOL.DRV'
343	'12224,iexplore.exe'	'msimg32.dll,C:Windowssystem32msimg32.dll'
344	'12224,iexplore.exe'	'vgx.dll,C:Program FilesCommon FilesMicrosoft SharedVGXvgx.dll'
345	'12224,iexplore.exe'	'T2EMBED.DLL,C:Windowssystem32T2EMBED.DLL'
346	'11772,iexplore.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
347	'11772,iexplore.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
348	'11772,iexplore.exe'	'WINSPOOL.DRV,C:WindowsSystem32WINSPOOL.DRV'
349	'11772,iexplore.exe'	'T2EMBED.DLL,C:Windowssystem32T2EMBED.DLL'
350	'11772,iexplore.exe'	'Dxtmsft.dll,C:WindowsSystem32Dxtmsft.dll'
351	'11772,iexplore.exe'	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
352	'12316,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'

353	'12348,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
354	'11584,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
355	'13488,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
356	'13668,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
357	'13668,iexplore.exe'	'13724,iexplore.exe'
358	'13668,iexplore.exe'	'15480,iexplore.exe'
359	'13724,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
360	'13908,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
361	'13928,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
362	'13376,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
363	'13412,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
364	'15012,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
365	'15228,calc.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
366	'8692,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
367	'15316,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
368	'15480,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
369	'15684,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
370	'15704,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
371	'16652,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
372	'16652,firefox.exe'	'16820,firefox.exe'
373	'16820,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
374	'17336,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
375	'17160,mip.exe'	'mshwgst.dll,C:Program FilesCommon FilesMicrosoft SharedInkmshwgst.dll'
376	'17160,mip.exe'	'mraut.DLL,C:Program FilesCommon Filesmicrosoft sharedinkmraut.DLL'
377	'17296,wisptis.exe'	tpcps.dll,C:Program FilesCommon FilesMicrosoft SharedInkpcps.dll'
378	'17792,mspaint.exe'	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
379	'17792,mspaint.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
380	'17792,mspaint.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
381	'17792,mspaint.exe'	'SAMLIB.dll,C:Windowssystem32SAMLIB.dll'
382	'17820,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
383	'18048,dllhost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
384	'18308,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
385	'18328,SearchFilterHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
386	'18328,SearchFilterHost.exe'	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
387	'18400,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
388	'18476,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
389	'18780,StikyNot.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
390	'18836,SearchProtocolHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
391	'18856,SearchFilterHost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'

392	'18896,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
393	'18980,StikyNot.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
394	'19372,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

7.2.2 Zeus Malware – Instance 2

Table 97: Zeus Malware Instance 2 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,XXX'
6	'360,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'400,wininit.exe'
9	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
10	'412,XXX'
11	'424,csrss.exe'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'504,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'520,lsass.exe'
17	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
18	'psbase.dll,C:Windowssystem32psbase.dll'
19	'532,lsm.exe'
20	'628,svchost.exe'
21	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
22	'692,VBoxService.exe'
23	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
24	'756,svchost.exe'
25	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
26	'852,svchost.exe'
27	'netutils.dll,C:WindowsSystem32netutils.dll'
28	'892,svchost.exe'
29	'credssp.dll,C:WindowsSystem32credssp.dll'
30	'928,svchost.exe'
31	'AVRT.dll,c:windowssystem32AVRT.dll'
32	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
33	'msxml3.dll,C:WindowsSystem32msxml3.dll'
34	tschannel.dll,C:Windowssystem32schannel.dll'
35	'344,svchost.exe'
36	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
37	'300,svchost.exe'
38	'SensApi.dll,C:Windowssystem32SensApi.dll'
39	'sfc_os.dll,C:Windowssystem32sfc_os.dll'
40	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
41	'1188,spoolsv.exe'
42	'1216,svchost.exe'
43	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
44	'pnpts.dll,C:Windowssystem32pnpts.dll'

45	'1376,svchost.exe'
46	'SXS.DLL,C:Windowssystem32SXS.DLL'
47	'1404,FoxitConnectedPDFService.exe'
48	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
49	'1920,svchost.exe'
50	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
51	'1632,dwm.exe'
52	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
53	'1580,XXX'
54	'1752,explorer.exe'
55	'MLANG.dll,C:Windowssystem32MLANG.dll'
56	thumbcache.dll,C:Windowssystem32humbcache.dll'
57	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
58	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
59	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
60	'tquery.dll,C:Windowssystem32query.dll'
61	'MsftEdit.dll,C:Windowssystem32MsftEdit.dll'
62	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
63	'1780,taskhost.exe'
64	'midimap.dll,C:Windowssystem32midimap.dll'
65	'2128,VBoxTray.exe'
66	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
67	'2144,MySQLNotifier.exe'
68	'2164,XXX'
69	'2240,jusched.exe'
70	'2440,WmiPrvSE.exe'
71	'VERSION.dll,C:Windowssystem32VERSION.dll'
72	'2604,SearchIndexer.exe'
73	'NLSLexicons0007.dll,C:WindowsSystem32NLSLexicons0007.dll'
74	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
75	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
76	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
77	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
78	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
79	'2848,wmpnetwk.exe'
80	'provsvc.dll,C:WindowsSystem32provsvc.dll'
81	'2032,sppsvc.exe'
82	'2924,svchost.exe'
83	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
84	'2120,mintty.exe'
85	'apphelp.dll,C:Windowssystem32apphelp.dll'
86	'1200,conhost.exe'
87	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
88	'2168,XXX'
89	'2516,bash.exe'
90	'authz.dll,C:Windowssystem32authz.dll'
91	'1000,zsb.exe'
92	'1896,audiodg.exe'
93	'3444,SearchProtocolHost.exe'
94	'profapi.dll,C:Windowssystem32profapi.dll'
95	'3824,SearchFilterHost.exe'

96	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
97	'3808,XXX'
98	'3764,driver_endpoint_netconn.exe'
99	'3364,firefox.exe'
100	'2284,firefox.exe'
101	'3068,dllhost.exe'
102	'3192,SearchProtocolHost.exe'
103	'3792,SearchFilterHost.exe'
104	'2352,FoxitReader.exe'
105	'3084,FoxitReaderUpdater.exe'
106	'4216,dllhost.exe'
107	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
108	'4900,mspaint.exe'
109	'oleacc.dll,C:Windowssystem32oleacc.dll'
110	'DUser.dll,C:Windowssystem32DUser.dll'
111	'4928,svchost.exe'
112	'5056,dllhost.exe'
113	'3080,notepad++.exe'
114	'4404,consent.exe'
115	'5156,dllhost.exe'
116	'IDStore.dll,C:WindowsSystem32IDStore.dll'
117	'5192,dllhost.exe'
118	**'5224,bot.exe'**
119	**'5236,voed.exe'**
120	'5640,FoxitReader.exe'
121	'21172,audiodg.exe'
122	'5260,WinMail.exe'
123	'CFGMGR32.dll,C:Windowssystem32CFGMGR32.dll'
124	'5776,SearchProtocolHost.exe'
125	'5796,SearchFilterHost.exe'
126	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
127	'5648,SearchProtocolHost.exe'
128	'5992,SearchFilterHost.exe'
129	'6200,iexplore.exe'
130	'6252,iexplore.exe'
131	'6512,iexplore.exe'
132	'6696,SearchProtocolHost.exe'
133	'6984,calc.exe'
134	'8168,iexplore.exe'
135	'7728,SearchProtocolHost.exe'
136	'7780,SearchFilterHost.exe'
137	'8580,taskhost.exe'
138	'9964,cmd.exe'
139	'8796,conhost.exe'
140	'10328,java.exe'
141	'10600,cmd.exe'
142	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
143	'10608,conhost.exe'
144	'10636,NETSTAT.EXE'
145	'winrnr.dll,C:WindowsSystem32winrnr.dll'
146	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'

147	'10732,Wireshark.exe'
148	**'10824,dumpcap.exe'**
149	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
150	'10880,dumpcap.exe'
151	'10888,conhost.exe'
152	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
153	'10684,FoxitReader.exe'
154	'10988,SearchProtocolHost.exe'
155	'11008,SearchFilterHost.exe'
156	'11120,mintty.exe'
157	'11184,conhost.exe'
158	'11200,XXX'
159	'11236,bash.exe'
160	'12112,SearchProtocolHost.exe'
161	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
162	'12132,SearchFilterHost.exe'
163	'OffFilt.dll,C:Windowssystem32OffFilt.dll'
164	'12756,java.exe'
165	'12788,conhost.exe'
166	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
167	'12744,SearchProtocolHost.exe'
168	'12776,SearchFilterHost.exe'
169	'12560,SearchProtocolHost.exe'
170	'12656,SearchFilterHost.exe'
171	'13884,iexplore.exe'
172	'14036,SearchProtocolHost.exe'
173	'14056,SearchFilterHost.exe'
174	'13856,Wireshark.exe'
175	'14004,gspawn-win64-helper.exe'
176	'14028,androiddump.exe'
177	'DUI70.dll,C:Windowssystem32DUI70.dll'
178	'14268,dumpcap.exe'
179	'14316,conhost.exe'
180	'13560,dumpcap.exe'
181	'13584,conhost.exe'
182	'14124,SearchProtocolHost.exe'
183	'14320,SearchFilterHost.exe'
184	'14596,dllhost.exe'
185	'14944,SearchProtocolHost.exe'
186	'14964,SearchFilterHost.exe'
187	'15316,firefox.exe'
188	'15008,firefox.exe'
189	'15788,SearchProtocolHost.exe'
190	'slc.dll,C:Windowssystem32slc.dll'
191	'15888,consent.exe'
192	'16000,dllhost.exe'
193	'16036,dllhost.exe'
194	'16068,Apache_OpenOffice_4.1.3_Win_x86_install_en-US.exe'
195	'16116,SearchFilterHost.exe'
196	'16140,setup.exe'
197	'16152,vcredist_x64.exe'

198	'16168,install.exe'
199	'16204,msiexec.exe'
200	'SAMLIB.dll,C:Windowssystem32SAMLIB.dll'
201	'RSTRTMGR.DLL,C:Windowssystem32RSTRTMGR.DLL'
202	'sxsstore.dll,C:Windowssystem32sxsstore.dll'
203	'MSVCR100_CLR0400.dll,C:Windowssystem32MSVCR100_CLR0400.dll'
204	'fusion.dll,C:WindowsMicrosoft.NETFramework64v4.0.30319fusion.dll'
205	'iertutil.dll,C:Windowssystem32iertutil.dll'
206	'16252,VSSVC.exe'
207	'16288,svchost.exe'
208	'VSSAPI.DLL,C:WindowsSystem32VSSAPI.DLL'
209	'15968,TrustedInstaller.exe'
210	'smiengine.dll,C:Windowswinsxsamd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.1.7601.17514_none_678566b7ddea04a5smiengine.dll'
211	'16108,dllhost.exe'
212	'16432,vcredist_x86.exe'
213	'16456,install.exe'
214	'16608,msiexec.exe'
215	'16648,msiexec.exe'
216	'16844,msiexec.exe'
217	'16980,dllhost.exe'
218	'16504,SearchProtocolHost.exe'
219	'16548,SearchFilterHost.exe'
220	'17072,dllhost.exe'
221	'17100,swriter.exe'
222	'17108,soffice.exe'
223	'17116,soffice.bin'
224	'18228,SearchProtocolHost.exe'
225	'18252,SearchFilterHost.exe'
226	'17440,Wireshark.exe'
227	'18124,dumpcap.exe'
228	'18360,conhost.exe'
229	'17444,dumpcap.exe'
230	'17472,conhost.exe'
231	'18716,iexplore.exe'
232	'19448,taskeng.exe'
233	'19844,pingsender.exe'
234	'19856,conhost.exe'
235	'18036,MySQLInstallerConsole.exe'
236	'18528,conhost.exe'
237	'System.ServiceProcess.ni.dll,C:WindowsassemblyNativeImages_v4.0.30319_64System.ServiceProce#7b167f31f23d4aed19dfa65ad3d29480System.ServiceProcess.ni.dll'
238	'20136,iexplore.exe'
239	'20328,audiodg.exe'
240	'20192,iexplore.exe'
241	'20420,SearchProtocolHost.exe'
242	'20440,SearchFilterHost.exe'
243	'19540,iexplore.exe'
244	'20612,taskhost.exe'
245	'21276,iexplore.exe'
246	'21460,SearchProtocolHost.exe'
247	'21480,SearchFilterHost.exe'

Table 98: Zeus Malware Instance 2 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'352,XXX'	'360,csrss.exe'
5	'352,XXX'	'400,wininit.exe'
6	'360,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'400,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
8	'400,wininit.exe'	'504,services.exe'
9	'400,wininit.exe'	'520,lsass.exe'
10	'400,wininit.exe'	'532,lsm.exe'
11	'412,XXX'	'424,csrss.exe'
12	'412,XXX'	'460,winlogon.exe'
13	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
14	'424,csrss.exe'	'1200,conhost.exe'
15	'424,csrss.exe'	'8796,conhost.exe'
16	'424,csrss.exe'	'10608,conhost.exe'
17	'424,csrss.exe'	'10888,conhost.exe'
18	'424,csrss.exe'	'11184,conhost.exe'
19	'424,csrss.exe'	'12788,conhost.exe'
20	'424,csrss.exe'	'14316,conhost.exe'
21	'424,csrss.exe'	'13584,conhost.exe'
22	'424,csrss.exe'	'18360,conhost.exe'
23	'424,csrss.exe'	'17472,conhost.exe'
24	'424,csrss.exe'	'19856,conhost.exe'
25	'424,csrss.exe'	'18528,conhost.exe'
26	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
27	'504,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
28	'504,services.exe'	'628,svchost.exe'
29	'504,services.exe'	'692,VBoxService.exe'
30	'504,services.exe'	'756,svchost.exe'
31	'504,services.exe'	'852,svchost.exe'
32	'504,services.exe'	'892,svchost.exe'
33	'504,services.exe'	'928,svchost.exe'
34	'504,services.exe'	'344,svchost.exe'
35	'504,services.exe'	'300,svchost.exe'
36	'504,services.exe'	'1188,spoolsv.exe'
37	'504,services.exe'	'1216,svchost.exe'
38	'504,services.exe'	'1376,svchost.exe'

39	'504,services.exe'	'1404,FoxitConnectedPDFService.exe'
40	'504,services.exe'	'1920,svchost.exe'
41	'504,services.exe'	'1780,taskhost.exe'
42	'504,services.exe'	'2604,SearchIndexer.exe'
43	'504,services.exe'	'2848,wmpnetwk.exe'
44	'504,services.exe'	'2032,sppsvc.exe'
45	'504,services.exe'	'2924,svchost.exe'
46	'504,services.exe'	'4928,svchost.exe'
47	'504,services.exe'	'8580,taskhost.exe'
48	'504,services.exe'	'16204,msiexec.exe'
49	'504,services.exe'	'16252,VSSVC.exe'
50	'504,services.exe'	'16288,svchost.exe'
51	'504,services.exe'	'15968,TrustedInstaller.exe'
52	'504,services.exe'	'20612,taskhost.exe'
53	'520,lsass.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
54	'520,lsass.exe'	'psbase.dll,C:Windowssystem32psbase.dll'
55	'532,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
56	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
57	'628,svchost.exe'	'2440,WmiPrvSE.exe'
58	'628,svchost.exe'	'3068,dllhost.exe'
59	'628,svchost.exe'	'4216,dllhost.exe'
60	'628,svchost.exe'	'5056,dllhost.exe'
61	'628,svchost.exe'	'5156,dllhost.exe'
62	'628,svchost.exe'	'5192,dllhost.exe'
63	'628,svchost.exe'	'5260,WinMail.exe'
64	'628,svchost.exe'	'14596,dllhost.exe'
65	'628,svchost.exe'	'16000,dllhost.exe'
66	'628,svchost.exe'	'16036,dllhost.exe'
67	'628,svchost.exe'	'16108,dllhost.exe'
68	'628,svchost.exe'	'16980,dllhost.exe'
69	'628,svchost.exe'	'17072,dllhost.exe'
70	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
71	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
72	'852,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
73	'852,svchost.exe'	'1896,audiodg.exe'
74	'852,svchost.exe'	'21172,audiodg.exe'
75	'852,svchost.exe'	'20328,audiodg.exe'
76	'892,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
77	'892,svchost.exe'	'1632,dwm.exe'
78	'928,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
79	'928,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'

80	'928,svchost.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
81	'928,svchost.exe'	tschannel.dll,C:Windowssystem32schannel.dll'
82	'928,svchost.exe'	'4404,consent.exe'
83	'928,svchost.exe'	'15888,consent.exe'
84	'928,svchost.exe'	'19448,taskeng.exe'
85	'344,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
86	'300,svchost.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
87	'300,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
88	'300,svchost.exe'	'sfc_os.dll,C:Windowssystem32sfc_os.dll'
89	'300,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
90	'1188,spoolsv.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
91	'1216,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
92	'1216,svchost.exe'	'pnpts.dll,C:Windowssystem32pnpts.dll'
93	'1376,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
94	'1404,FoxitConnected PDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
95	'1920,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
96	'1632,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
97	'1580,XXX'	'1752,explorer.exe'
98	'1752,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
99	'1752,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
100	'1752,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
101	'1752,explorer.exe'	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
102	'1752,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
103	'1752,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
104	'1752,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
105	'1752,explorer.exe'	'MsftEdit.dll,C:Windowssystem32MsftEdit.dll'
106	'1752,explorer.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
107	'1752,explorer.exe'	'2128,VBoxTray.exe'
108	'1752,explorer.exe'	'2144,MySQLNotifier.exe'
109	'1752,explorer.exe'	'2120,mintty.exe'
110	'1752,explorer.exe'	'1000,zsb.exe'
111	'1752,explorer.exe'	'3364,firefox.exe'
112	'1752,explorer.exe'	'4900,mspaint.exe'
113	'1752,explorer.exe'	'3080,notepad++.exe'
114	**'1752,explorer.exe'**	**'5224,bot.exe'**
115	'1752,explorer.exe'	'5640,FoxitReader.exe'
116	'1752,explorer.exe'	'6200,iexplore.exe'
117	'1752,explorer.exe'	'6984,calc.exe'
118	'1752,explorer.exe'	'9964,cmd.exe'
119	'1752,explorer.exe'	'10600,cmd.exe'
120	'1752,explorer.exe'	'10732,Wireshark.exe'

121	'1752,explorer.exe'	'10684,FoxitReader.exe'
122	'1752,explorer.exe'	'11120,mintty.exe'
123	'1752,explorer.exe'	'13856,Wireshark.exe'
124	'1752,explorer.exe'	'15316,firefox.exe'
125	'1752,explorer.exe'	'17100,swriter.exe'
126	'1752,explorer.exe'	'17440,Wireshark.exe'
127	'1752,explorer.exe'	'20136,iexplore.exe'
128	'1780,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
129	'2128,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
130	'2144,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
131	'2164,XXX'	'2240,jusched.exe'
132	'2240,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
133	'2440,WmiPrvSE.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
134	'2604,SearchIndexer.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
135	'2604,SearchIndexer.exe'	'NLSLexicons0007.dll,C:WindowsSystem32NLSLexicons0007.dll'
136	'2604,SearchIndexer.exe'	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
137	'2604,SearchIndexer.exe'	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
138	'2604,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
139	'2604,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
140	'2604,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
141	'2604,SearchIndexer.exe'	'3444,SearchProtocolHost.exe'
142	'2604,SearchIndexer.exe'	'3824,SearchFilterHost.exe'
143	'2604,SearchIndexer.exe'	'3192,SearchProtocolHost.exe'
144	'2604,SearchIndexer.exe'	'3792,SearchFilterHost.exe'
145	'2604,SearchIndexer.exe'	'5776,SearchProtocolHost.exe'
146	'2604,SearchIndexer.exe'	'5796,SearchFilterHost.exe'
147	'2604,SearchIndexer.exe'	'5648,SearchProtocolHost.exe'
148	'2604,SearchIndexer.exe'	'5992,SearchFilterHost.exe'
149	'2604,SearchIndexer.exe'	'6696,SearchProtocolHost.exe'
150	'2604,SearchIndexer.exe'	'7728,SearchProtocolHost.exe'
151	'2604,SearchIndexer.exe'	'7780,SearchFilterHost.exe'
152	'2604,SearchIndexer.exe'	'10988,SearchProtocolHost.exe'

153	'2604,SearchIndexer.exe'	'11008,SearchFilterHost.exe'
154	'2604,SearchIndexer.exe'	'12112,SearchProtocolHost.exe'
155	'2604,SearchIndexer.exe'	'12132,SearchFilterHost.exe'
156	'2604,SearchIndexer.exe'	'12744,SearchProtocolHost.exe'
157	'2604,SearchIndexer.exe'	'12776,SearchFilterHost.exe'
158	'2604,SearchIndexer.exe'	'12560,SearchProtocolHost.exe'
159	'2604,SearchIndexer.exe'	'12656,SearchFilterHost.exe'
160	'2604,SearchIndexer.exe'	'14036,SearchProtocolHost.exe'
161	'2604,SearchIndexer.exe'	'14056,SearchFilterHost.exe'
162	'2604,SearchIndexer.exe'	'14124,SearchProtocolHost.exe'
163	'2604,SearchIndexer.exe'	'14320,SearchFilterHost.exe'
164	'2604,SearchIndexer.exe'	'14944,SearchProtocolHost.exe'
165	'2604,SearchIndexer.exe'	'14964,SearchFilterHost.exe'
166	'2604,SearchIndexer.exe'	'15788,SearchProtocolHost.exe'
167	'2604,SearchIndexer.exe'	'16116,SearchFilterHost.exe'
168	'2604,SearchIndexer.exe'	'16504,SearchProtocolHost.exe'
169	'2604,SearchIndexer.exe'	'16548,SearchFilterHost.exe'
170	'2604,SearchIndexer.exe'	'18228,SearchProtocolHost.exe'
171	'2604,SearchIndexer.exe'	'18252,SearchFilterHost.exe'
172	'2604,SearchIndexer.exe'	'20420,SearchProtocolHost.exe'
173	'2604,SearchIndexer.exe'	'20440,SearchFilterHost.exe'
174	'2604,SearchIndexer.exe'	'21460,SearchProtocolHost.exe'
175	'2604,SearchIndexer.exe'	'21480,SearchFilterHost.exe'
176	'2848,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
177	'2032,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
178	'2924,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
179	'2120,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
180	'1200,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
181	'2168,XXX'	'2516,bash.exe'
182	'2516,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
183	'1000,zsb.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

184	'3444,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
185	'3824,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
186	'3808,XXX'	'3764,driver_endpoint_netconn.exe'
187	'3764,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
188	'3364,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
189	'3364,firefox.exe'	'2284,firefox.exe'
190	'3364,firefox.exe'	'2352,FoxitReader.exe'
191	'2284,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
192	'3068,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
193	'3192,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
194	'3792,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
195	'2352,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
196	'2352,FoxitReader.exe'	'3084,FoxitReaderUpdater.exe'
197	'3084,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
198	'4216,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
199	'4900,mspaint.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
200	'4900,mspaint.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
201	'4928,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
202	'5056,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
203	'3080,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
204	'4404,consent.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
205	'5156,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
206	'5192,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
207	**'5224,bot.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
208	**'5224,bot.exe'**	**'5236,voed.exe'**
209	**'5236,voed.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
210	'5260,WinMail.exe'	'CFGMGR32.dll,C:Windowssystem32CFGMGR32.dll'
211	'5776,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
212	'5796,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
213	'5648,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
214	'5992,SearchFilterHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
215	'6200,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
216	'6200,iexplore.exe'	'6252,iexplore.exe'
217	'6200,iexplore.exe'	'6512,iexplore.exe'
218	'6200,iexplore.exe'	'8168,iexplore.exe'
219	'6200,iexplore.exe'	'13884,iexplore.exe'

220	'6200,iexplore.exe'	'18716,iexplore.exe'
221	'6252,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
222	'6512,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
223	'6696,SearchProtocol Host.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
224	'6984,calc.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
225	'8168,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
226	'7728,SearchProtocol Host.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
227	'7780,SearchFilterHost .exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
228	'8580,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
229	'9964,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
230	'9964,cmd.exe'	'10328,java.exe'
231	'8796,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
232	'10328,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
233	'10328,java.exe'	'12756,java.exe'
234	'10600,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
235	'10600,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
236	'10600,cmd.exe'	'10636,NETSTAT.EXE'
237	'10608,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
238	'10636,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
239	'10636,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
240	'10732,Wireshark.exe'	'10824,dumpcap.exe'
241	'10732,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
242	'10732,Wireshark.exe'	'10880,dumpcap.exe'
243	'10880,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
244	'10888,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
245	'10684,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
246	'10988,SearchProtocol Host.exe'	'authz.dll,C:Windowssystem32authz.dll'
247	'11008,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
248	'11120,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
249	'11184,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
250	'11200,XXX'	'11236,bash.exe'
251	'11236,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
252	'12112,SearchProtocol Host.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
253	'12132,SearchFilterHost.exe'	'OffFilt.dll,C:Windowssystem32OffFilt.dll'
254	'12756,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
255	'12788,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
256	'12744,SearchProtocol Host.exe'	'authz.dll,C:Windowssystem32authz.dll'

257	'12744,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
258	'12776,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
259	'12776,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
260	'12560,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
261	'12656,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
262	'13884,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
263	'14036,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
264	'14056,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
265	'13856,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
266	'13856,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
267	'13856,Wireshark.exe'	'14004,gspawn-win64-helper.exe'
268	'13856,Wireshark.exe'	'DUI70.dll,C:Windowssystem32DUI70.dll'
269	'13856,Wireshark.exe'	'14268,dumpcap.exe'
270	'13856,Wireshark.exe'	'13560,dumpcap.exe'
271	'14004,gspawn-win64-helper.exe'	'14028,androiddump.exe'
272	'14268,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
273	'14316,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
274	'13560,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
275	'13584,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
276	'14124,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
277	'14320,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
278	'14596,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
279	'14944,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
280	'14964,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
281	'14964,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
282	'15316,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
283	'15316,firefox.exe'	'15008,firefox.exe'
284	'15316,firefox.exe'	'16068,Apache_OpenOffice_4.1.3_Win_x86_install_en-US.exe'
285	'15316,firefox.exe'	'19844,pingsender.exe'
286	'15008,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
287	'15788,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
288	'15788,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
289	'15788,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
290	'15888,consent.exe'	'midimap.dll,C:Windowssystem32midimap.dll'

291	'16000,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
292	'16036,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
293	'16068,Apache_OpenOffice_4.1.3_Win_x86_install_en-US.exe'	'16140,setup.exe'
294	'16116,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
295	'16116,SearchFilterHost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
296	'16140,setup.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
297	'16140,setup.exe'	'16152,vcredist_x64.exe'
298	'16140,setup.exe'	'16432,vcredist_x86.exe'
299	'16140,setup.exe'	'16608,msiexec.exe'
300	'16152,vcredist_x64.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
301	'16152,vcredist_x64.exe'	'16168,install.exe'
302	'16168,install.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
303	'16204,msiexec.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
304	'16204,msiexec.exe'	'SAMLIB.dll,C:Windowssystem32SAMLIB.dll'
305	'16204,msiexec.exe'	'RSTRTMGR.DLL,C:Windowssystem32RSTRTMGR.DLL'
306	'16204,msiexec.exe'	'sxsstore.dll,C:Windowssystem32sxsstore.dll'
307	'16204,msiexec.exe'	'MSVCR100_CLR0400.dll,C:Windowssystem32MSVCR100_CLR0400.dll'
308	'16204,msiexec.exe'	'fusion.dll,C:WindowsMicrosoft.NETFramework64v4.0.30319fusion.dll'
309	'16204,msiexec.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
310	'16204,msiexec.exe'	'16648,msiexec.exe'
311	'16204,msiexec.exe'	'16844,msiexec.exe'
312	'16252,VSSVC.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
313	'16288,svchost.exe'	'VSSAPI.DLL,C:WindowsSystem32VSSAPI.DLL'
314	'15968,TrustedInstaller.exe'	'smiengine.dll,C:Windowswinsxsamd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.1.7601.17514_none_678566b7ddea04a5smiengine.dll'
315	'16108,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
316	'16432,vcredist_x86.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
317	'16432,vcredist_x86.exe'	'16456,install.exe'
318	'16456,install.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
319	'16608,msiexec.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
320	'16648,msiexec.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
321	'16844,msiexec.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
322	'16980,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
323	'16504,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
324	'16548,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
325	'17072,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'

326	'17100,swriter.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
327	'17100,swriter.exe'	'17108,soffice.exe'
328	'17108,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
329	'17108,soffice.exe'	'17116,soffice.bin'
330	'17116,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
331	'18228,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
332	'18252,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
333	'17440,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
334	'17440,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
335	'17440,Wireshark.exe'	'18124,dumpcap.exe'
336	'17440,Wireshark.exe'	'17444,dumpcap.exe'
337	'18124,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
338	'18360,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
339	'17444,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
340	'17472,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
341	'18716,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
342	'19448,taskeng.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
343	'19448,taskeng.exe'	'18036,MySQLInstallerConsole.exe'
344	'18036,MySQLInstallerConsole.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
345	'18036,MySQLInstallerConsole.exe'	'System.ServiceProcess.ni.dll,C:WindowsassemblyNativeImages_v4.0.30319_64System.ServiceProce#7b167f31f23d4aed19dfa65ad3d29480System.ServiceProcess.ni.dll'
346	'18528,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
347	'20136,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
348	'20136,iexplore.exe'	'20192,iexplore.exe'
349	'20136,iexplore.exe'	'19540,iexplore.exe'
350	'20136,iexplore.exe'	'21276,iexplore.exe'
351	'20192,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
352	'20420,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
353	'20440,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
354	'19540,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
355	'20612,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
356	'21276,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
357	'21460,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
358	'21480,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'

7.2.3 Citadel Malware – Instance 1

Table 99: Citadel Malware Instance 1 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'356,XXX'
6	'364,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'404,wininit.exe'
9	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
10	'412,XXX'
11	'424,csrss.exe'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'504,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'528,lsm.exe'
17	'520,lsass.exe'
18	'netutils.dll,C:Windowssystem32netutils.dll'
19	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
20	'psbase.dll,C:Windowssystem32psbase.dll'
21	'632,svchost.exe'
22	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
23	'696,VBoxService.exe'
24	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
25	'760,svchost.exe'
26	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
27	'832,svchost.exe'
28	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
29	'888,svchost.exe'
30	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
31	'920,svchost.exe'
32	'AVRT.dll,c:windowssystem32AVRT.dll'
33	'appinfo.dll,c:windowssystem32appinfo.dll'
34	'ES.DLL,C:Windowssystem32ES.DLL'
35	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'

36	'rasman.dll,C:Windowssystem32rasman.dll'
37	'372,svchost.exe'
38	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
39	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
40	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
41	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
42	'msxml3.dll,C:WindowsSystem32msxml3.dll'
43	'profapi.dll,C:Windowssystem32profapi.dll'
44	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
45	'sensapi.dll,C:Windowssystem32sensapi.dll'
46	'msxml6.dll,C:WindowsSystem32msxml6.dll'
47	'996,svchost.exe'
48	'psapi.dll,C:Windowssystem32psapi.dll'
49	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
50	'1220,spoolsv.exe'
51	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
52	'1248,svchost.exe'
53	'1376,svchost.exe'
54	'SXS.DLL,C:Windowssystem32SXS.DLL'
55	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
56	'1468,FoxitConnectedPDFService.exe'
57	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
58	'1812,svchost.exe'
59	'1980,taskhost.exe'
60	'dsrole.dll,C:Windowssystem32dsrole.dll'
61	'midimap.dll,C:Windowssystem32midimap.dll'
62	'1372,dwm.exe'
63	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
64	'1084,XXX'
65	'1972,explorer.exe'
66	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
67	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
68	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
69	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
70	'MLANG.dll,C:Windowssystem32MLANG.dll'
71	'NetworkExplorer.dll,C:Windowssystem32NetworkExplorer.dll'
72	'browcli.dll,C:Windowssystem32rowcli.dll'
73	'MsftEdit.dll,C:Windowssystem32MsftEdit.dll'
74	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
75	taskschd.dll,C:Windowssystem32askschd.dll'
76	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'

77	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
78	'2096,VBoxTray.exe'
79	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
80	'2112,MySQLNotifier.exe'
81	'2188,XXX'
82	'2220,jusched.exe'
83	'2248,update.exe'
84	'2472,WmiPrvSE.exe'
85	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
86	'perfos.dll,C:WindowsSystem32perfos.dll'
87	'2684,XXX'
88	'2736,RegSvcs.exe'
89	'2784,SearchIndexer.exe'
90	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
91	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
92	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
93	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
94	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
95	'3004,wmpnetwk.exe'
96	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
97	'provsvc.dll,C:WindowsSystem32provsvc.dll'
98	'iertutil.dll,C:Windowssystem32iertutil.dll'
99	'1532,sppsvc.exe'
100	'2228,audiodg.exe'
101	'2944,svchost.exe'
102	'416,mintty.exe'
103	'apphelp.dll,C:Windowssystem32apphelp.dll'
104	'2424,conhost.exe'
105	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
106	'1728,XXX'
107	'2980,bash.exe'
108	'authz.dll,C:Windowssystem32authz.dll'
109	'1876,XXX'
110	'2604,taskmgr.exe'
111	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
112	'1828,XXX'
113	'1484,driver_endpoint_netconn.exe'
114	'1760,taskmgr.exe'
115	'1348,dllhost.exe'
116	'IDStore.dll,C:WindowsSystem32IDStore.dll'
117	'2636,dllhost.exe'

118	'2972,taskmgr.exe'
119	'4452,audiodg.exe'
120	'3120,taskhost.exe'
121	'3764,cmd.exe'
122	'3776,conhost.exe'
123	'3880,java.exe'
124	'4032,firefox.exe'
125	'3780,firefox.exe'
126	'4572,cmd.exe'
127	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
128	'4580,conhost.exe'
129	'4628,NETSTAT.EXE'
130	'winrnr.dll,C:WindowsSystem32winrnr.dll'
131	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
132	'4736,notepad++.exe'
133	'4768,Wireshark.exe'
134	'4832,gspawn-win64-helper.exe'
135	'schannel.DLL,C:Windowssystem32schannel.DLL'
136	'msimtf.dll,C:Windowssystem32msimtf.dll'
137	'4912,dumpcap.exe'
138	'4920,conhost.exe'
139	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
140	'4844,FoxitReader.exe'
141	'4492,SearchProtocolHost.exe'
142	'4176,SearchFilterHost.exe'
143	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
144	'5340,mintty.exe'
145	'5376,conhost.exe'
146	'5392,XXX'
147	'5408,bash.exe'
148	'5820,SearchProtocolHost.exe'
149	'5480,SearchFilterHost.exe'
150	'OffFilt.dll,C:Windowssystem32OffFilt.dll'
151	'6176,plugin-container.exe'
152	'6240,FlashPlayerPlugin_22_0_0_209.exe'
153	'6260,FlashPlayerPlugin_22_0_0_209.exe'
154	'5948,dllhost.exe'
155	'6648,dllhost.exe'
156	'6788,dllhost.exe'
157	'7048,dllhost.exe'
158	'6192,dllhost.exe'

159	'6404,dllhost.exe'
160	**'4472,citadel.exe'**
161	'6432,cmd.exe'
162	'6448,conhost.exe'
163	'6288,PING.EXE'
164	'6276,notepad.exe'
165	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
166	'6308,dllhost.exe'
167	**'6480,citadel.exe'**
168	**'7028,citadel.exe'**
169	'6996,XXX'
170	**'6992,Lpgz.YVH'**
171	'7140,RegSvcs.exe'
172	'4988,consent.exe'
173	'4464,dllhost.exe'
174	'7024,dllhost.exe'
175	**'5724,soft.exe'**
176	**'6632,puxa.exe'**
177	'13016,audiodg.exe'
178	'7000,WinMail.exe'
179	'CFGMGR32.dll,C:Windowssystem32CFGMGR32.dll'
180	'7704,slui.exe'
181	'8264,iexplore.exe'
182	'8340,iexplore.exe'
183	'8532,iexplore.exe'
184	'8688,audiodg.exe'
185	'12600,slui.exe'
186	'8620,SearchProtocolHost.exe'
187	'8640,SearchFilterHost.exe'
188	'10088,WmiPrvSE.exe'
189	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
190	'10220,iexplore.exe'
191	'9380,SearchProtocolHost.exe'
192	'9396,SearchFilterHost.exe'
193	'10668,slui.exe'
194	'11020,SearchProtocolHost.exe'
195	'11040,SearchFilterHost.exe'
196	'10832,msdt.exe'
197	'10936,sdiagnhost.exe'
198	'10956,conhost.exe'
199	'13128,SearchProtocolHost.exe'

200	'13156,SearchFilterHost.exe'
201	'12744,iexplore.exe'
202	'14276,iexplore.exe'
203	'13976,SearchProtocolHost.exe'
204	'14036,SearchFilterHost.exe'
205	'14412,mspaint.exe'
206	'oleacc.dll,C:Windowssystem32oleacc.dll'
207	'DUser.dll,C:Windowssystem32DUser.dll'
208	'SAMLIB.dll,C:Windowssystem32SAMLIB.dll'
209	'WININET.dll,C:Windowssystem32WININET.dll'
210	'14440,svchost.exe'
211	'14684,dllhost.exe'
212	'14920,SearchProtocolHost.exe'
213	'slc.dll,C:Windowssystem32slc.dll'
214	'ehtrace.dll,C:Windowsehomeehtrace.dll'
215	'14940,SearchFilterHost.exe'
216	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
217	'14992,dllhost.exe'
218	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
219	'15068,dllhost.exe'
220	'15136,XXX'
221	'15152,setup_wm.exe'
222	'15300,wmplayer.exe'
223	'14728,dllhost.exe'
224	'15588,taskhost.exe'
225	'15708,dllhost.exe'
226	'16100,calc.exe'
227	'16248,cmd.exe'
228	'16256,conhost.exe'
229	'16360,java.exe'
230	'16280,slui.exe'
231	'17324,firefox.exe'
232	'17436,firefox.exe'
233	'17860,audiodg.exe'
234	'18064,cmd.exe'
235	'18072,conhost.exe'
236	'18132,NETSTAT.EXE'
237	'18224,notepad++.exe'
238	'18264,Wireshark.exe'
239	'18400,dumpcap.exe'
240	'18408,conhost.exe'

241	'18260,FoxitReader.exe'
242	'18324,FoxitReaderUpdater.exe'
243	'18856,SearchProtocolHost.exe'
244	'18876,SearchFilterHost.exe'
245	'19020,mintty.exe'
246	'19056,conhost.exe'
247	'19072,XXX'
248	'19088,bash.exe'
249	'19136,firefox.exe'

Table 100: Citadel Malware Instance 1 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'356,XXX'	'364,csrss.exe'
5	'356,XXX'	'404,wininit.exe'
6	'364,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'404,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
8	'404,wininit.exe'	'504,services.exe'
9	'404,wininit.exe'	'528,lsm.exe'
10	'404,wininit.exe'	'520,lsass.exe'
11	'412,XXX'	'424,csrss.exe'
12	'412,XXX'	'460,winlogon.exe'
13	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
14	'424,csrss.exe'	'2424,conhost.exe'
15	'424,csrss.exe'	'3776,conhost.exe'
16	'424,csrss.exe'	'4580,conhost.exe'
17	'424,csrss.exe'	'4920,conhost.exe'
18	'424,csrss.exe'	'5376,conhost.exe'
19	'424,csrss.exe'	'6448,conhost.exe'
20	'424,csrss.exe'	'10956,conhost.exe'
21	'424,csrss.exe'	'16256,conhost.exe'
22	'424,csrss.exe'	'18072,conhost.exe'
23	'424,csrss.exe'	'18408,conhost.exe'
24	'424,csrss.exe'	'19056,conhost.exe'
25	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
26	'504,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
27	'504,services.exe'	'632,svchost.exe'
28	'504,services.exe'	'696,VBoxService.exe'
29	'504,services.exe'	'760,svchost.exe'
30	'504,services.exe'	'832,svchost.exe'
31	'504,services.exe'	'888,svchost.exe'
32	'504,services.exe'	'920,svchost.exe'
33	'504,services.exe'	'372,svchost.exe'
34	'504,services.exe'	'996,svchost.exe'
35	'504,services.exe'	'1220,spoolsv.exe'
36	'504,services.exe'	'1248,svchost.exe'
37	'504,services.exe'	'1376,svchost.exe'
38	'504,services.exe'	'1468,FoxitConnectedPDFService.exe'
39	'504,services.exe'	'1812,svchost.exe'

40	'504,services.exe'	'1980,taskhost.exe'
41	'504,services.exe'	'2784,SearchIndexer.exe'
42	'504,services.exe'	'3004,wmpnetwk.exe'
43	'504,services.exe'	'1532,sppsvc.exe'
44	'504,services.exe'	'2944,svchost.exe'
45	'504,services.exe'	'3120,taskhost.exe'
46	'504,services.exe'	'14440,svchost.exe'
47	'504,services.exe'	'15588,taskhost.exe'
48	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
49	'520,lsass.exe'	'netutils.dll,C:Windowssystem32netutils.dll'
50	'520,lsass.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
51	'520,lsass.exe'	'psbase.dll,C:Windowssystem32psbase.dll'
52	'632,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
53	'632,svchost.exe'	'2472,WmiPrvSE.exe'
54	'632,svchost.exe'	'1348,dllhost.exe'
55	'632,svchost.exe'	'2636,dllhost.exe'
56	'632,svchost.exe'	'5948,dllhost.exe'
57	'632,svchost.exe'	'6648,dllhost.exe'
58	'632,svchost.exe'	'6788,dllhost.exe'
59	'632,svchost.exe'	'7048,dllhost.exe'
60	'632,svchost.exe'	'6192,dllhost.exe'
61	'632,svchost.exe'	'6404,dllhost.exe'
62	'632,svchost.exe'	'6308,dllhost.exe'
63	'632,svchost.exe'	'4464,dllhost.exe'
64	'632,svchost.exe'	'7024,dllhost.exe'
65	'632,svchost.exe'	'7000,WinMail.exe'
66	'632,svchost.exe'	'7704,slui.exe'
67	'632,svchost.exe'	'12600,slui.exe'
68	'632,svchost.exe'	'10088,WmiPrvSE.exe'
69	'632,svchost.exe'	'10668,slui.exe'
70	'632,svchost.exe'	'10936,sdiagnhost.exe'
71	'632,svchost.exe'	'14684,dllhost.exe'
72	'632,svchost.exe'	'14992,dllhost.exe'
73	'632,svchost.exe'	'15068,dllhost.exe'
74	'632,svchost.exe'	'14728,dllhost.exe'
75	'632,svchost.exe'	'15708,dllhost.exe'
76	'632,svchost.exe'	'16280,slui.exe'
77	'696,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
78	'760,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
79	'832,svchost.exe'	'netutils.dll,C:Windowssystem32netutils.dll'
80	'832,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'

81	'832,svchost.exe'	'2228,audiodg.exe'
82	'832,svchost.exe'	'4452,audiodg.exe'
83	'832,svchost.exe'	'13016,audiodg.exe'
84	'832,svchost.exe'	'8688,audiodg.exe'
85	'832,svchost.exe'	'17860,audiodg.exe'
86	'888,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
87	'888,svchost.exe'	'1372,dwm.exe'
88	'920,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
89	'920,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
90	'920,svchost.exe'	'ES.DLL,C:Windowssystem32ES.DLL'
91	'920,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
92	'920,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
93	'920,svchost.exe'	'4988,consent.exe'
94	'372,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
95	'372,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
96	'372,svchost.exe'	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
97	'372,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
98	'372,svchost.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
99	'372,svchost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
100	'372,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
101	'372,svchost.exe'	'sensapi.dll,C:Windowssystem32sensapi.dll'
102	'372,svchost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
103	'996,svchost.exe'	'sensapi.dll,C:Windowssystem32sensapi.dll'
104	'996,svchost.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
105	'996,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
106	'1220,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
107	'1248,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
108	'1376,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
109	'1376,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
110	'1376,svchost.exe'	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
111	'1468,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
112	'1812,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
113	'1980,taskhost.exe'	'dsrole.dll,C:Windowssystem32dsrole.dll'
114	'1980,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
115	'1372,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
116	'1084,XXX'	'1972,explorer.exe'
117	'1972,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
118	'1972,explorer.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
119	'1972,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
120	'1972,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'

121	'1972,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
122	'1972,explorer.exe'	'NetworkExplorer.dll,C:Windowssystem32NetworkExplorer.dll'
123	'1972,explorer.exe'	'browcli.dll,C:Windowssystem32rowcli.dll'
124	'1972,explorer.exe'	'MsftEdit.dll,C:Windowssystem32MsftEdit.dll'
125	'1972,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
126	'1972,explorer.exe'	taskschd.dll,C:Windowssystem32askschd.dll'
127	'1972,explorer.exe'	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
128	'1972,explorer.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
129	'1972,explorer.exe'	'2096,VBoxTray.exe'
130	'1972,explorer.exe'	'2112,MySQLNotifier.exe'
131	'1972,explorer.exe'	'416,mintty.exe'
132	'1972,explorer.exe'	'1760,taskmgr.exe'
133	'1972,explorer.exe'	'3764,cmd.exe'
134	'1972,explorer.exe'	'4032,firefox.exe'
135	'1972,explorer.exe'	'4572,cmd.exe'
136	'1972,explorer.exe'	'4736,notepad++.exe'
137	'1972,explorer.exe'	'4768,Wireshark.exe'
138	'1972,explorer.exe'	'4844,FoxitReader.exe'
139	'1972,explorer.exe'	'5340,mintty.exe'
140	**'1972,explorer.exe'**	**'4472,citadel.exe'**
141	'1972,explorer.exe'	'6276,notepad.exe'
142	**'1972,explorer.exe'**	**'5724,soft.exe'**
143	'1972,explorer.exe'	'8264,iexplore.exe'
144	'1972,explorer.exe'	'14412,mspaint.exe'
145	'1972,explorer.exe'	'16100,calc.exe'
146	'1972,explorer.exe'	'16248,cmd.exe'
147	'1972,explorer.exe'	'17324,firefox.exe'
148	'1972,explorer.exe'	'18064,cmd.exe'
149	'1972,explorer.exe'	'18224,notepad++.exe'
150	'1972,explorer.exe'	'18264,Wireshark.exe'
151	'1972,explorer.exe'	'18260,FoxitReader.exe'
152	'1972,explorer.exe'	'19020,mintty.exe'
153	'1972,explorer.exe'	'19136,firefox.exe'
154	'2096,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
155	'2112,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
156	'2188,XXX'	'2220,jusched.exe'
157	'2188,XXX'	'2248,update.exe'
158	'2220,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
159	'2248,update.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
160	'2472,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
161	'2472,WmiPrvSE.exe'	'perfos.dll,C:WindowsSystem32perfos.dll'

162	'2684,XXX'	'2736,RegSvcs.exe'
163	'2736,RegSvcs.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
164	'2784,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
165	'2784,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
166	'2784,SearchIndexer.exe'	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
167	'2784,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
168	'2784,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
169	'2784,SearchIndexer.exe'	'4492,SearchProtocolHost.exe'
170	'2784,SearchIndexer.exe'	'4176,SearchFilterHost.exe'
171	'2784,SearchIndexer.exe'	'5820,SearchProtocolHost.exe'
172	'2784,SearchIndexer.exe'	'5480,SearchFilterHost.exe'
173	'2784,SearchIndexer.exe'	'8620,SearchProtocolHost.exe'
174	'2784,SearchIndexer.exe'	'8640,SearchFilterHost.exe'
175	'2784,SearchIndexer.exe'	'9380,SearchProtocolHost.exe'
176	'2784,SearchIndexer.exe'	'9396,SearchFilterHost.exe'
177	'2784,SearchIndexer.exe'	'11020,SearchProtocolHost.exe'
178	'2784,SearchIndexer.exe'	'11040,SearchFilterHost.exe'
179	'2784,SearchIndexer.exe'	'13128,SearchProtocolHost.exe'
180	'2784,SearchIndexer.exe'	'13156,SearchFilterHost.exe'
181	'2784,SearchIndexer.exe'	'13976,SearchProtocolHost.exe'
182	'2784,SearchIndexer.exe'	'14036,SearchFilterHost.exe'
183	'2784,SearchIndexer.exe'	'14920,SearchProtocolHost.exe'
184	'2784,SearchIndexer.exe'	'14940,SearchFilterHost.exe'
185	'2784,SearchIndexer.exe'	'18856,SearchProtocolHost.exe'
186	'2784,SearchIndexer.exe'	'18876,SearchFilterHost.exe'
187	'3004,wmpnetwk.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
188	'3004,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
189	'3004,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
190	'3004,wmpnetwk.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
191	'1532,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
192	'2944,svchost.exe'	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
193	'416,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
194	'2424,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
195	'1728,XXX'	'2980,bash.exe'
196	'2980,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
197	'1876,XXX'	'2604,taskmgr.exe'
198	'2604,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
199	'1828,XXX'	'1484,driver_endpoint_netconn.exe'
200	'1484,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
201	'1760,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
202	'1760,taskmgr.exe'	'2972,taskmgr.exe'

203	'1348,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
204	'2636,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
205	'2972,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
206	'3120,taskhost.exe'	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
207	'3764,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
208	'3764,cmd.exe'	'3880,java.exe'
209	'3776,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
210	'3880,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
211	'4032,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
212	'4032,firefox.exe'	'3780,firefox.exe'
213	'4032,firefox.exe'	'6176,plugin-container.exe'
214	'3780,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
215	'4572,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
216	'4572,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
217	'4572,cmd.exe'	'4628,NETSTAT.EXE'
218	'4580,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
219	'4628,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
220	'4628,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
221	'4736,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
222	'4768,Wireshark.exe'	'4832,gspawn-win64-helper.exe'
223	'4768,Wireshark.exe'	'schannel.DLL,C:Windowssystem32schannel.DLL'
224	'4768,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
225	'4768,Wireshark.exe'	'4912,dumpcap.exe'
226	'4912,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
227	'4920,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
228	'4844,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
229	'4492,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
230	'4176,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
231	'5340,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
232	'5376,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
233	'5392,XXX'	'5408,bash.exe'
234	'5408,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
235	'5820,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
236	'5820,SearchProtocolHost.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
237	'5480,SearchFilterHost.exe'	'OffFilt.dll,C:Windowssystem32OffFilt.dll'
238	'6176,plugin-container.exe'	'6240,FlashPlayerPlugin_22_0_0_209.exe'
239	'6240,FlashPlayerPlugin_22_0_0_209.exe'	'6260,FlashPlayerPlugin_22_0_0_209.exe'
240	'5948,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
241	'6648,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
242	'6788,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
243	'7048,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'

244	'6192,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
245	'6404,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
246	**'4472,citadel.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
247	'4472,citadel.exe'	'6432,cmd.exe'
248	'6432,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
249	'6432,cmd.exe'	'6288,PING.EXE'
250	**'6432,cmd.exe'**	**'6480,citadel.exe'**
251	'6448,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
252	'6288,PING.EXE'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
253	'6276,notepad.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
254	'6308,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
255	**'6480,citadel.exe'**	**'7028,citadel.exe'**
256	**'7028,citadel.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
257	**'6996,XXX'**	**'6992,Lpgz.YVH'**
258	**'6992,Lpgz.YVH'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
259	'6992,Lpgz.YVH'	'7140,RegSvcs.exe'
260	'7140,RegSvcs.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
261	'4988,consent.exe'	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
262	'4464,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
263	'7024,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
264	**'5724,soft.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
265	**'5724,soft.exe'**	**'6632,puxa.exe'**
266	**'6632,puxa.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
267	'7000,WinMail.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
268	'7000,WinMail.exe'	'CFGMGR32.dll,C:Windowssystem32CFGMGR32.dll'
269	'7704,slui.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
270	'8264,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
271	'8264,iexplore.exe'	'8340,iexplore.exe'
272	'8264,iexplore.exe'	'8532,iexplore.exe'
273	'8264,iexplore.exe'	'10220,iexplore.exe'
274	'8264,iexplore.exe'	'10832,msdt.exe'
275	'8264,iexplore.exe'	'12744,iexplore.exe'
276	'8264,iexplore.exe'	'14276,iexplore.exe'
277	'8340,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
278	'8532,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
279	'8620,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
280	'8640,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
281	'10088,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
282	'10220,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
283	'9380,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
284	'9396,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'

285	'11020,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
286	'11040,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
287	'10832,msdt.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
288	'10936,sdiagnhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
289	'10956,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
290	'13128,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
291	'13156,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
292	'12744,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
293	'14276,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
294	'13976,SearchProtocolHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
295	'14036,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
296	'14412,mspaint.exe'	'browcli.dll,C:Windowssystem32rowcli.dll'
297	'14412,mspaint.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
298	'14412,mspaint.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
299	'14412,mspaint.exe'	'SAMLIB.dll,C:Windowssystem32SAMLIB.dll'
300	'14412,mspaint.exe'	'WININET.dll,C:Windowssystem32WININET.dll'
301	'14440,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
302	'14684,dllhost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
303	'14920,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
304	'14920,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
305	'14920,SearchProtocolHost.exe'	'ehtrace.dll,C:Windowsehomeehtrace.dll'
306	'14940,SearchFilterHost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
307	'14940,SearchFilterHost.exe'	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
308	'14992,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
309	'15068,dllhost.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
310	'15136,XXX'	'15152,setup_wm.exe'
311	'15152,setup_wm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
312	'15152,setup_wm.exe'	'15300,wmplayer.exe'
313	'15300,wmplayer.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
314	'14728,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
315	'15588,taskhost.exe'	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
316	'15708,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
317	'16100,calc.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
318	'16248,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
319	'16248,cmd.exe'	'16360,java.exe'
320	'16256,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
321	'16360,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
322	'17324,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
323	'17324,firefox.exe'	'17436,firefox.exe'
324	'17436,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
325	'18064,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'

326	'18064,cmd.exe'	'18132,NETSTAT.EXE'
327	'18072,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
328	'18132,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
329	'18132,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
330	'18224,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
331	'18264,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
332	'18264,Wireshark.exe'	'18400,dumpcap.exe'
333	'18400,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
334	'18408,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
335	'18260,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
336	'18260,FoxitReader.exe'	'18324,FoxitReaderUpdater.exe'
337	'18324,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
338	'18856,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
339	'18876,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
340	'19020,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
341	'19056,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
342	'19072,XXX'	'19088,bash.exe'
343	'19088,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'

7.2.4 Citadel Malware – Instance 2

Table 101: Citadel Malware Instance 2 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,XXX'
6	'360,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'400,wininit.exe'
9	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
10	'412,XXX'
11	'424,csrss.exe'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'504,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'528,lsm.exe'
17	'520,lsass.exe'
18	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
19	'psbase.dll,C:Windowssystem32psbase.dll'
20	'wkscli.dll,C:Windowssystem32wkscli.dll'
21	'628,svchost.exe'
22	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
23	'692,VBoxService.exe'
24	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
25	'756,svchost.exe'
26	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
27	'828,svchost.exe'
28	'rasadhlp.dll,C:WindowsSystem32rasadhlp.dll'
29	'winrnr.dll,C:WindowsSystem32winrnr.dll'
30	'876,svchost.exe'
31	'credssp.dll,C:WindowsSystem32credssp.dll'
32	'912,svchost.exe'
33	'AVRT.dll,c:windowssystem32AVRT.dll'
34	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
35	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'

36	'332,svchost.exe'
37	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
38	'1060,svchost.exe'
39	'msxml3.dll,C:WindowsSystem32msxml3.dll'
40	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
41	'1184,spoolsv.exe'
42	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
43	'1212,svchost.exe'
44	'pnpts.dll,C:Windowssystem32pnpts.dll'
45	'1324,svchost.exe'
46	'SXS.DLL,C:Windowssystem32SXS.DLL'
47	'1348,FoxitConnectedPDFService.exe'
48	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
49	'1908,svchost.exe'
50	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
51	'644,taskhost.exe'
52	'midimap.dll,C:Windowssystem32midimap.dll'
53	'1548,dwm.exe'
54	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
55	'1392,XXX'
56	'1556,explorer.exe'
57	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
58	thumbcache.dll,C:Windowssystem32humbcache.dll'
59	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
60	'SearchFolder.dll,C:Windowssystem32SearchFolder.dll'
61	'MLANG.dll,C:Windowssystem32MLANG.dll'
62	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
63	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
64	'shlxthdl_x64.dll,C:Program Files (x86)OpenOffice 4programshlxthdlshlxthdl_x64.dll'
65	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
66	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
67	'2160,VBoxTray.exe'
68	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
69	'2172,MySQLNotifier.exe'
70	'2236,update.exe'
71	'2256,XXX'
72	'2280,jusched.exe'
73	'2380,XXX'
74	**'2404,Lpgz.YVH'**
75	'2644,RegSvcs.exe'
76	'2668,WmiPrvSE.exe'

77	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
78	'perfos.dll,C:WindowsSystem32perfos.dll'
79	'2820,SearchIndexer.exe'
80	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
81	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
82	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
83	'2064,wmpnetwk.exe'
84	'provsvc.dll,C:WindowsSystem32provsvc.dll'
85	'1560,sppsvc.exe'
86	'3412,audiodg.exe'
87	'700,svchost.exe'
88	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
89	'3904,mintty.exe'
90	'apphelp.dll,C:Windowssystem32apphelp.dll'
91	'3548,conhost.exe'
92	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
93	'2576,XXX'
94	'2420,bash.exe'
95	'authz.dll,C:Windowssystem32authz.dll'
96	'3388,XXX'
97	'1192,driver_endpoint_netconn.exe'
98	'2932,firefox.exe'
99	'2508,firefox.exe'
100	'2980,dllhost.exe'
101	'3640,SearchProtocolHost.exe'
102	'profapi.dll,C:Windowssystem32profapi.dll'
103	'892,SearchFilterHost.exe'
104	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
105	'3828,dllhost.exe'
106	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
107	'4152,swriter.exe'
108	'4160,soffice.exe'
109	'4168,soffice.bin'
110	'4280,consent.exe'
111	'4356,dllhost.exe'
112	'IDStore.dll,C:WindowsSystem32IDStore.dll'
113	'4400,dllhost.exe'
114	**'4432,soft.exe'**
115	**'4444,ahce.exe'**
116	'4488,WinMail.exe'
117	'CFGMGR32.dll,C:Windowssystem32CFGMGR32.dll'

118	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
119	'4292,dllhost.exe'
120	'4844,dllhost.exe'
121	'4912,dllhost.exe'
122	**'5012,citadel.exe'**
123	'4816,XXX'
124	**'5072,citadel.exe'**
125	'19868,audiodg.exe'
126	'5040,conhost.exe'
127	'5056,cmd.exe'
128	'5068,PING.EXE'
129	'5148,dllhost.exe'
130	'5188,notepad++.exe'
131	'5316,dllhost.exe'
132	'5352,iexplore.exe'
133	'5512,iexplore.exe'
134	'6380,SearchProtocolHost.exe'
135	'6400,SearchFilterHost.exe'
136	'6444,iexplore.exe'
137	'6744,iexplore.exe'
138	'7176,SearchProtocolHost.exe'
139	'7204,SearchFilterHost.exe'
140	'7924,iexplore.exe'
141	'8024,SearchProtocolHost.exe'
142	'8044,SearchFilterHost.exe'
143	'8760,sbase.exe'
144	'8768,soffice.exe'
145	'8776,soffice.bin'
146	'9164,dllhost.exe'
147	'9208,simpress.exe'
148	'8216,soffice.exe'
149	'8372,soffice.bin'
150	'8904,splwow64.exe'
151	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
152	'9744,dllhost.exe'
153	'9812,taskhost.exe'
154	'9880,SearchProtocolHost.exe'
155	'9900,SearchFilterHost.exe'
156	'10016,dllhost.exe'
157	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
158	'10080,FoxitReader.exe'

159	'12132,SearchProtocolHost.exe'
160	'12156,SearchFilterHost.exe'
161	'12896,SearchProtocolHost.exe'
162	'12916,SearchFilterHost.exe'
163	'MSVCR90.dll,C:WindowsWinSxSamd64_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6161_none_08e61857a83bc251MSVCR90.dll'
164	'propertyhdl_x64.dll,C:Program Files (x86)OpenOffice 4programshlxthdlpropertyhdl_x64.dll'
165	'13020,dllhost.exe'
166	'12528,dllhost.exe'
167	'13132,dllhost.exe'
168	'14404,cmd.exe'
169	'14412,conhost.exe'
170	'14520,java.exe'
171	'16352,pingsender.exe'
172	'16364,conhost.exe'
173	'16376,firefox.exe'
174	'16420,firefox.exe'
175	'16904,cmd.exe'
176	'16912,conhost.exe'
177	'16928,NETSTAT.EXE'
178	'16992,notepad++.exe'
179	'17032,Wireshark.exe'
180	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
181	'17172,dumpcap.exe'
182	'17180,conhost.exe'
183	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
184	'16600,FoxitReader.exe'
185	'17224,SearchProtocolHost.exe'
186	'17232,SearchFilterHost.exe'
187	'17692,mintty.exe'
188	'17732,conhost.exe'
189	'17748,XXX'
190	'17764,bash.exe'
191	'18272,simpress.exe'
192	'18292,soffice.exe'
193	'18300,soffice.bin'
194	'17648,java.exe'
195	'18076,conhost.exe'
196	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
197	'18484,SearchProtocolHost.exe'
198	'18504,SearchFilterHost.exe'

199	'19000,smath.exe'
200	'19008,soffice.exe'
201	'19016,soffice.bin'
202	'19192,scalc.exe'
203	'19200,soffice.exe'
204	'19208,soffice.bin'
205	'19732,taskhost.exe'
206	'19984,firefox.exe'
207	'20148,firefox.exe'
208	'19608,iexplore.exe'
209	'19832,iexplore.exe'
210	'20488,iexplore.exe'
211	'20624,SearchProtocolHost.exe'
212	'20644,SearchFilterHost.exe'
213	'21268,SearchProtocolHost.exe'
214	'21288,SearchFilterHost.exe'

Table 102: Citadel Malware Instance 2 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'352,XXX'	'360,csrss.exe'
5	'352,XXX'	'400,wininit.exe'
6	'360,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'400,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
8	'400,wininit.exe'	'504,services.exe'
9	'400,wininit.exe'	'528,lsm.exe'
10	'400,wininit.exe'	'520,lsass.exe'
11	'412,XXX'	'424,csrss.exe'
12	'412,XXX'	'460,winlogon.exe'
13	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
14	'424,csrss.exe'	'3548,conhost.exe'
15	'424,csrss.exe'	'5040,conhost.exe'
16	'424,csrss.exe'	'14412,conhost.exe'
17	'424,csrss.exe'	'16364,conhost.exe'
18	'424,csrss.exe'	'16912,conhost.exe'
19	'424,csrss.exe'	'17180,conhost.exe'
20	'424,csrss.exe'	'17732,conhost.exe'
21	'424,csrss.exe'	'18076,conhost.exe'
22	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
23	'504,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
24	'504,services.exe'	'628,svchost.exe'
25	'504,services.exe'	'692,VBoxService.exe'
26	'504,services.exe'	'756,svchost.exe'
27	'504,services.exe'	'828,svchost.exe'
28	'504,services.exe'	'876,svchost.exe'
29	'504,services.exe'	'912,svchost.exe'
30	'504,services.exe'	'332,svchost.exe'
31	'504,services.exe'	'1060,svchost.exe'
32	'504,services.exe'	'1184,spoolsv.exe'
33	'504,services.exe'	'1212,svchost.exe'
34	'504,services.exe'	'1324,svchost.exe'
35	'504,services.exe'	'1348,FoxitConnectedPDFService.exe'
36	'504,services.exe'	'1908,svchost.exe'
37	'504,services.exe'	'644,taskhost.exe'

38	'504,services.exe'	'2820,SearchIndexer.exe'
39	'504,services.exe'	'2064,wmpnetwk.exe'
40	'504,services.exe'	'1560,sppsvc.exe'
41	'504,services.exe'	'700,svchost.exe'
42	'504,services.exe'	'9812,taskhost.exe'
43	'504,services.exe'	'19732,taskhost.exe'
44	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
45	'520,lsass.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
46	'520,lsass.exe'	'psbase.dll,C:Windowssystem32psbase.dll'
47	'520,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
48	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
49	'628,svchost.exe'	'2668,WmiPrvSE.exe'
50	'628,svchost.exe'	'2980,dllhost.exe'
51	'628,svchost.exe'	'3828,dllhost.exe'
52	'628,svchost.exe'	'4356,dllhost.exe'
53	'628,svchost.exe'	'4400,dllhost.exe'
54	'628,svchost.exe'	'4488,WinMail.exe'
55	'628,svchost.exe'	'4292,dllhost.exe'
56	'628,svchost.exe'	'4844,dllhost.exe'
57	'628,svchost.exe'	'4912,dllhost.exe'
58	'628,svchost.exe'	'5148,dllhost.exe'
59	'628,svchost.exe'	'5316,dllhost.exe'
60	'628,svchost.exe'	'9164,dllhost.exe'
61	'628,svchost.exe'	'9744,dllhost.exe'
62	'628,svchost.exe'	'10016,dllhost.exe'
63	'628,svchost.exe'	'13020,dllhost.exe'
64	'628,svchost.exe'	'12528,dllhost.exe'
65	'628,svchost.exe'	'13132,dllhost.exe'
66	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
67	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
68	'828,svchost.exe'	'rasadhlp.dll,C:WindowsSystem32rasadhlp.dll'
69	'828,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
70	'828,svchost.exe'	'3412,audiodg.exe'
71	'828,svchost.exe'	'19868,audiodg.exe'
72	'876,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
73	'876,svchost.exe'	'1548,dwm.exe'
74	'912,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
75	'912,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
76	'912,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
77	'912,svchost.exe'	'4280,consent.exe'
78	'332,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'

79	'1060,svchost.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
80	'1060,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
81	'1184,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
82	'1212,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
83	'1212,svchost.exe'	'pnpts.dll,C:Windowssystem32pnpts.dll'
84	'1324,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
85	'1348,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
86	'1908,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
87	'644,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
88	'1548,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
89	'1392,XXX'	'1556,explorer.exe'
90	'1556,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
91	'1556,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
92	'1556,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
93	'1556,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
94	'1556,explorer.exe'	'SearchFolder.dll,C:Windowssystem32SearchFolder.dll'
95	'1556,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
96	'1556,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
97	'1556,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
98	'1556,explorer.exe'	'shlxthdl_x64.dll,C:Program Files (x86)OpenOffice 4programshlxthdlshlxthdl_x64.dll'
99	'1556,explorer.exe'	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
100	'1556,explorer.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
101	'1556,explorer.exe'	'2160,VBoxTray.exe'
102	'1556,explorer.exe'	'2172,MySQLNotifier.exe'
103	'1556,explorer.exe'	'2236,update.exe'
104	'1556,explorer.exe'	'3904,mintty.exe'
105	'1556,explorer.exe'	'2932,firefox.exe'
106	'1556,explorer.exe'	'4152,swriter.exe'
107	**'1556,explorer.exe'**	**'4432,soft.exe'**
108	**'1556,explorer.exe'**	**'5012,citadel.exe'**
109	'1556,explorer.exe'	'5188,notepad++.exe'
110	'1556,explorer.exe'	'5352,iexplore.exe'
111	'1556,explorer.exe'	'8760,sbase.exe'
112	'1556,explorer.exe'	'9208,simpress.exe'
113	'1556,explorer.exe'	'10080,FoxitReader.exe'
114	'1556,explorer.exe'	'14404,cmd.exe'
115	'1556,explorer.exe'	'16376,firefox.exe'
116	'1556,explorer.exe'	'16904,cmd.exe'
117	'1556,explorer.exe'	'16992,notepad++.exe'
118	'1556,explorer.exe'	'17032,Wireshark.exe'
119	'1556,explorer.exe'	'16600,FoxitReader.exe'

120	'1556,explorer.exe'	'17692,mintty.exe'
121	'1556,explorer.exe'	'19000,smath.exe'
122	'1556,explorer.exe'	'19192,scalc.exe'
123	'1556,explorer.exe'	'19984,firefox.exe'
124	'1556,explorer.exe'	'19608,iexplore.exe'
125	'2160,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
126	'2172,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
127	'2236,update.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
128	'2256,XXX'	'2280,jusched.exe'
129	'2280,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
130	**'2380,XXX'**	**'2404,Lpgz.YVH'**
131	**'2404,Lpgz.YVH'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
132	'2404,Lpgz.YVH'	'2644,RegSvcs.exe'
133	'2644,RegSvcs.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
134	'2668,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
135	'2668,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
136	'2668,WmiPrvSE.exe'	'perfos.dll,C:WindowsSystem32perfos.dll'
137	'2820,SearchIndexer.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
138	'2820,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
139	'2820,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
140	'2820,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
141	'2820,SearchIndexer.exe'	'3640,SearchProtocolHost.exe'
142	'2820,SearchIndexer.exe'	'892,SearchFilterHost.exe'
143	'2820,SearchIndexer.exe'	'6380,SearchProtocolHost.exe'
144	'2820,SearchIndexer.exe'	'6400,SearchFilterHost.exe'
145	'2820,SearchIndexer.exe'	'7176,SearchProtocolHost.exe'
146	'2820,SearchIndexer.exe'	'7204,SearchFilterHost.exe'
147	'2820,SearchIndexer.exe'	'8024,SearchProtocolHost.exe'
148	'2820,SearchIndexer.exe'	'8044,SearchFilterHost.exe'
149	'2820,SearchIndexer.exe'	'9880,SearchProtocolHost.exe'
150	'2820,SearchIndexer.exe'	'9900,SearchFilterHost.exe'
151	'2820,SearchIndexer.exe'	'12132,SearchProtocolHost.exe'
152	'2820,SearchIndexer.exe'	'12156,SearchFilterHost.exe'

153	'2820,SearchIndexer.exe'	'12896,SearchProtocolHost.exe'
154	'2820,SearchIndexer.exe'	'12916,SearchFilterHost.exe'
155	'2820,SearchIndexer.exe'	'17224,SearchProtocolHost.exe'
156	'2820,SearchIndexer.exe'	'17232,SearchFilterHost.exe'
157	'2820,SearchIndexer.exe'	'18484,SearchProtocolHost.exe'
158	'2820,SearchIndexer.exe'	'18504,SearchFilterHost.exe'
159	'2820,SearchIndexer.exe'	'20624,SearchProtocolHost.exe'
160	'2820,SearchIndexer.exe'	'20644,SearchFilterHost.exe'
161	'2820,SearchIndexer.exe'	'21268,SearchProtocolHost.exe'
162	'2820,SearchIndexer.exe'	'21288,SearchFilterHost.exe'
163	'2064,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
164	'1560,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
165	'700,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
166	'3904,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
167	'3548,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
168	'2576,XXX'	'2420,bash.exe'
169	'2420,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
170	'3388,XXX'	'1192,driver_endpoint_netconn.exe'
171	'1192,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
172	'2932,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
173	'2932,firefox.exe'	'2508,firefox.exe'
174	'2932,firefox.exe'	'16352,pingsender.exe'
175	'2508,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
176	'2980,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
177	'3640,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
178	'892,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
179	'3828,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
180	'4152,swriter.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
181	'4152,swriter.exe'	'4160,soffice.exe'
182	'4160,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
183	'4160,soffice.exe'	'4168,soffice.bin'
184	'4168,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
185	'4168,soffice.bin'	'8904,splwow64.exe'
186	'4356,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
187	'4400,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'

188	**'4432,soft.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
189	**'4432,soft.exe'**	**'4444,ahce.exe'**
190	**'4444,ahce.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
191	'4488,WinMail.exe'	'CFGMGR32.dll,C:Windowssystem32CFGMGR32.dll'
192	'4488,WinMail.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
193	'4292,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
194	'4844,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
195	'4912,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
196	**'5012,citadel.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
197	'5012,citadel.exe'	'5056,cmd.exe'
198	**'4816,XXX'**	**'5072,citadel.exe'**
199	**'5072,citadel.exe'**	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
200	'5056,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
201	'5056,cmd.exe'	'5068,PING.EXE'
202	'5148,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
203	'5188,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
204	'5316,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
205	'5352,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
206	'5352,iexplore.exe'	'5512,iexplore.exe'
207	'5352,iexplore.exe'	'6444,iexplore.exe'
208	'5352,iexplore.exe'	'6744,iexplore.exe'
209	'5352,iexplore.exe'	'7924,iexplore.exe'
210	'5512,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
211	'6380,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
212	'6400,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
213	'6444,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
214	'6744,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
215	'7176,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
216	'7204,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
217	'7924,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
218	'8024,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
219	'8044,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
220	'8760,sbase.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
221	'8760,sbase.exe'	'8768,soffice.exe'
222	'8768,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
223	'8768,soffice.exe'	'8776,soffice.bin'
224	'8776,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
225	'9164,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
226	'9208,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

227	'9208,simpress.exe'	'8216,soffice.exe'
228	'8216,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
229	'8216,soffice.exe'	'8372,soffice.bin'
230	'8372,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
231	'8904,splwow64.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
232	'8904,splwow64.exe'	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
233	'9744,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
234	'9812,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
235	'9880,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
236	'9900,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
237	'10016,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
238	'10080,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
239	'12132,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
240	'12156,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
241	'12896,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
242	'12896,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
243	'12916,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
244	'12916,SearchFilterHost.exe'	'MSVCR90.dll,C:WindowsWinSxSamd64_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6161_none_08e61857a83bc251MSVCR90.dll'
245	'12916,SearchFilterHost.exe'	'propertyhdl_x64.dll,C:Program Files (x86)OpenOffice 4programshlxthdlpropertyhdl_x64.dll'
246	'13020,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
247	'12528,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
248	'13132,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
249	'14404,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
250	'14404,cmd.exe'	'14520,java.exe'
251	'14412,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
252	'14520,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
253	'14520,java.exe'	'17648,java.exe'
254	'16376,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
255	'16376,firefox.exe'	'16420,firefox.exe'
256	'16376,firefox.exe'	'18272,simpress.exe'
257	'16420,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
258	'16904,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
259	'16904,cmd.exe'	'16928,NETSTAT.EXE'
260	'16912,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
261	'16928,NETSTAT.EXE'	'rasadhlp.dll,C:WindowsSystem32rasadhlp.dll'
262	'16928,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
263	'16992,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

264	'17032,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
265	'17032,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
266	'17032,Wireshark.exe'	'17172,dumpcap.exe'
267	'17172,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
268	'17180,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
269	'16600,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
270	'17224,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
271	'17232,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
272	'17692,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
273	'17732,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
274	'17748,XXX'	'17764,bash.exe'
275	'17764,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
276	'18272,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
277	'18272,simpress.exe'	'18292,soffice.exe'
278	'18292,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
279	'18292,soffice.exe'	'18300,soffice.bin'
280	'18300,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
281	'17648,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
282	'18076,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
283	'18484,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
284	'18504,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
285	'19000,smath.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
286	'19000,smath.exe'	'19008,soffice.exe'
287	'19008,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
288	'19008,soffice.exe'	'19016,soffice.bin'
289	'19016,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
290	'19192,scalc.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
291	'19192,scalc.exe'	'19200,soffice.exe'
292	'19200,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
293	'19200,soffice.exe'	'19208,soffice.bin'
294	'19208,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
295	'19732,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
296	'19984,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
297	'19984,firefox.exe'	'20148,firefox.exe'
298	'20148,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
299	'19608,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
300	'19608,iexplore.exe'	'19832,iexplore.exe'
301	'19608,iexplore.exe'	'20488,iexplore.exe'
302	'19832,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
303	'20488,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

304	'20624,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
305	'20644,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
306	'21268,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
307	'21288,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'

7.2.5 Hupigon Malware – Instance 1

Table 103: Hupigon Malware Instance 1 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,XXX'
6	'360,csrss.exe'
7	**'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'**
8	'412,XXX'
9	'424,csrss.exe'
10	'400,wininit.exe'
11	'credssp.dll,C:Windowssystem32credssp.dll'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'504,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'528,lsm.exe'
17	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
18	'520,lsass.exe'
19	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
20	'wkscli.dll,C:Windowssystem32wkscli.dll'
21	'628,svchost.exe'
22	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
23	'688,VBoxService.exe'
24	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
25	'752,svchost.exe'
26	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
27	'852,svchost.exe'
28	'netutils.dll,C:WindowsSystem32netutils.dll'
29	'winrnr.dll,C:WindowsSystem32winrnr.dll'
30	'884,svchost.exe'
31	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
32	'988,audiodg.exe'
33	'920,svchost.exe'
34	'appinfo.dll,c:windowssystem32appinfo.dll'
35	'AVRT.dll,c:windowssystem32AVRT.dll'

36	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
37	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
38	'124,svchost.exe'
39	'dsrole.dll,C:Windowssystem32dsrole.dll'
40	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
41	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
42	'908,svchost.exe'
43	'SensApi.dll,C:Windowssystem32SensApi.dll'
44	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
45	'1120,spoolsv.exe'
46	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
47	'1148,svchost.exe'
48	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
49	'1260,svchost.exe'
50	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
51	'1300,FoxitConnectedPDFService.exe'
52	**'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'**
53	'1848,svchost.exe'
54	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
55	'1352,taskhost.exe'
56	'midimap.dll,C:Windowssystem32midimap.dll'
57	'348,XXX'
58	'1780,explorer.exe'
59	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
60	'564,dwm.exe'
61	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
62	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
63	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
64	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
65	tquery.dll,C:Windowssystem32query.dll'
66	'MSVCP90.dll,C:WindowsWinSxSamd64_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6161_none_08e61857a83bc251MSVCP90.dll'
67	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
68	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
69	'bcryptprimitives.dll,C:Windowssystem32cryptprimitives.dll'
70	'1232,MySQLNotifier.exe'
71	'1732,VBoxTray.exe'
72	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
73	'1684,XXX'
74	'2204,jusched.exe'
75	'2232,WmiPrvSE.exe'

76	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
77	'2672,SearchIndexer.exe'
78	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
79	'NLSLexicons0010.dll,C:WindowsSystem32NLSLexicons0010.dll'
80	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
81	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
82	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
83	'2996,wmpnetwk.exe'
84	'provsvc.dll,C:WindowsSystem32provsvc.dll'
85	'2936,sppsvc.exe'
86	'3040,svchost.exe'
87	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
88	'4040,XXX'
89	'1160,taskmgr.exe'
90	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
91	'iertutil.dll,C:Windowssystem32iertutil.dll'
92	'OLEACC.dll,C:Windowssystem32OLEACC.dll'
93	'WINMM.dll,C:Windowssystem32WINMM.dll'
94	'SXS.DLL,C:Windowssystem32SXS.DLL'
95	'1432,mintty.exe'
96	'apphelp.dll,C:Windowssystem32apphelp.dll'
97	'1372,conhost.exe'
98	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
99	'736,XXX'
100	'3008,bash.exe'
101	'authz.dll,C:Windowssystem32authz.dll'
102	'472,XXX'
103	'3984,driver_endpoint_netconn.exe'
104	'2852,cmd.exe'
105	'2664,conhost.exe'
106	'2076,java.exe'
107	'636,firefox.exe'
108	'944,firefox.exe'
109	'1828,cmd.exe'
110	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
111	'3128,conhost.exe'
112	'1436,NETSTAT.EXE'
113	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
114	'3876,notepad++.exe'
115	'3116,gspawn-win64-helper.exe'
116	'1444,androiddump.exe'

117	'2364,Wireshark.exe'
118	'3224,dumpcap.exe'
119	'3524,conhost.exe'
120	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
121	'3960,FoxitReader.exe'
122	'3400,FoxitReaderUpdater.exe'
123	'5600,consent.exe'
124	'6156,audiodg.exe'
125	'4212,SearchProtocolHost.exe'
126	'4232,SearchFilterHost.exe'
127	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
128	'4648,mintty.exe'
129	'4684,conhost.exe'
130	'4700,XXX'
131	'4716,bash.exe'
132	'1104,simpress.exe'
133	'4396,soffice.exe'
134	'4408,soffice.bin'
135	'5588,java.exe'
136	'5596,conhost.exe'
137	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
138	'5972,SearchProtocolHost.exe'
139	'profapi.dll,C:Windowssystem32profapi.dll'
140	'5996,SearchFilterHost.exe'
141	'5360,plugin-container.exe'
142	'5400,FlashPlayerPlugin_22_0_0_209.exe'
143	'5684,conhost.exe'
144	'5704,cmd.exe'
145	'5168,dllhost.exe'
146	'6256,dllhost.exe'
147	'IDStore.dll,C:WindowsSystem32IDStore.dll'
148	'6292,dllhost.exe'
149	'6328,Hupigon.exe'
150	**'6336,cmd.exe'**
151	**'6344,conhost.exe'**
152	**'6384,Hacker.com.cn.exe'**
153	**'6392,cmd.exe'**
154	**'6400,conhost.exe'**
155	'6436,SearchProtocolHost.exe'
156	'6444,iexplore.exe'
157	'6464,SearchFilterHost.exe'

158	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
159	'6916,dllhost.exe'
160	'7188,svchost.exe'
161	'12984,audiodg.exe'
162	'19616,slui.exe'
163	'7296,firefox.exe'
164	'7468,firefox.exe'
165	'7776,Wireshark.exe'
166	'msimtf.dll,C:Windowssystem32msimtf.dll'
167	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
168	'7924,dumpcap.exe'
169	'7932,conhost.exe'
170	'8048,dumpcap.exe'
171	'8056,conhost.exe'
172	'9048,audiodg.exe'
173	'8340,calc.exe'
174	'8556,iexplore.exe'
175	'npmproxy.dll,C:WindowsSystem32npmproxy.dll'
176	'msxml3.dll,C:WindowsSystem32msxml3.dll'
177	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
178	'Secur32.dll,C:WindowsSystem32Secur32.dll'
179	'8608,iexplore.exe'
180	'Dxtmsft.dll,C:WindowsSystem32Dxtmsft.dll'
181	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
182	'8832,SearchProtocolHost.exe'
183	'8852,SearchFilterHost.exe'
184	'8952,iexplore.exe'
185	'msimg32.dll,C:Windowssystem32msimg32.dll'
186	'WINSPOOL.DRV,C:WindowsSystem32WINSPOOL.DRV'
187	'9112,SearchProtocolHost.exe'
188	'9096,SearchFilterHost.exe'
189	'9640,dllhost.exe'
190	'9812,taskhost.exe'
191	'9896,SearchProtocolHost.exe'
192	'9920,SearchFilterHost.exe'
193	'10056,slui.exe'
194	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
195	'10112,firefox.exe'
196	'10408,pingsender.exe'
197	'9500,firefox.exe'
198	'10536,cmd.exe'

199	'10544,conhost.exe'
200	'10576,PING.EXE'
201	'10984,soffice.exe'
202	'10992,soffice.bin'
203	'10748,dllhost.exe'
204	'10932,SearchProtocolHost.exe'
205	'11272,SearchFilterHost.exe'
206	'MSVCR90.dll,C:WindowsWinSxSamd64_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6161_none_08e61857a83bc251MSVCR90.dll'
207	'propertyhdl_x64.dll,C:Program Files (x86)OpenOffice 4programshlxthdlpropertyhdl_x64.dll'
208	'11476,dllhost.exe'
209	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
210	'11544,swriter.exe'
211	'11552,soffice.exe'
212	'11560,soffice.bin'
213	'11672,FoxitReader.exe'
214	'12008,firefox.exe'
215	'12172,firefox.exe'
216	'12836,dllhost.exe'
217	'13088,dllhost.exe'
218	'13192,dllhost.exe'
219	'13228,notepad.exe'
220	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
221	'13280,dllhost.exe'
222	'12536,dllhost.exe'
223	'12744,notepad++.exe'
224	'12708,notepad.exe'
225	'13020,dllhost.exe'
226	'13148,dllhost.exe'
227	'12728,dllhost.exe'
228	'13448,dllhost.exe'
229	'13524,cmd.exe'
230	'13532,conhost.exe'
231	'13624,dllhost.exe'
232	'13664,cipher.exe'
233	'13672,conhost.exe'
234	'13712,dllhost.exe'
235	'13816,WmiPrvSE.exe'
236	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
237	'13876,dllhost.exe'
238	'13912,XXX'
239	'13920,mstsc.exe'

240	'14036,dllhost.exe'
241	'14252,dllhost.exe'
242	'14288,dllhost.exe'
243	'14320,logman.exe'
244	'14328,conhost.exe'
245	'14068,dllhost.exe'
246	'13492,dllhost.exe'
247	'14316,dllhost.exe'
248	'14400,dllhost.exe'
249	'14476,swriter.exe'
250	'14488,soffice.exe'
251	'14496,soffice.bin'
252	'14552,SearchProtocolHost.exe'
253	'14572,SearchFilterHost.exe'
254	'14648,soffice.exe'
255	'14656,soffice.bin'
256	'14976,dllhost.exe'
257	'15208,SearchProtocolHost.exe'
258	'15232,SearchFilterHost.exe'
259	'15280,dllhost.exe'
260	'12992,dllhost.exe'
261	'15348,dllhost.exe'
262	'15520,firefox.exe'
263	'15688,firefox.exe'
264	'16052,SearchProtocolHost.exe'
265	'16072,SearchFilterHost.exe'
266	'13004,cmd.exe'
267	'16296,conhost.exe'
268	'16440,java.exe'
269	'16580,firefox.exe'
270	'16744,firefox.exe'
271	'17180,cmd.exe'
272	'17188,conhost.exe'
273	'17208,NETSTAT.EXE'
274	'17288,notepad++.exe'
275	'17344,Wireshark.exe'
276	'16400,dumpcap.exe'
277	'16492,conhost.exe'
278	'13008,FoxitReader.exe'
279	'17796,mintty.exe'
280	'17836,conhost.exe'

281	'17880,XXX'
282	'17896,bash.exe'
283	'18408,simpress.exe'
284	'18400,soffice.exe'
285	'18388,soffice.bin'
286	'19112,java.exe'
287	'19220,conhost.exe'
288	'18628,SearchProtocolHost.exe'
289	'18704,SearchFilterHost.exe'

Table 104: Hupigon Malware Instance 1 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'352,XXX'	'360,csrss.exe'
5	'352,XXX'	'400,wininit.exe'
6	'360,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'360,csrss.exe'	'6400,conhost.exe'
8	'412,XXX'	'424,csrss.exe'
9	'412,XXX'	'460,winlogon.exe'
10	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
11	'424,csrss.exe'	'1372,conhost.exe'
12	'424,csrss.exe'	'2664,conhost.exe'
13	'424,csrss.exe'	'3128,conhost.exe'
14	'424,csrss.exe'	'3524,conhost.exe'
15	'424,csrss.exe'	'4684,conhost.exe'
16	'424,csrss.exe'	'5596,conhost.exe'
17	'424,csrss.exe'	'5684,conhost.exe'
18	'424,csrss.exe'	'6344,conhost.exe'
19	'424,csrss.exe'	'7932,conhost.exe'
20	'424,csrss.exe'	'8056,conhost.exe'
21	'424,csrss.exe'	'10544,conhost.exe'
22	'424,csrss.exe'	'13532,conhost.exe'
23	'424,csrss.exe'	'13672,conhost.exe'
24	'424,csrss.exe'	'14328,conhost.exe'
25	'424,csrss.exe'	'16296,conhost.exe'
26	'424,csrss.exe'	'17188,conhost.exe'
27	'424,csrss.exe'	'16492,conhost.exe'
28	'424,csrss.exe'	'17836,conhost.exe'
29	'424,csrss.exe'	'19220,conhost.exe'
30	'400,wininit.exe'	'credssp.dll,C:Windowssystem32credssp.dll'
31	'400,wininit.exe'	'504,services.exe'
32	'400,wininit.exe'	'528,lsm.exe'
33	'400,wininit.exe'	'520,lsass.exe'
34	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
35	'504,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
36	'504,services.exe'	'628,svchost.exe'
37	'504,services.exe'	'688,VBoxService.exe'
38	'504,services.exe'	'752,svchost.exe'
39	'504,services.exe'	'852,svchost.exe'

40	'504,services.exe'	'884,svchost.exe'
41	'504,services.exe'	'920,svchost.exe'
42	'504,services.exe'	'124,svchost.exe'
43	'504,services.exe'	'908,svchost.exe'
44	'504,services.exe'	'1120,spoolsv.exe'
45	'504,services.exe'	'1148,svchost.exe'
46	'504,services.exe'	'1260,svchost.exe'
47	'504,services.exe'	'1300,FoxitConnectedPDFService.exe'
48	'504,services.exe'	'1848,svchost.exe'
49	'504,services.exe'	'1352,taskhost.exe'
50	'504,services.exe'	'2672,SearchIndexer.exe'
51	'504,services.exe'	'2996,wmpnetwk.exe'
52	'504,services.exe'	'2936,sppsvc.exe'
53	'504,services.exe'	'3040,svchost.exe'
54	'504,services.exe'	'6384,Hacker.com.cn.exe'
55	'504,services.exe'	'7188,svchost.exe'
56	'504,services.exe'	'9812,taskhost.exe'
57	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
58	'520,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
59	'520,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
60	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
61	'628,svchost.exe'	'2232,WmiPrvSE.exe'
62	'628,svchost.exe'	'5168,dllhost.exe'
63	'628,svchost.exe'	'6256,dllhost.exe'
64	'628,svchost.exe'	'6292,dllhost.exe'
65	'628,svchost.exe'	'6916,dllhost.exe'
66	'628,svchost.exe'	'19616,slui.exe'
67	'628,svchost.exe'	'9640,dllhost.exe'
68	'628,svchost.exe'	'10056,slui.exe'
69	'628,svchost.exe'	'10748,dllhost.exe'
70	'628,svchost.exe'	'11476,dllhost.exe'
71	'628,svchost.exe'	'12836,dllhost.exe'
72	'628,svchost.exe'	'13088,dllhost.exe'
73	'628,svchost.exe'	'13192,dllhost.exe'
74	'628,svchost.exe'	'13280,dllhost.exe'
75	'628,svchost.exe'	'12536,dllhost.exe'
76	'628,svchost.exe'	'13020,dllhost.exe'
77	'628,svchost.exe'	'13148,dllhost.exe'
78	'628,svchost.exe'	'12728,dllhost.exe'
79	'628,svchost.exe'	'13448,dllhost.exe'
80	'628,svchost.exe'	'13624,dllhost.exe'

81	'628,svchost.exe'	'13712,dllhost.exe'
82	'628,svchost.exe'	'13816,WmiPrvSE.exe'
83	'628,svchost.exe'	'13876,dllhost.exe'
84	'628,svchost.exe'	'14036,dllhost.exe'
85	'628,svchost.exe'	'14252,dllhost.exe'
86	'628,svchost.exe'	'14288,dllhost.exe'
87	'628,svchost.exe'	'14068,dllhost.exe'
88	'628,svchost.exe'	'13492,dllhost.exe'
89	'628,svchost.exe'	'14316,dllhost.exe'
90	'628,svchost.exe'	'14400,dllhost.exe'
91	'628,svchost.exe'	'14976,dllhost.exe'
92	'628,svchost.exe'	'15280,dllhost.exe'
93	'628,svchost.exe'	'12992,dllhost.exe'
94	'628,svchost.exe'	'15348,dllhost.exe'
95	'688,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
96	'752,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
97	'852,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
98	'852,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
99	'852,svchost.exe'	'988,audiodg.exe'
100	'852,svchost.exe'	'6156,audiodg.exe'
101	'852,svchost.exe'	'12984,audiodg.exe'
102	'852,svchost.exe'	'9048,audiodg.exe'
103	'884,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
104	'884,svchost.exe'	'564,dwm.exe'
105	'920,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
106	'920,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
107	'920,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
108	'920,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
109	'920,svchost.exe'	'5600,consent.exe'
110	'124,svchost.exe'	'dsrole.dll,C:Windowssystem32dsrole.dll'
111	'124,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
112	'124,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
113	'908,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
114	'908,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
115	'1120,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
116	'1148,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
117	'1148,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
118	'1260,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
119	'1300,FoxitConnectedPDF Service.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
120	'1848,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'

121	'1352,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
122	'348,XXX'	'1780,explorer.exe'
123	'1780,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
124	'1780,explorer.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
125	'1780,explorer.exe'	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
126	'1780,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
127	'1780,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
128	'1780,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
129	'1780,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
130	'1780,explorer.exe'	'tquery.dll,C:Windowssystem32
131	'1780,explorer.exe'	'MSVCP90.dll,C:WindowsWinSxSamd64_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6161_none_08e61857a83bc251MSVCP90.dll'
132	'1780,explorer.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
133	'1780,explorer.exe'	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
134	'1780,explorer.exe'	'bcryptprimitives.dll,C:Windowssystem32cryptprimitives.dll'
135	'1780,explorer.exe'	'1232,MySQLNotifier.exe'
136	'1780,explorer.exe'	'1732,VBoxTray.exe'
137	'1780,explorer.exe'	'1432,mintty.exe'
138	'1780,explorer.exe'	'2852,cmd.exe'
139	'1780,explorer.exe'	'636,firefox.exe'
140	'1780,explorer.exe'	'1828,cmd.exe'
141	'1780,explorer.exe'	'3876,notepad++.exe'
142	'1780,explorer.exe'	'2364,Wireshark.exe'
143	'1780,explorer.exe'	'3960,FoxitReader.exe'
144	'1780,explorer.exe'	'4648,mintty.exe'
145	'1780,explorer.exe'	'5704,cmd.exe'
146	'1780,explorer.exe'	'6328,Hupigon.exe'
147	'1780,explorer.exe'	'7296,firefox.exe'
148	'1780,explorer.exe'	'7776,Wireshark.exe'
149	'1780,explorer.exe'	'8340,calc.exe'
150	'1780,explorer.exe'	'8556,iexplore.exe'
151	'1780,explorer.exe'	'10112,firefox.exe'
152	'1780,explorer.exe'	'10536,cmd.exe'
153	'1780,explorer.exe'	'10984,soffice.exe'
154	'1780,explorer.exe'	'11544,swriter.exe'
155	'1780,explorer.exe'	'11672,FoxitReader.exe'
156	'1780,explorer.exe'	'12008,firefox.exe'
157	'1780,explorer.exe'	'13228,notepad.exe'
158	'1780,explorer.exe'	'12744,notepad++.exe'
159	'1780,explorer.exe'	'12708,notepad.exe'
160	'1780,explorer.exe'	'13524,cmd.exe'
161	'1780,explorer.exe'	'13664,cipher.exe'

162	'1780,explorer.exe'	'14320,logman.exe'
163	'1780,explorer.exe'	'14476,swriter.exe'
164	'1780,explorer.exe'	'14648,soffice.exe'
165	'1780,explorer.exe'	'15520,firefox.exe'
166	'1780,explorer.exe'	'13004,cmd.exe'
167	'1780,explorer.exe'	'16580,firefox.exe'
168	'1780,explorer.exe'	'17180,cmd.exe'
169	'1780,explorer.exe'	'17288,notepad++.exe'
170	'1780,explorer.exe'	'17344,Wireshark.exe'
171	'1780,explorer.exe'	'13008,FoxitReader.exe'
172	'1780,explorer.exe'	'17796,mintty.exe'
173	'564,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
174	'1232,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
175	'1732,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
176	'1684,XXX'	'2204,jusched.exe'
177	'2204,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
178	'2232,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
179	'2232,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
180	'2672,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
181	'2672,SearchIndexer.exe'	'NLSLexicons0010.dll,C:WindowsSystem32NLSLexicons0010.dll'
182	'2672,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
183	'2672,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
184	'2672,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
185	'2672,SearchIndexer.exe'	'4212,SearchProtocolHost.exe'
186	'2672,SearchIndexer.exe'	'4232,SearchFilterHost.exe'
187	'2672,SearchIndexer.exe'	'5972,SearchProtocolHost.exe'
188	'2672,SearchIndexer.exe'	'5996,SearchFilterHost.exe'
189	'2672,SearchIndexer.exe'	'6436,SearchProtocolHost.exe'
190	'2672,SearchIndexer.exe'	'6464,SearchFilterHost.exe'
191	'2672,SearchIndexer.exe'	'8832,SearchProtocolHost.exe'
192	'2672,SearchIndexer.exe'	'8852,SearchFilterHost.exe'
193	'2672,SearchIndexer.exe'	'9112,SearchProtocolHost.exe'
194	'2672,SearchIndexer.exe'	'9096,SearchFilterHost.exe'
195	'2672,SearchIndexer.exe'	'9896,SearchProtocolHost.exe'
196	'2672,SearchIndexer.exe'	'9920,SearchFilterHost.exe'
197	'2672,SearchIndexer.exe'	'10932,SearchProtocolHost.exe'
198	'2672,SearchIndexer.exe'	'11272,SearchFilterHost.exe'
199	'2672,SearchIndexer.exe'	'14552,SearchProtocolHost.exe'
200	'2672,SearchIndexer.exe'	'14572,SearchFilterHost.exe'
201	'2672,SearchIndexer.exe'	'15208,SearchProtocolHost.exe'
202	'2672,SearchIndexer.exe'	'15232,SearchFilterHost.exe'

203	'2672,SearchIndexer.exe'	'16052,SearchProtocolHost.exe'
204	'2672,SearchIndexer.exe'	'16072,SearchFilterHost.exe'
205	'2672,SearchIndexer.exe'	'18628,SearchProtocolHost.exe'
206	'2672,SearchIndexer.exe'	'18704,SearchFilterHost.exe'
207	'2996,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
208	'2996,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
209	'2936,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
210	'3040,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
211	'4040,XXX'	'1160,taskmgr.exe'
212	'1160,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
213	'1160,taskmgr.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
214	'1160,taskmgr.exe'	'OLEACC.dll,C:Windowssystem32OLEACC.dll'
215	'1160,taskmgr.exe'	'WINMM.dll,C:Windowssystem32WINMM.dll'
216	'1160,taskmgr.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
217	'1432,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
218	'1372,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
219	'736,XXX'	'3008,bash.exe'
220	'3008,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
221	'472,XXX'	'3984,driver_endpoint_netconn.exe'
222	'3984,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
223	'2852,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
224	'2852,cmd.exe'	'2076,java.exe'
225	'2664,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
226	'2076,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
227	'2076,java.exe'	'5588,java.exe'
228	'636,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
229	'636,firefox.exe'	'944,firefox.exe'
230	'636,firefox.exe'	'1104,simpress.exe'
231	'636,firefox.exe'	'5360,plugin-container.exe'
232	'944,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
233	'1828,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
234	'1828,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
235	'1828,cmd.exe'	'1436,NETSTAT.EXE'
236	'3128,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
237	'1436,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
238	'1436,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
239	'3876,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
240	'3116,gspawn-win64-helper.exe'	'1444,androiddump.exe'
241	'2364,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
242	'2364,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'

243	'2364,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
244	'2364,Wireshark.exe'	'3116,gspawn-win64-helper.exe'
245	'2364,Wireshark.exe'	'3224,dumpcap.exe'
246	'3224,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
247	'3524,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
248	'3960,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
249	'3960,FoxitReader.exe'	'3400,FoxitReaderUpdater.exe'
250	'3400,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
251	'4212,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
252	'4232,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
253	'4648,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
254	'4684,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
255	'4700,XXX'	'4716,bash.exe'
256	'4716,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
257	'1104,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
258	'1104,simpress.exe'	'4396,soffice.exe'
259	'4396,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
260	'4396,soffice.exe'	'4408,soffice.bin'
261	'4408,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
262	'5588,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
263	'5596,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
264	'5972,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
265	'5996,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
266	'5360,plugin-container.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
267	'5360,plugin-container.exe'	'5400,FlashPlayerPlugin_22_0_0_209.exe'
268	'5400,FlashPlayerPlugin_22_0_0_209.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
269	'5684,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
270	'5704,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
271	'5168,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
272	'6256,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
273	'6292,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
274	'6328,Hupigon.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
275	'6328,Hupigon.exe'	'6336,cmd.exe'
276	'6336,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
277	'6344,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
278	'6384,Hacker.com.cn.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
279	'6384,Hacker.com.cn.exe'	'6392,cmd.exe'
280	'6384,Hacker.com.cn.exe'	'6444,iexplore.exe'

281	'6392,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
282	'6400,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
283	'6436,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
284	'6464,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
285	'6916,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
286	'7188,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
287	'7296,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
288	'7296,firefox.exe'	'7468,firefox.exe'
289	'7468,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
290	'7776,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
291	'7776,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
292	'7776,Wireshark.exe'	'7924,dumpcap.exe'
293	'7776,Wireshark.exe'	'8048,dumpcap.exe'
294	'7924,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
295	'7932,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
296	'8048,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
297	'8056,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
298	'8340,calc.exe'	'OLEACC.dll,C:Windowssystem32OLEACC.dll'
299	'8556,iexplore.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
300	'8556,iexplore.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
301	'8556,iexplore.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
302	'8556,iexplore.exe'	'npmproxy.dll,C:WindowsSystem32npmproxy.dll'
303	'8556,iexplore.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
304	'8556,iexplore.exe'	'tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedink
305	'8556,iexplore.exe'	'Secur32.dll,C:WindowsSystem32Secur32.dll'
306	'8556,iexplore.exe'	'8608,iexplore.exe'
307	'8556,iexplore.exe'	'8952,iexplore.exe'
308	'8608,iexplore.exe'	'credssp.dll,C:Windowssystem32credssp.dll'
309	'8608,iexplore.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
310	'8608,iexplore.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
311	'8608,iexplore.exe'	'Dxtmsft.dll,C:WindowsSystem32Dxtmsft.dll'
312	'8608,iexplore.exe'	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
313	'8832,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
314	'8852,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
315	'8952,iexplore.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
316	'8952,iexplore.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
317	'8952,iexplore.exe'	'Dxtmsft.dll,C:WindowsSystem32Dxtmsft.dll'
318	'8952,iexplore.exe'	'msimg32.dll,C:Windowssystem32msimg32.dll'
319	'8952,iexplore.exe'	'WINSPOOL.DRV,C:WindowsSystem32WINSPOOL.DRV'

320	'9112,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
321	'9096,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
322	'9640,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
323	'9812,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
324	'9896,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
325	'9920,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
326	'10056,slui.exe'	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
327	'10112,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
328	'10112,firefox.exe'	'10408,pingsender.exe'
329	'10112,firefox.exe'	'9500,firefox.exe'
330	'9500,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
331	'10536,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
332	'10536,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
333	'10536,cmd.exe'	'10576,PING.EXE'
334	'10544,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
335	'10576,PING.EXE'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
336	'10984,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
337	'10984,soffice.exe'	'10992,soffice.bin'
338	'10992,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
339	'10748,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
340	'10932,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
341	'10932,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
342	'11272,SearchFilterHost.exe'	'MSVCR90.dll,C:WindowsWinSxSamd64_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6161_none_08e61857a83bc251MSVCR90.dll'
343	'11272,SearchFilterHost.exe'	'propertyhdl_x64.dll,C:Program Files (x86)OpenOffice 4programshlxthdlpropertyhdl_x64.dll'
344	'11476,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
345	'11544,swriter.exe'	'11552,soffice.exe'
346	'11552,soffice.exe'	'11560,soffice.bin'
347	'11672,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
348	'12008,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
349	'12008,firefox.exe'	'12172,firefox.exe'
350	'12172,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
351	'12836,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
352	'13088,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
353	'13192,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
354	'13228,notepad.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
355	'13280,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
356	'12536,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
357	'12744,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

358	'12708,notepad.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
359	'13020,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
360	'13148,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
361	'12728,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
362	'13448,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
363	'13524,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
364	'13532,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
365	'13624,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
366	'13712,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
367	'13816,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
368	'13876,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
369	'13912,XXX'	'13920,mstsc.exe'
370	'13920,mstsc.exe'	'tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedink
371	'14036,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
372	'14252,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
373	'14288,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
374	'14068,dllhost.exe'	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
375	'14068,dllhost.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
376	'13492,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
377	'14316,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
378	'14400,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
379	'14476,swriter.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
380	'14476,swriter.exe'	'14488,soffice.exe'
381	'14488,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
382	'14488,soffice.exe'	'14496,soffice.bin'
383	'14496,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
384	'14552,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
385	'14572,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
386	'14648,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
387	'14648,soffice.exe'	'14656,soffice.bin'
388	'14656,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
389	'14976,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
390	'15208,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
391	'15232,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
392	'15280,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
393	'12992,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
394	'15348,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
395	'15520,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
396	'15520,firefox.exe'	'15688,firefox.exe'

397	'15688,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
398	'16052,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
399	'16072,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
400	'13004,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
401	'13004,cmd.exe'	'16440,java.exe'
402	'16296,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
403	'16440,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
404	'16440,java.exe'	'19112,java.exe'
405	'16580,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
406	'16580,firefox.exe'	'16744,firefox.exe'
407	'16580,firefox.exe'	'18408,simpress.exe'
408	'16744,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
409	'17180,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
410	'17180,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
411	'17180,cmd.exe'	'17208,NETSTAT.EXE'
412	'17188,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
413	'17208,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
414	'17208,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
415	'17288,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
416	'17344,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
417	'17344,Wireshark.exe'	'16400,dumpcap.exe'
418	'16400,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
419	'16492,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
420	'13008,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
421	'17796,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
422	'17836,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
423	'17880,XXX'	'17896,bash.exe'
424	'17896,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
425	'18408,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
426	'18408,simpress.exe'	'18400,soffice.exe'
427	'18400,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
428	'18400,soffice.exe'	'18388,soffice.bin'
429	'18388,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
430	'19112,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
431	'19220,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
432	'18628,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
433	'18704,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'

7.2.6 Hupigon Malware – Instance 2

Table 105: Hupigon Malware Instance 2 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'356,XXX'
6	'368,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'416,XXX'
9	'428,csrss.exe'
10	'408,wininit.exe'
11	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
12	'464,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'512,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'528,lsm.exe'
17	'520,lsass.exe'
18	'GPAPI.dll,C:Windowssystem32GPAPI.dll'
19	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
20	'628,svchost.exe'
21	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
22	'692,VBoxService.exe'
23	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
24	'756,svchost.exe'
25	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
26	'848,svchost.exe'
27	'netutils.dll,C:WindowsSystem32netutils.dll'
28	'1008,audiodg.exe'
29	'904,svchost.exe'
30	'credssp.dll,C:WindowsSystem32credssp.dll'
31	'940,svchost.exe'
32	'rasman.dll,C:Windowssystem32rasman.dll'
33	'AVRT.dll,c:windowssystem32AVRT.dll'
34	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
35	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'

36	'420,svchost.exe'
37	'dsrole.dll,C:Windowssystem32dsrole.dll'
38	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
39	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
40	'832,svchost.exe'
41	'SensApi.dll,C:Windowssystem32SensApi.dll'
42	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
43	'1204,spoolsv.exe'
44	'1232,svchost.exe'
45	'1348,svchost.exe'
46	'1404,FoxitConnectedPDFService.exe'
47	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
48	'1860,svchost.exe'
49	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
50	'2000,taskhost.exe'
51	'midimap.dll,C:Windowssystem32midimap.dll'
52	'1340,dwm.exe'
53	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
54	'1052,XXX'
55	'1136,explorer.exe'
56	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
57	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
58	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
59	tquery.dll,C:Windowssystem32query.dll'
60	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
61	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
62	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
63	'bcryptprimitives.dll,C:Windowssystem32cryptprimitives.dll'
64	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
65	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
66	'2120,VBoxTray.exe'
67	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
68	'2136,MySQLNotifier.exe'
69	'2180,XXX'
70	'2228,jusched.exe'
71	'2416,WmiPrvSE.exe'
72	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
73	'2600,SearchIndexer.exe'
74	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
75	'NLSLexicons0010.dll,C:WindowsSystem32NLSLexicons0010.dll'
76	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'

77	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
78	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
79	'2776,sppsvc.exe'
80	'2952,svchost.exe'
81	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
82	'2920,mintty.exe'
83	'apphelp.dll,C:Windowssystem32apphelp.dll'
84	'2956,conhost.exe'
85	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
86	'2280,XXX'
87	'1376,bash.exe'
88	'authz.dll,C:Windowssystem32authz.dll'
89	'300,wmpnetwk.exe'
90	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
91	'provsvc.dll,C:WindowsSystem32provsvc.dll'
92	'1212,conhost.exe'
93	'1180,taskmgr.exe'
94	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
95	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
96	'DUser.dll,C:Windowssystem32DUser.dll'
97	'1108,XXX'
98	'2712,driver_endpoint_netconn.exe'
99	'1064,dllhost.exe'
100	'4020,SearchProtocolHost.exe'
101	'VERSION.dll,C:Windowssystem32VERSION.dll'
102	'4008,SearchFilterHost.exe'
103	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
104	'2864,cmd.exe'
105	'1792,java.exe'
106	'3056,conhost.exe'
107	'3132,java.exe'
108	'3364,firefox.exe'
109	'2704,firefox.exe'
110	'3476,conhost.exe'
111	'3784,pingsender.exe'
112	'3916,java.exe'
113	'1960,conhost.exe'
114	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
115	'1692,cmd.exe'
116	'3936,java.exe'
117	'364,firefox.exe'

118	'1016,firefox.exe'
119	'4524,cmd.exe'
120	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
121	'4532,conhost.exe'
122	'4552,NETSTAT.EXE'
123	'winrnr.dll,C:WindowsSystem32winrnr.dll'
124	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
125	'4636,notepad++.exe'
126	'4676,Wireshark.exe'
127	'4740,gspawn-win64-helper.exe'
128	'4752,androiddump.exe'
129	'msimtf.dll,C:Windowssystem32msimtf.dll'
130	'4824,dumpcap.exe'
131	'4832,conhost.exe'
132	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
133	'4776,FoxitReader.exe'
134	'4804,FoxitReaderUpdater.exe'
135	'5264,audiodg.exe'
136	'5108,SearchProtocolHost.exe'
137	'4144,SearchFilterHost.exe'
138	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
139	'5356,mintty.exe'
140	'5392,conhost.exe'
141	'5408,SearchFilterHost.exe'
142	'5424,bash.exe'
143	'5888,simpress.exe'
144	'5896,soffice.exe'
145	'5916,soffice.bin'
146	'6552,java.exe'
147	'6560,conhost.exe'
148	'6820,pingsender.exe'
149	'6844,conhost.exe'
150	'6952,SearchProtocolHost.exe'
151	'profapi.dll,C:Windowssystem32profapi.dll'
152	'6988,SearchFilterHost.exe'
153	'SXS.DLL,C:Windowssystem32SXS.DLL'
154	'6292,dllhost.exe'
155	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
156	'6788,dllhost.exe'
157	'6936,dllhost.exe'
158	'5092,consent.exe'

159	'6220,dllhost.exe'
160	'IDStore.dll,C:WindowsSystem32IDStore.dll'
161	'6652,dllhost.exe'
162	'6544,Hupigon.exe'
163	'6760,cmd.exe'
164	'6780,conhost.exe'
165	'6872,Hacker.com.cn.exe'
166	'6820,conhost.exe'
167	'6828,cmd.exe'
168	'9516,audiodg.exe'
169	'12404,audiodg.exe'
170	'14512,firefox.exe'
171	'15528,pingsender.exe'
172	'15540,conhost.exe'
173	'4896,iexplore.exe'
174	'1536,SearchProtocolHost.exe'
175	'7516,iexplore.exe'
176	'7576,iexplore.exe'
177	'7768,SearchProtocolHost.exe'
178	'7788,SearchFilterHost.exe'
179	'8028,iexplore.exe'
180	'npmproxy.dll,C:WindowsSystem32npmproxy.dll'
181	'msxml3.dll,C:WindowsSystem32msxml3.dll'
182	'8076,iexplore.exe'
183	'Dxtmsft.dll,C:WindowsSystem32Dxtmsft.dll'
184	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
185	'8340,dllhost.exe'
186	'8484,dllhost.exe'
187	'8564,firefox.exe'
188	'8736,firefox.exe'
189	'9232,soffice.exe'
190	'9244,soffice.bin'
191	'9584,taskhost.exe'
192	'9328,dllhost.exe'
193	'10236,SearchProtocolHost.exe'
194	'10252,SearchFilterHost.exe'
195	'10384,dllhost.exe'
196	'10456,WinRAR.exe'
197	'msimg32.dll,C:Windowssystem32msimg32.dll'
198	'10620,WinRAR.exe'
199	'rsaenh.dll,C:Windowssystem32rsaenh.dll'

200	'10676,WinRAR.exe'
201	'10760,WinRAR.exe'
202	'iertutil.dll,C:Windowssystem32iertutil.dll'
203	'10792,cmd.exe'
204	'10800,conhost.exe'
205	'11092,Wireshark.exe'
206	'11164,gspawn-win64-helper.exe'
207	'11176,androiddump.exe'
208	'11244,dumpcap.exe'
209	'11252,conhost.exe'
210	'10552,dumpcap.exe'
211	'10576,conhost.exe'
212	'11148,mspaint.exe'
213	'oleacc.dll,C:Windowssystem32oleacc.dll'
214	'browcli.dll,C:Windowssystem32rowcli.dll'
215	'SAMLIB.dll,C:Windowssystem32SAMLIB.dll'
216	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
217	'11180,svchost.exe'
218	'11352,slui.exe'
219	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
220	'11484,dllhost.exe'
221	'msxml6.dll,C:WindowsSystem32msxml6.dll'
222	'11716,SearchProtocolHost.exe'
223	'11740,SearchFilterHost.exe'
224	'12176,XXX'
225	'12184,javaw.exe'
226	'11872,dllhost.exe'
227	'12492,dllhost.exe'
228	'12612,splwow64.exe'
229	'12680,dllhost.exe'
230	'12696,notepad.exe'
231	'12764,dllhost.exe'
232	'12800,notepad.exe'
233	'12828,dllhost.exe'
234	'12868,notepad.exe'
235	'12920,dllhost.exe'
236	'12936,XXX'
237	'12976,wordpad.exe'
238	'13372,FoxitReader.exe'
239	'13500,SearchProtocolHost.exe'
240	'13520,SearchFilterHost.exe'

241	'13664,FoxitReader.exe'
242	'13896,firefox.exe'
243	'14064,firefox.exe'
244	'14676,firefox.exe'
245	'15640,WmiPrvSE.exe'
246	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
247	'15808,cmd.exe'
248	'15816,conhost.exe'
249	'15920,java.exe'
250	'16084,firefox.exe'
251	'16248,firefox.exe'
252	'15528,SearchProtocolHost.exe'
253	'15780,SearchFilterHost.exe'
254	'16472,cmd.exe'
255	'16480,conhost.exe'
256	'16516,NETSTAT.EXE'
257	'16576,notepad++.exe'
258	'16620,Wireshark.exe'
259	'16760,dumpcap.exe'
260	'16768,conhost.exe'
261	'17144,FoxitReader.exe'
262	'17356,SearchProtocolHost.exe'
263	'17392,SearchFilterHost.exe'
264	'17004,mintty.exe'
265	'17052,conhost.exe'
266	'17076,XXX'
267	'17084,bash.exe'
268	'16816,simpress.exe'
269	'16864,soffice.exe'
270	'16808,soffice.bin'
271	'17576,svchost.exe'
272	'18812,java.exe'
273	'18772,conhost.exe'
274	'19032,SearchProtocolHost.exe'
275	'19068,SearchFilterHost.exe'
276	'18456,conhost.exe'
277	'18480,pingsender.exe'
278	'19216,firefox.exe'
279	'18616,firefox.exe'
280	'19676,soffice.exe'
281	'19684,soffice.bin'

282	'19756,splwow64.exe'
283	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
284	'19860,firefox.exe'
285	'20024,firefox.exe'
286	'20360,audiodg.exe'
287	'20568,cmd.exe'
288	'20576,conhost.exe'
289	'20608,taskmgr.exe'
290	'21016,dllhost.exe'
291	'21124,dllhost.exe'
292	'21196,dllhost.exe'
293	'21232,dllhost.exe'
294	'21320,dllhost.exe'
295	'21332,cmd.exe'
296	'21360,conhost.exe'
297	'21460,cmd.exe'
298	'21468,conhost.exe'
299	'20956,SearchProtocolHost.exe'
300	'20972,SearchFilterHost.exe'
301	'21260,XXX'
302	'21264,msdt.exe'
303	'21484,sdiagnhost.exe'
304	'21060,dllhost.exe'
305	'21288,dllhost.exe'
306	'20868,dllhost.exe'
307	'21472,Hupigon.exe'
308	'21292,cmd.exe'
309	'21432,conhost.exe'
310	'21700,dllhost.exe'
311	'21736,dllhost.exe'
312	'21768,Hupigon.exe'
313	'21776,cmd.exe'
314	'21784,conhost.exe'
315	'21956,SearchProtocolHost.exe'
316	'slc.dll,C:Windowssystem32slc.dll'
317	'21976,SearchFilterHost.exe'
318	'22048,consent.exe'
319	'22148,dllhost.exe'
320	'22184,dllhost.exe'
321	'22220,Hupigon.exe'
322	'22228,cmd.exe'

323	'22236,conhost.exe'
324	'22392,consent.exe'
325	'22304,dllhost.exe'
326	'22416,dllhost.exe'
327	'22452,dllhost.exe'
328	'22484,taskmgr.exe'
329	'22352,iexplore.exe'
330	'wer.dll,C:Windowssystem32wer.dll'
331	'DUI70.dll,C:Windowssystem32DUI70.dll'
332	'22392,iexplore.exe'
333	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
334	'T2EMBED.DLL,C:Windowssystem32T2EMBED.DLL'
335	'hlink.dll,C:Windowssystem32hlink.dll'
336	'23040,SearchProtocolHost.exe'
337	'23060,SearchFilterHost.exe'
338	'22572,iexplore.exe'
339	'pngfilt.dll,C:WindowsSystem32pngfilt.dll'
340	'24020,taskhost.exe'

Table 106: Hupigon Malware Instance 2 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'356,XXX'	'368,csrss.exe'
5	'356,XXX'	'408,wininit.exe'
6	'368,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'368,csrss.exe'	'6820,conhost.exe'
8	'416,XXX'	'428,csrss.exe'
9	'416,XXX'	'464,winlogon.exe'
10	'428,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
11	'428,csrss.exe'	'2956,conhost.exe'
12	'428,csrss.exe'	'1212,conhost.exe'
13	'428,csrss.exe'	'3056,conhost.exe'
14	'428,csrss.exe'	'3476,conhost.exe'
15	'428,csrss.exe'	'1960,conhost.exe'
16	'428,csrss.exe'	'4532,conhost.exe'
17	'428,csrss.exe'	'4832,conhost.exe'
18	'428,csrss.exe'	'5392,conhost.exe'
19	'428,csrss.exe'	'6560,conhost.exe'
20	'428,csrss.exe'	'6844,conhost.exe'
21	'428,csrss.exe'	'6780,conhost.exe'
22	'428,csrss.exe'	'15540,conhost.exe'
23	'428,csrss.exe'	'10800,conhost.exe'
24	'428,csrss.exe'	'11252,conhost.exe'
25	'428,csrss.exe'	'10576,conhost.exe'
26	'428,csrss.exe'	'15816,conhost.exe'
27	'428,csrss.exe'	'16480,conhost.exe'
28	'428,csrss.exe'	'16768,conhost.exe'
29	'428,csrss.exe'	'17052,conhost.exe'
30	'428,csrss.exe'	'18772,conhost.exe'
31	'428,csrss.exe'	'18456,conhost.exe'
32	'428,csrss.exe'	'20576,conhost.exe'
33	'428,csrss.exe'	'21360,conhost.exe'
34	'428,csrss.exe'	'21468,conhost.exe'
35	'428,csrss.exe'	'21432,conhost.exe'
36	'428,csrss.exe'	'21784,conhost.exe'
37	'428,csrss.exe'	'22236,conhost.exe'
38	'408,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
39	'408,wininit.exe'	'512,services.exe'

40	'408,wininit.exe'	'528,lsm.exe'
41	'408,wininit.exe'	'520,lsass.exe'
42	'464,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
43	'512,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
44	'512,services.exe'	'628,svchost.exe'
45	'512,services.exe'	'692,VBoxService.exe'
46	'512,services.exe'	'756,svchost.exe'
47	'512,services.exe'	'848,svchost.exe'
48	'512,services.exe'	'904,svchost.exe'
49	'512,services.exe'	'940,svchost.exe'
50	'512,services.exe'	'420,svchost.exe'
51	'512,services.exe'	'832,svchost.exe'
52	'512,services.exe'	'1204,spoolsv.exe'
53	'512,services.exe'	'1232,svchost.exe'
54	'512,services.exe'	'1348,svchost.exe'
55	'512,services.exe'	'1404,FoxitConnectedPDFService.exe'
56	'512,services.exe'	'1860,svchost.exe'
57	'512,services.exe'	'2000,taskhost.exe'
58	'512,services.exe'	'2600,SearchIndexer.exe'
59	'512,services.exe'	'2776,sppsvc.exe'
60	'512,services.exe'	'2952,svchost.exe'
61	'512,services.exe'	'300,wmpnetwk.exe'
62	'512,services.exe'	'6872,Hacker.com.cn.exe'
63	'512,services.exe'	'9584,taskhost.exe'
64	'512,services.exe'	'11180,svchost.exe'
65	'512,services.exe'	'17576,svchost.exe'
66	'512,services.exe'	'24020,taskhost.exe'
67	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
68	'520,lsass.exe'	'GPAPI.dll,C:Windowssystem32GPAPI.dll'
69	'520,lsass.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
70	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
71	'628,svchost.exe'	'2416,WmiPrvSE.exe'
72	'628,svchost.exe'	'1064,dllhost.exe'
73	'628,svchost.exe'	'6292,dllhost.exe'
74	'628,svchost.exe'	'6788,dllhost.exe'
75	'628,svchost.exe'	'6936,dllhost.exe'
76	'628,svchost.exe'	'6220,dllhost.exe'
77	'628,svchost.exe'	'6652,dllhost.exe'
78	'628,svchost.exe'	'8340,dllhost.exe'
79	'628,svchost.exe'	'8484,dllhost.exe'
80	'628,svchost.exe'	'9328,dllhost.exe'

81	'628,svchost.exe'	'10384,dllhost.exe'
82	'628,svchost.exe'	'11352,slui.exe'
83	'628,svchost.exe'	'11484,dllhost.exe'
84	'628,svchost.exe'	'11872,dllhost.exe'
85	'628,svchost.exe'	'12492,dllhost.exe'
86	'628,svchost.exe'	'12680,dllhost.exe'
87	'628,svchost.exe'	'12764,dllhost.exe'
88	'628,svchost.exe'	'12828,dllhost.exe'
89	'628,svchost.exe'	'12920,dllhost.exe'
90	'628,svchost.exe'	'15640,WmiPrvSE.exe'
91	'628,svchost.exe'	'21016,dllhost.exe'
92	'628,svchost.exe'	'21124,dllhost.exe'
93	'628,svchost.exe'	'21196,dllhost.exe'
94	'628,svchost.exe'	'21232,dllhost.exe'
95	'628,svchost.exe'	'21320,dllhost.exe'
96	'628,svchost.exe'	'21484,sdiagnhost.exe'
97	'628,svchost.exe'	'21060,dllhost.exe'
98	'628,svchost.exe'	'21288,dllhost.exe'
99	'628,svchost.exe'	'20868,dllhost.exe'
100	'628,svchost.exe'	'21700,dllhost.exe'
101	'628,svchost.exe'	'21736,dllhost.exe'
102	'628,svchost.exe'	'22148,dllhost.exe'
103	'628,svchost.exe'	'22184,dllhost.exe'
104	'628,svchost.exe'	'22304,dllhost.exe'
105	'628,svchost.exe'	'22416,dllhost.exe'
106	'628,svchost.exe'	'22452,dllhost.exe'
107	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
108	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
109	'848,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
110	'848,svchost.exe'	'1008,audiodg.exe'
111	'848,svchost.exe'	'5264,audiodg.exe'
112	'848,svchost.exe'	'9516,audiodg.exe'
113	'848,svchost.exe'	'12404,audiodg.exe'
114	'848,svchost.exe'	'20360,audiodg.exe'
115	'904,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
116	'904,svchost.exe'	'1340,dwm.exe'
117	'940,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
118	'940,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
119	'940,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
120	'940,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
121	'940,svchost.exe'	'5092,consent.exe'

122	'940,svchost.exe'	'22048,consent.exe'
123	'940,svchost.exe'	'22392,consent.exe'
124	'420,svchost.exe'	'dsrole.dll,C:Windowssystem32dsrole.dll'
125	'420,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
126	'420,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
127	'832,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
128	'832,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
129	'1204,spoolsv.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
130	'1232,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
131	'1232,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
132	'1348,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
133	'1404,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
134	'1860,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
135	'2000,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
136	'1340,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
137	'1052,XXX'	'1136,explorer.exe'
138	'1136,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
139	'1136,explorer.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
140	'1136,explorer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
141	'1136,explorer.exe'	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
142	'1136,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
143	'1136,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
144	'1136,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
145	'1136,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
146	'1136,explorer.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
147	'1136,explorer.exe'	'bcryptprimitives.dll,C:Windowssystem32cryptprimitives.dll'
148	'1136,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
149	'1136,explorer.exe'	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
150	'1136,explorer.exe'	'2120,VBoxTray.exe'
151	'1136,explorer.exe'	'2136,MySQLNotifier.exe'
152	'1136,explorer.exe'	'2920,mintty.exe'
153	'1136,explorer.exe'	'2864,cmd.exe'
154	'1136,explorer.exe'	'3364,firefox.exe'
155	'1136,explorer.exe'	'1692,cmd.exe'
156	'1136,explorer.exe'	'364,firefox.exe'
157	'1136,explorer.exe'	'4524,cmd.exe'
158	'1136,explorer.exe'	'4636,notepad++.exe'
159	'1136,explorer.exe'	'4676,Wireshark.exe'
160	'1136,explorer.exe'	'4776,FoxitReader.exe'
161	'1136,explorer.exe'	'5356,mintty.exe'

162	'1136,explorer.exe'	'6544,Hupigon.exe'
163	'1136,explorer.exe'	'14512,firefox.exe'
164	'1136,explorer.exe'	'7516,iexplore.exe'
165	'1136,explorer.exe'	'8028,iexplore.exe'
166	'1136,explorer.exe'	'8564,firefox.exe'
167	'1136,explorer.exe'	'9232,soffice.exe'
168	'1136,explorer.exe'	'10456,WinRAR.exe'
169	'1136,explorer.exe'	'10620,WinRAR.exe'
170	'1136,explorer.exe'	'10676,WinRAR.exe'
171	'1136,explorer.exe'	'10760,WinRAR.exe'
172	'1136,explorer.exe'	'11092,Wireshark.exe'
173	'1136,explorer.exe'	'11148,mspaint.exe'
174	'1136,explorer.exe'	'12612,splwow64.exe'
175	'1136,explorer.exe'	'12696,notepad.exe'
176	'1136,explorer.exe'	'12800,notepad.exe'
177	'1136,explorer.exe'	'12868,notepad.exe'
178	'1136,explorer.exe'	'13372,FoxitReader.exe'
179	'1136,explorer.exe'	'13664,FoxitReader.exe'
180	'1136,explorer.exe'	'13896,firefox.exe'
181	'1136,explorer.exe'	'15808,cmd.exe'
182	'1136,explorer.exe'	'16084,firefox.exe'
183	'1136,explorer.exe'	'16472,cmd.exe'
184	'1136,explorer.exe'	'16576,notepad++.exe'
185	'1136,explorer.exe'	'16620,Wireshark.exe'
186	'1136,explorer.exe'	'17144,FoxitReader.exe'
187	'1136,explorer.exe'	'17004,mintty.exe'
188	'1136,explorer.exe'	'19216,firefox.exe'
189	'1136,explorer.exe'	'19676,soffice.exe'
190	'1136,explorer.exe'	'19860,firefox.exe'
191	'1136,explorer.exe'	'20568,cmd.exe'
192	'1136,explorer.exe'	'20608,taskmgr.exe'
193	'1136,explorer.exe'	'21332,cmd.exe'
194	'1136,explorer.exe'	'21460,cmd.exe'
195	'1136,explorer.exe'	'21472,Hupigon.exe'
196	'1136,explorer.exe'	'21768,Hupigon.exe'
197	'1136,explorer.exe'	'22220,Hupigon.exe'
198	'1136,explorer.exe'	'22352,iexplore.exe'
199	'2120,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
200	'2136,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
201	'2180,XXX'	'2228,jusched.exe'
202	'2228,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

203	'2416,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
204	'2600,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
205	'2600,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
206	'2600,SearchIndexer.exe'	'NLSLexicons0010.dll,C:WindowsSystem32NLSLexicons0010.dll'
207	'2600,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
208	'2600,SearchIndexer.exe'	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
209	'2600,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
210	'2600,SearchIndexer.exe'	'4020,SearchProtocolHost.exe'
211	'2600,SearchIndexer.exe'	'4008,SearchFilterHost.exe'
212	'2600,SearchIndexer.exe'	'5108,SearchProtocolHost.exe'
213	'2600,SearchIndexer.exe'	'4144,SearchFilterHost.exe'
214	'2600,SearchIndexer.exe'	'5408,SearchFilterHost.exe'
215	'2600,SearchIndexer.exe'	'6952,SearchProtocolHost.exe'
216	'2600,SearchIndexer.exe'	'6988,SearchFilterHost.exe'
217	'2600,SearchIndexer.exe'	'1536,SearchProtocolHost.exe'
218	'2600,SearchIndexer.exe'	'7768,SearchProtocolHost.exe'
219	'2600,SearchIndexer.exe'	'7788,SearchFilterHost.exe'
220	'2600,SearchIndexer.exe'	'10236,SearchProtocolHost.exe'
221	'2600,SearchIndexer.exe'	'10252,SearchFilterHost.exe'
222	'2600,SearchIndexer.exe'	'11716,SearchProtocolHost.exe'
223	'2600,SearchIndexer.exe'	'11740,SearchFilterHost.exe'
224	'2600,SearchIndexer.exe'	'13500,SearchProtocolHost.exe'
225	'2600,SearchIndexer.exe'	'13520,SearchFilterHost.exe'
226	'2600,SearchIndexer.exe'	'15528,SearchProtocolHost.exe'
227	'2600,SearchIndexer.exe'	'15780,SearchFilterHost.exe'
228	'2600,SearchIndexer.exe'	'17356,SearchProtocolHost.exe'
229	'2600,SearchIndexer.exe'	'17392,SearchFilterHost.exe'
230	'2600,SearchIndexer.exe'	'19032,SearchProtocolHost.exe'
231	'2600,SearchIndexer.exe'	'19068,SearchFilterHost.exe'

232	'2600,SearchIndexer.exe'	'20956,SearchProtocolHost.exe'
233	'2600,SearchIndexer.exe'	'20972,SearchFilterHost.exe'
234	'2600,SearchIndexer.exe'	'21956,SearchProtocolHost.exe'
235	'2600,SearchIndexer.exe'	'21976,SearchFilterHost.exe'
236	'2600,SearchIndexer.exe'	'23040,SearchProtocolHost.exe'
237	'2600,SearchIndexer.exe'	'23060,SearchFilterHost.exe'
238	'2776,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
239	'2952,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
240	'2920,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
241	'2956,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
242	'2280,XXX'	'1376,bash.exe'
243	'1376,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
244	'300,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
245	'300,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
246	'1212,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
247	'1212,conhost.exe'	'1180,taskmgr.exe'
248	'1180,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
249	'1180,taskmgr.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
250	'1180,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
251	'1108,XXX'	'2712,driver_endpoint_netconn.exe'
252	'2712,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
253	'1064,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
254	'4020,SearchProtocolHost.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
255	'4008,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
256	'2864,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
257	'2864,cmd.exe'	'1792,java.exe'
258	'2864,cmd.exe'	'3132,java.exe'
259	'3056,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
260	'3132,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
261	'3132,java.exe'	'3916,java.exe'
262	'3364,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
263	'3364,firefox.exe'	'2704,firefox.exe'
264	'3364,firefox.exe'	'3784,pingsender.exe'
265	'2704,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
266	'3476,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
267	'3784,pingsender.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
268	'3916,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

269	'1960,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
270	'1692,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
271	'1692,cmd.exe'	'3936,java.exe'
272	'3936,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
273	'3936,java.exe'	'6552,java.exe'
274	'364,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
275	'364,firefox.exe'	'1016,firefox.exe'
276	'364,firefox.exe'	'5888,simpress.exe'
277	'364,firefox.exe'	'6820,pingsender.exe'
278	'1016,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
279	'4524,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
280	'4524,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
281	'4524,cmd.exe'	'4552,NETSTAT.EXE'
282	'4532,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
283	'4552,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
284	'4552,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
285	'4636,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
286	'4676,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
287	'4676,Wireshark.exe'	'4740,gspawn-win64-helper.exe'
288	'4676,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
289	'4676,Wireshark.exe'	'4824,dumpcap.exe'
290	'4740,gspawn-win64-helper.exe'	'4752,androiddump.exe'
291	'4824,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
292	'4832,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
293	'4776,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
294	'4776,FoxitReader.exe'	'4804,FoxitReaderUpdater.exe'
295	'4804,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
296	'5108,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
297	'4144,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
298	'5356,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
299	'5392,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
300	'5408,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
301	'5408,SearchFilterHost.exe'	'5424,bash.exe'
302	'5424,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
303	'5888,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
304	'5888,simpress.exe'	'5896,soffice.exe'
305	'5896,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
306	'5896,soffice.exe'	'5916,soffice.bin'
307	'5916,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

308	'6552,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
309	'6560,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
310	'6952,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
311	'6988,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
312	'6292,dllhost.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
313	'6788,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
314	'6936,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
315	'5092,consent.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
316	'6220,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
317	'6652,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
318	'6544,Hupigon.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
319	'6544,Hupigon.exe'	'6760,cmd.exe'
320	'6760,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
321	'6780,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
322	'6872,Hacker.com.cn.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
323	'6872,Hacker.com.cn.exe'	'6828,cmd.exe'
324	'6872,Hacker.com.cn.exe'	'4896,iexplore.exe'
325	'6820,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
326	'6828,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
327	'14512,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
328	'14512,firefox.exe'	'15528,pingsender.exe'
329	'14512,firefox.exe'	'14676,firefox.exe'
330	'1536,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
331	'7516,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
332	'7516,iexplore.exe'	'7576,iexplore.exe'
333	'7576,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
334	'7768,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
335	'7788,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
336	'8028,iexplore.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
337	'8028,iexplore.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
338	'8028,iexplore.exe'	'npmproxy.dll,C:WindowsSystem32npmproxy.dll'
339	'8028,iexplore.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
340	'8028,iexplore.exe'	'8076,iexplore.exe'
341	'8076,iexplore.exe'	'Dxtmsft.dll,C:WindowsSystem32Dxtmsft.dll'
342	'8076,iexplore.exe'	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
343	'8340,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
344	'8484,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'

345	'8564,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
346	'8564,firefox.exe'	'8736,firefox.exe'
347	'8736,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
348	'9232,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
349	'9232,soffice.exe'	'9244,soffice.bin'
350	'9244,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
351	'9584,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
352	'9328,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
353	'10236,SearchProtocol Host.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
354	'10252,SearchFilterHost .exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
355	'10252,SearchFilterHost .exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
356	'10384,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
357	'10456,WinRAR.exe'	'msimg32.dll,C:Windowssystem32msimg32.dll'
358	'10620,WinRAR.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
359	'10676,WinRAR.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
360	'10760,WinRAR.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
361	'10760,WinRAR.exe'	'10792,cmd.exe'
362	'10792,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
363	'10800,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
364	'11092,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
365	'11092,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
366	'11092,Wireshark.exe'	'11164,gspawn-win64-helper.exe'
367	'11092,Wireshark.exe'	'11244,dumpcap.exe'
368	'11092,Wireshark.exe'	'10552,dumpcap.exe'
369	'11164,gspawn-win64-helper.exe'	'11176,androiddump.exe'
370	'10552,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
371	'10576,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
372	'11148,mspaint.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
373	'11148,mspaint.exe'	'browcli.dll,C:Windowssystem32rowcli.dll'
374	'11148,mspaint.exe'	'SAMLIB.dll,C:Windowssystem32SAMLIB.dll'
375	'11148,mspaint.exe'	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
376	'11180,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
377	'11352,slui.exe'	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
378	'11484,dllhost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
379	'11716,SearchProtocol Host.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
380	'11740,SearchFilterHost .exe'	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
381	'12176,XXX'	'12184,javaw.exe'
382	'12184,javaw.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
383	'11872,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'

384	'12492,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
385	'12612,splwow64.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
386	'12680,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
387	'12764,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
388	'12800,notepad.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
389	'12828,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
390	'12868,notepad.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
391	'12920,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
392	'12936,XXX'	'12976,wordpad.exe'
393	'12976,wordpad.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
394	'13372,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
395	'13500,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
396	'13520,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
397	'13664,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
398	'13896,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
399	'13896,firefox.exe'	'14064,firefox.exe'
400	'14064,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
401	'14676,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
402	'15640,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
403	'15808,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
404	'15808,cmd.exe'	'15920,java.exe'
405	'15816,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
406	'15920,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
407	'15920,java.exe'	'18812,java.exe'
408	'16084,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
409	'16084,firefox.exe'	'16248,firefox.exe'
410	'16084,firefox.exe'	'16816,simpress.exe'
411	'16084,firefox.exe'	'18480,pingsender.exe'
412	'16248,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
413	'15528,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
414	'15780,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
415	'16472,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
416	'16472,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
417	'16472,cmd.exe'	'16516,NETSTAT.EXE'
418	'16480,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
419	'16516,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
420	'16516,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
421	'16576,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
422	'16620,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'

423	'16620,Wireshark.exe'	'16760,dumpcap.exe'
424	'16760,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
425	'16768,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
426	'17144,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
427	'17356,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
428	'17392,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
429	'17004,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
430	'17052,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
431	'17076,XXX'	'17084,bash.exe'
432	'17084,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
433	'16816,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
434	'16816,simpress.exe'	'16864,soffice.exe'
435	'16864,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
436	'16864,soffice.exe'	'16808,soffice.bin'
437	'16808,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
438	'17576,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
439	'18812,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
440	'18772,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
441	'19032,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
442	'19068,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
443	'19216,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
444	'19216,firefox.exe'	'18616,firefox.exe'
445	'18616,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
446	'19676,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
447	'19676,soffice.exe'	'19684,soffice.bin'
448	'19684,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
449	'19684,soffice.bin'	'19756,splwow64.exe'
450	'19756,splwow64.exe'	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
451	'19860,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
452	'19860,firefox.exe'	'20024,firefox.exe'
453	'20024,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
454	'20568,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
455	'20576,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
456	'20608,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
457	'20608,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
458	'20608,taskmgr.exe'	'22484,taskmgr.exe'
459	'21016,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
460	'21124,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
461	'21196,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'

462	'21232,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
463	'21320,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
464	'21332,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
465	'21360,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
466	'21460,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
467	'21468,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
468	'20956,SearchProtocol Host.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
469	'20972,SearchFilterHost .exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
470	'21260,XXX'	'21264,msdt.exe'
471	'21060,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
472	'21288,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
473	'20868,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
474	'21472,Hupigon.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
475	'21472,Hupigon.exe'	'21292,cmd.exe'
476	'21292,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
477	'21432,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
478	'21700,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
479	'21736,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
480	'21768,Hupigon.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
481	'21768,Hupigon.exe'	'21776,cmd.exe'
482	'21776,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
483	'21784,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
484	'21956,SearchProtocol Host.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
485	'21956,SearchProtocol Host.exe'	'slc.dll,C:Windowssystem32slc.dll'
486	'21976,SearchFilterHost .exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
487	'21976,SearchFilterHost .exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
488	'22148,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
489	'22184,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
490	'22220,Hupigon.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
491	'22220,Hupigon.exe'	'22228,cmd.exe'
492	'22228,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
493	'22236,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
494	'22304,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
495	'22416,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
496	'22452,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
497	'22484,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
498	'22352,iexplore.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
499	'22352,iexplore.exe'	'npmproxy.dll,C:WindowsSystem32npmproxy.dll'
500	'22352,iexplore.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'

501	'22352,iexplore.exe'	'slc.dll,C:Windowssystem32slc.dll'
502	'22352,iexplore.exe'	'wer.dll,C:Windowssystem32wer.dll'
503	'22352,iexplore.exe'	'DUI70.dll,C:Windowssystem32DUI70.dll'
504	'22352,iexplore.exe'	'22392,iexplore.exe'
505	'22352,iexplore.exe'	'22572,iexplore.exe'
506	'22392,iexplore.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
507	'22392,iexplore.exe'	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
508	'22392,iexplore.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
509	'22392,iexplore.exe'	'T2EMBED.DLL,C:Windowssystem32T2EMBED.DLL'
510	'22392,iexplore.exe'	'hlink.dll,C:Windowssystem32hlink.dll'
511	'23040,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
512	'23060,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
513	'22572,iexplore.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
514	'22572,iexplore.exe'	'T2EMBED.DLL,C:Windowssystem32T2EMBED.DLL'
515	'22572,iexplore.exe'	'pngfilt.dll,C:WindowsSystem32pngfilt.dll'
516	'24020,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'

7.2.7 Zurgop Malware – Instance 1

Table 107: Zurgop Malware Instance 1 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,XXX'
6	'360,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'400,wininit.exe'
9	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
10	'412,XXX'
11	'424,csrss.exe'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'508,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'524,lsm.exe'
17	'516,lsass.exe'
18	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
19	'wkscli.dll,C:Windowssystem32wkscli.dll'
20	'628,svchost.exe'
21	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
22	'692,VBoxService.exe'
23	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
24	'756,svchost.exe'
25	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
26	'840,svchost.exe'
27	'rasadhlp.dll,C:WindowsSystem32rasadhlp.dll'
28	'winrnr.dll,C:WindowsSystem32winrnr.dll'
29	'888,svchost.exe'
30	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
31	'932,svchost.exe'
32	'appinfo.dll,c:windowssystem32appinfo.dll'
33	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
34	'AVRT.dll,c:windowssystem32AVRT.dll'
35	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'

36	'356,svchost.exe'
37	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
38	'316,svchost.exe'
39	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
40	'1136,spoolsv.exe'
41	'1180,svchost.exe'
42	'pnpts.dll,C:Windowssystem32pnpts.dll'
43	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
44	'1340,svchost.exe'
45	'SXS.DLL,C:Windowssystem32SXS.DLL'
46	'1380,FoxitConnectedPDFService.exe'
47	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
48	'1856,svchost.exe'
49	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
50	'1460,sppsvc.exe'
51	'1220,svchost.exe'
52	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
53	'1672,taskhost.exe'
54	'midimap.dll,C:Windowssystem32midimap.dll'
55	'864,dwm.exe'
56	'348,XXX'
57	'1888,explorer.exe'
58	'eappcfg.dll,C:Windowssystem32eappcfg.dll'
59	'tquery.dll,C:Windowssystem32query.dll'
60	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
61	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
62	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
63	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
64	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
65	'docprop.dll,C:Windowssystem32docprop.dll'
66	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
67	'connect.dll,C:Windowssystem32connect.dll'
68	'netprofm.dll,C:WindowsSystem32netprofm.dll'
69	'MSVCP90.dll,C:WindowsWinSxSamd64_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6161_none_08e61857a83bc251MSVCP90.dll'
70	'pwrshsip.dll,C:WindowsSystem32WindowsPowerShellv1.0pwrshsip.dll'
71	'956,VBoxTray.exe'
72	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
73	'1964,MySQLNotifier.exe'
74	'1008,XXX'
75	'2160,jusched.exe'
76	'2300,WmiPrvSE.exe'

77	'WMI.DLL,C:Windowssystem32WMI.DLL'
78	'1848,audiodg.exe'
79	'2656,wmpnetwk.exe'
80	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
81	'provsvc.dll,C:WindowsSystem32provsvc.dll'
82	'2620,mintty.exe'
83	'apphelp.dll,C:Windowssystem32apphelp.dll'
84	'1980,conhost.exe'
85	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
86	'2336,XXX'
87	'2812,bash.exe'
88	'authz.dll,C:Windowssystem32authz.dll'
89	'2900,SearchFilterHost.exe'
90	'2976,taskmgr.exe'
91	'DUser.dll,C:Windowssystem32DUser.dll'
92	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
93	'iertutil.dll,C:Windowssystem32iertutil.dll'
94	'OLEACC.dll,C:Windowssystem32OLEACC.dll'
95	'WINMM.dll,C:Windowssystem32WINMM.dll'
96	'600,SearchIndexer.exe'
97	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
98	'NLSLexicons0010.dll,C:WindowsSystem32NLSLexicons0010.dll'
99	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
100	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
101	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
102	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
103	'propsys.dll,C:Windowssystem32propsys.dll'
104	'332,SearchProtocolHost.exe'
105	'2144,XXX'
106	'856,driver_endpoint_netconn.exe'
107	'1944,TrustedInstaller.exe'
108	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
109	'smiengine.dll,C:Windowswinsxsamd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.1.7601.17514_none_678566b7ddea04a5smiengine.dll'
110	'1824,SearchFilterHost.exe'
111	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
112	'344,SearchProtocolHost.exe'
113	'2936,cmd.exe'
114	'2580,conhost.exe'
115	'2888,java.exe'
116	'2852,java.exe'
117	'3112,firefox.exe'

118	'3280,firefox.exe'
119	'3904,cmd.exe'
120	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
121	'3912,conhost.exe'
122	'3944,NETSTAT.EXE'
123	'4020,notepad++.exe'
124	'4076,Wireshark.exe'
125	'3604,gspawn-win64-helper.exe'
126	'3704,androiddump.exe'
127	'cryptnet.dll,C:Windowssystem32cryptnet.dll'
128	'3692,dumpcap.exe'
129	'3708,conhost.exe'
130	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
131	'4256,FoxitReader.exe'
132	'4292,FoxitReaderUpdater.exe'
133	'4472,SearchProtocolHost.exe'
134	'4492,SearchFilterHost.exe'
135	'4928,mintty.exe'
136	'4964,conhost.exe'
137	'4980,XXX'
138	'4996,bash.exe'
139	'4308,SearchProtocolHost.exe'
140	'4584,SearchFilterHost.exe'
141	'4200,simpress.exe'
142	'4284,soffice.exe'
143	'4304,soffice.bin'
144	'5556,SearchProtocolHost.exe'
145	'profapi.dll,C:Windowssystem32profapi.dll'
146	'5576,SearchFilterHost.exe'
147	'5492,plugin-container.exe'
148	'5540,FlashPlayerPlugin_22_0_0_209.exe'
149	'5616,FlashPlayerPlugin_22_0_0_209.exe'
150	'6044,java.exe'
151	'6052,conhost.exe'
152	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
153	'5160,svchost.exe'
154	'5784,slui.exe'
155	'5516,dllhost.exe'
156	'5760,WinRAR.exe'
157	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
158	'5848,SearchProtocolHost.exe'

159	'slc.dll,C:Windowssystem32slc.dll'
160	'VERSION.dll,C:Windowssystem32VERSION.dll'
161	'5808,SearchFilterHost.exe'
162	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
163	'5936,dllhost.exe'
164	'5644,dllhost.exe'
165	'5944,dllhost.exe'
166	'6164,consent.exe'
167	'6264,dllhost.exe'
168	'IDStore.dll,C:WindowsSystem32IDStore.dll'
169	'6300,dllhost.exe'
170	'6336,XXX'
171	'6344,svchost.exe'
172	'10208,audiodg.exe'
173	'10652,slui.exe'
174	'13848,audiodg.exe'
175	'14796,consent.exe'
176	'6500,dllhost.exe'
177	'6552,Wireshark.exe'
178	'msimtf.dll,C:Windowssystem32msimtf.dll'
179	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
180	'netutils.dll,C:Windowssystem32netutils.dll'
181	'6224,conhost.exe'
182	'6244,dumpcap.exe'
183	'DUI70.dll,C:Windowssystem32DUI70.dll'
184	'6692,dumpcap.exe'
185	'6700,conhost.exe'
186	'6824,dumpcap.exe'
187	'6832,conhost.exe'
188	'6864,dllhost.exe'
189	'6648,dumpcap.exe'
190	'6660,conhost.exe'
191	'6772,firefox.exe'
192	'7464,pingsender.exe'
193	'7492,conhost.exe'
194	'7148,firefox.exe'
195	'7876,cmd.exe'
196	'7884,conhost.exe'
197	'8196,sdraw.exe'
198	'8208,soffice.exe'
199	'8216,soffice.bin'

200	'8328,swriter.exe'
201	'8336,soffice.exe'
202	'8344,soffice.bin'
203	'8432,WmiPrvSE.exe'
204	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
205	'8804,dllhost.exe'
206	'8892,SearchProtocolHost.exe'
207	'8912,SearchFilterHost.exe'
208	'MSVCR90.dll,C:WindowsWinSxSamd64_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6161_none_08e61857a83bc251MSVCR90.dll'
209	'propertyhdl_x64.dll,C:Program Files (x86)OpenOffice 4programshlxthdlpropertyhdl_x64.dll'
210	'8996,dllhost.exe'
211	'9120,dllhost.exe'
212	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
213	'9100,dllhost.exe'
214	'9344,mspaint.exe'
215	'9376,svchost.exe'
216	'10032,dllhost.exe'
217	'9828,notepad++.exe'
218	'9864,dllhost.exe'
219	'11120,cmd.exe'
220	'11128,conhost.exe'
221	'11232,java.exe'
222	'11108,firefox.exe'
223	'11316,firefox.exe'
224	'11764,cmd.exe'
225	'11772,conhost.exe'
226	'11788,NETSTAT.EXE'
227	'11844,notepad++.exe'
228	'11888,Wireshark.exe'
229	'12040,dumpcap.exe'
230	'12048,conhost.exe'
231	'11944,FoxitReader.exe'
232	'12204,SearchProtocolHost.exe'
233	'12240,SearchFilterHost.exe'
234	'11840,mintty.exe'
235	'12084,conhost.exe'
236	'12304,XXX'
237	'12320,bash.exe'
238	'12756,simpress.exe'
239	'12780,soffice.exe'
240	'12788,soffice.bin'

241	'13244,firefox.exe'
242	'12728,java.exe'
243	'12884,conhost.exe'
244	'13508,plugin-container.exe'
245	'13544,FlashPlayerPlugin_22_0_0_209.exe'
246	'13568,FlashPlayerPlugin_22_0_0_209.exe'
247	'14096,dumpcap.exe'
248	'14104,conhost.exe'
249	'14124,SearchProtocolHost.exe'
250	'14144,SearchFilterHost.exe'
251	'13416,dllhost.exe'
252	'13492,slui.exe'
253	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
254	'13700,dllhost.exe'
255	'14064,dllhost.exe'
256	'13452,dllhost.exe'
257	'14016,consent.exe'
258	'12192,dllhost.exe'
259	'14032,dllhost.exe'
260	'14896,dllhost.exe'
261	'14932,dllhost.exe'
262	'14968,regedit.exe'
263	'15016,SearchProtocolHost.exe'
264	'15036,SearchFilterHost.exe'
265	'14484,dllhost.exe'
266	'14736,firefox.exe'
267	'14476,firefox.exe'
268	'15856,svchost.exe'
269	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
270	'15888,taskhost.exe'
271	'408,csrss.exe'
272	'416,wininit.exe'
273	'456,winlogon.exe'
274	'504,services.exe'
275	'520,lsm.exe'
276	'512,lsass.exe'
277	'620,svchost.exe'
278	'684,VBoxService.exe'
279	'748,svchost.exe'
280	'816,svchost.exe'
281	'USERENV.dll,C:WindowsSystem32USERENV.dll'

282	'880,svchost.exe'
283	'credssp.dll,C:WindowsSystem32credssp.dll'
284	'992,audiodg.exe'
285	'912,svchost.exe'
286	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
287	'wer.dll,C:Windowssystem32wer.dll'
288	'rasman.dll,C:Windowssystem32rasman.dll'
289	'320,svchost.exe'
290	'1060,svchost.exe'
291	'psapi.dll,C:Windowssystem32psapi.dll'
292	'1200,spoolsv.exe'
293	'1228,svchost.exe'
294	'1348,svchost.exe'
295	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
296	'1808,svchost.exe'
297	'1504,taskhost.exe'
298	'2088,sppsvc.exe'
299	'2244,dwm.exe'
300	'2236,XXX'
301	'2272,explorer.exe'
302	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
303	'browcli.dll,C:Windowssystem32rowcli.dll'
304	thumbcache.dll,C:Windowssystem32humbcache.dll'
305	'2356,VBoxTray.exe'
306	'2364,MySQLNotifier.exe'
307	'2436,XXX'
308	'2468,svchost.exe'
309	'2388,XXX'
310	'2600,jusched.exe'
311	'2748,WmiPrvSE.exe'
312	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
313	'2908,SearchIndexer.exe'
314	'2996,SearchProtocolHost.exe'
315	'3020,SearchFilterHost.exe'
316	'2004,wmpnetwk.exe'
317	'2268,mintty.exe'
318	'2616,conhost.exe'
319	'2716,XXX'
320	'2704,bash.exe'
321	'2540,XXX'
322	'2836,driver_endpoint_netconn.exe'

323	'2880,taskmgr.exe'
324	'2160,dllhost.exe'
325	'2676,dllhost.exe'
326	'2064,taskmgr.exe'
327	'2620,svchost.exe'
328	'3236,svchost.exe'
329	tdh.dll,C:WindowsSystem32dh.dll'
330	'3428,firefox.exe'
331	'3600,firefox.exe'
332	'3408,WMIADAP.exe'
333	'3796,WmiPrvSE.exe'
334	'4628,dllhost.exe'
335	'4928,dllhost.exe'
336	'4056,svchost.exe'

Table 108: Zurgop Malware Instance 1 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'352,XXX'	'360,csrss.exe'
5	'352,XXX'	'400,wininit.exe'
6	'352,XXX'	'416,wininit.exe'
7	'360,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'400,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
9	'400,wininit.exe'	'508,services.exe'
10	'400,wininit.exe'	'524,lsm.exe'
11	'400,wininit.exe'	'516,lsass.exe'
12	'400,wininit.exe'	'408,csrss.exe'
13	'400,wininit.exe'	'456,winlogon.exe'
14	'412,XXX'	'424,csrss.exe'
15	'412,XXX'	'460,winlogon.exe'
16	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
17	'424,csrss.exe'	'1980,conhost.exe'
18	'424,csrss.exe'	'2580,conhost.exe'
19	'424,csrss.exe'	'3912,conhost.exe'
20	'424,csrss.exe'	'3708,conhost.exe'
21	'424,csrss.exe'	'4964,conhost.exe'
22	'424,csrss.exe'	'6052,conhost.exe'
23	'424,csrss.exe'	'6224,conhost.exe'
24	'424,csrss.exe'	'6700,conhost.exe'
25	'424,csrss.exe'	'6832,conhost.exe'
26	'424,csrss.exe'	'6660,conhost.exe'
27	'424,csrss.exe'	'7492,conhost.exe'
28	'424,csrss.exe'	'7884,conhost.exe'
29	'424,csrss.exe'	'11128,conhost.exe'
30	'424,csrss.exe'	'11772,conhost.exe'
31	'424,csrss.exe'	'12048,conhost.exe'
32	'424,csrss.exe'	'12084,conhost.exe'
33	'424,csrss.exe'	'12884,conhost.exe'
34	'424,csrss.exe'	'14104,conhost.exe'
35	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
36	'508,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
37	'508,services.exe'	'628,svchost.exe'

38	'508,services.exe'	'692,VBoxService.exe'
39	'508,services.exe'	'756,svchost.exe'
40	'508,services.exe'	'840,svchost.exe'
41	'508,services.exe'	'888,svchost.exe'
42	'508,services.exe'	'932,svchost.exe'
43	'508,services.exe'	'356,svchost.exe'
44	'508,services.exe'	'316,svchost.exe'
45	'508,services.exe'	'1136,spoolsv.exe'
46	'508,services.exe'	'1180,svchost.exe'
47	'508,services.exe'	'1340,svchost.exe'
48	'508,services.exe'	'1380,FoxitConnectedPDFService.exe'
49	'508,services.exe'	'1856,svchost.exe'
50	'508,services.exe'	'1460,sppsvc.exe'
51	'508,services.exe'	'1220,svchost.exe'
52	'508,services.exe'	'1672,taskhost.exe'
53	'508,services.exe'	'2656,wmpnetwk.exe'
54	'508,services.exe'	'600,SearchIndexer.exe'
55	'508,services.exe'	'1944,TrustedInstaller.exe'
56	'508,services.exe'	'5160,svchost.exe'
57	'508,services.exe'	'9376,svchost.exe'
58	'508,services.exe'	'15856,svchost.exe'
59	'508,services.exe'	'15888,taskhost.exe'
60	'524,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
61	'516,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
62	'516,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
63	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
64	'628,svchost.exe'	'2300,WmiPrvSE.exe'
65	'628,svchost.exe'	'5784,slui.exe'
66	'628,svchost.exe'	'5516,dllhost.exe'
67	'628,svchost.exe'	'5936,dllhost.exe'
68	'628,svchost.exe'	'5644,dllhost.exe'
69	'628,svchost.exe'	'5944,dllhost.exe'
70	'628,svchost.exe'	'6264,dllhost.exe'
71	'628,svchost.exe'	'6300,dllhost.exe'
72	'628,svchost.exe'	'10652,slui.exe'
73	'628,svchost.exe'	'6500,dllhost.exe'
74	'628,svchost.exe'	'6864,dllhost.exe'
75	'628,svchost.exe'	'8432,WmiPrvSE.exe'
76	'628,svchost.exe'	'8804,dllhost.exe'
77	'628,svchost.exe'	'8996,dllhost.exe'
78	'628,svchost.exe'	'9120,dllhost.exe'

79	'628,svchost.exe'	'9100,dllhost.exe'
80	'628,svchost.exe'	'10032,dllhost.exe'
81	'628,svchost.exe'	'9864,dllhost.exe'
82	'628,svchost.exe'	'13416,dllhost.exe'
83	'628,svchost.exe'	'13492,slui.exe'
84	'628,svchost.exe'	'13700,dllhost.exe'
85	'628,svchost.exe'	'14064,dllhost.exe'
86	'628,svchost.exe'	'13452,dllhost.exe'
87	'628,svchost.exe'	'12192,dllhost.exe'
88	'628,svchost.exe'	'14032,dllhost.exe'
89	'628,svchost.exe'	'14896,dllhost.exe'
90	'628,svchost.exe'	'14932,dllhost.exe'
91	'628,svchost.exe'	'14484,dllhost.exe'
92	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
93	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
94	'840,svchost.exe'	'rasadhlp.dll,C:WindowsSystem32rasadhlp.dll'
95	'840,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
96	'840,svchost.exe'	'1848,audiodg.exe'
97	'840,svchost.exe'	'10208,audiodg.exe'
98	'840,svchost.exe'	'13848,audiodg.exe'
99	'888,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
100	'888,svchost.exe'	'864,dwm.exe'
101	'932,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
102	'932,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
103	'932,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
104	'932,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
105	'932,svchost.exe'	'6164,consent.exe'
106	'932,svchost.exe'	'14796,consent.exe'
107	'932,svchost.exe'	'14016,consent.exe'
108	'356,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
109	'316,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
110	'1136,spoolsv.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
111	'1180,svchost.exe'	'pnpts.dll,C:Windowssystem32pnpts.dll'
112	'1180,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
113	'1340,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
114	'1380,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
115	'1856,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
116	'1460,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
117	'1220,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
118	'1672,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'

119	'864,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
120	'348,XXX'	'1888,explorer.exe'
121	'1888,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
122	'1888,explorer.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
123	'1888,explorer.exe'	'eappcfg.dll,C:Windowssystem32eappcfg.dll'
124	'1888,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
125	'1888,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
126	'1888,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
127	'1888,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
128	'1888,explorer.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
129	'1888,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
130	'1888,explorer.exe'	'docprop.dll,C:Windowssystem32docprop.dll'
131	'1888,explorer.exe'	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
132	'1888,explorer.exe'	'connect.dll,C:Windowssystem32connect.dll'
133	'1888,explorer.exe'	'netprofm.dll,C:WindowsSystem32netprofm.dll'
134	'1888,explorer.exe'	'MSVCP90.dll,C:WindowsWinSxSamd64_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6161_none_08e61857a83bc251MSVCP90.dll'
135	'1888,explorer.exe'	'pwrshsip.dll,C:WindowsSystem32WindowsPowerShellv1.0pwrshsip.dll'
136	'1888,explorer.exe'	'956,VBoxTray.exe'
137	'1888,explorer.exe'	'1964,MySQLNotifier.exe'
138	'1888,explorer.exe'	'2620,mintty.exe'
139	'1888,explorer.exe'	'2936,cmd.exe'
140	'1888,explorer.exe'	'3112,firefox.exe'
141	'1888,explorer.exe'	'3904,cmd.exe'
142	'1888,explorer.exe'	'4020,notepad++.exe'
143	'1888,explorer.exe'	'4076,Wireshark.exe'
144	'1888,explorer.exe'	'4256,FoxitReader.exe'
145	'1888,explorer.exe'	'4928,mintty.exe'
146	'1888,explorer.exe'	'5760,WinRAR.exe'
147	'1888,explorer.exe'	'6552,Wireshark.exe'
148	'1888,explorer.exe'	'6772,firefox.exe'
149	'1888,explorer.exe'	'7876,cmd.exe'
150	'1888,explorer.exe'	'8196,sdraw.exe'
151	'1888,explorer.exe'	'8328,swriter.exe'
152	'1888,explorer.exe'	'9344,mspaint.exe'
153	'1888,explorer.exe'	'9828,notepad++.exe'
154	'1888,explorer.exe'	'11120,cmd.exe'
155	'1888,explorer.exe'	'11108,firefox.exe'
156	'1888,explorer.exe'	'11764,cmd.exe'
157	'1888,explorer.exe'	'11844,notepad++.exe'

158	'1888,explorer.exe'	'11888,Wireshark.exe'
159	'1888,explorer.exe'	'11944,FoxitReader.exe'
160	'1888,explorer.exe'	'11840,mintty.exe'
161	'1888,explorer.exe'	'13244,firefox.exe'
162	'1888,explorer.exe'	'14968,regedit.exe'
163	'1888,explorer.exe'	'14736,firefox.exe'
164	'956,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
165	'1964,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
166	'1008,XXX'	'2160,jusched.exe'
167	'2160,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
168	'2300,WmiPrvSE.exe'	'rasadhlp.dll,C:WindowsSystem32rasadhlp.dll'
169	'2300,WmiPrvSE.exe'	'WMI.DLL,C:Windowssystem32WMI.DLL'
170	'2656,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
171	'2656,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
172	'2620,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
173	'1980,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
174	'2336,XXX'	'2812,bash.exe'
175	'2812,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
176	'2900,SearchFilterHost.exe'	'2976,taskmgr.exe'
177	'2900,SearchFilterHost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
178	'2976,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
179	'2976,taskmgr.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
180	'2976,taskmgr.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
181	'2976,taskmgr.exe'	'OLEACC.dll,C:Windowssystem32OLEACC.dll'
182	'2976,taskmgr.exe'	'WINMM.dll,C:Windowssystem32WINMM.dll'
183	'600,SearchIndexer.exe'	'2900,SearchFilterHost.exe'
184	'600,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
185	'600,SearchIndexer.exe'	'NLSLexicons0010.dll,C:WindowsSystem32NLSLexicons0010.dll'
186	'600,SearchIndexer.exe'	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
187	'600,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
188	'600,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
189	'600,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
190	'600,SearchIndexer.exe'	'332,SearchProtocolHost.exe'
191	'600,SearchIndexer.exe'	'1824,SearchFilterHost.exe'
192	'600,SearchIndexer.exe'	'344,SearchProtocolHost.exe'

193	'600,SearchIndexer.exe'	'4472,SearchProtocolHost.exe'
194	'600,SearchIndexer.exe'	'4492,SearchFilterHost.exe'
195	'600,SearchIndexer.exe'	'4308,SearchProtocolHost.exe'
196	'600,SearchIndexer.exe'	'4584,SearchFilterHost.exe'
197	'600,SearchIndexer.exe'	'5556,SearchProtocolHost.exe'
198	'600,SearchIndexer.exe'	'5576,SearchFilterHost.exe'
199	'600,SearchIndexer.exe'	'5848,SearchProtocolHost.exe'
200	'600,SearchIndexer.exe'	'5808,SearchFilterHost.exe'
201	'600,SearchIndexer.exe'	'8892,SearchProtocolHost.exe'
202	'600,SearchIndexer.exe'	'8912,SearchFilterHost.exe'
203	'600,SearchIndexer.exe'	'12204,SearchProtocolHost.exe'
204	'600,SearchIndexer.exe'	'12240,SearchFilterHost.exe'
205	'600,SearchIndexer.exe'	'14124,SearchProtocolHost.exe'
206	'600,SearchIndexer.exe'	'14144,SearchFilterHost.exe'
207	'600,SearchIndexer.exe'	'15016,SearchProtocolHost.exe'
208	'600,SearchIndexer.exe'	'15036,SearchFilterHost.exe'
209	'332,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
210	'2144,XXX'	'856,driver_endpoint_netconn.exe'
211	'2144,XXX'	'2620,svchost.exe'
212	'856,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
213	'1944,TrustedInstaller.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
214	'1944,TrustedInstaller.exe'	'smiengine.dll,C:Windowswinsxsamd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.1.7601.17514_none_678566b7ddea04a5smiengine.dll'
215	'1824,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
216	'344,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
217	'2936,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
218	'2936,cmd.exe'	'2888,java.exe'
219	'2936,cmd.exe'	'2852,java.exe'
220	'2580,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
221	'2852,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
222	'2852,java.exe'	'6044,java.exe'
223	'3112,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
224	'3112,firefox.exe'	'3280,firefox.exe'
225	'3112,firefox.exe'	'4200,simpress.exe'
226	'3112,firefox.exe'	'5492,plugin-container.exe'
227	'3280,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
228	'3904,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
229	'3904,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'

230	'3904,cmd.exe'	'3944,NETSTAT.EXE'
231	'3912,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
232	'3944,NETSTAT.EXE'	'rasadhlp.dll,C:WindowsSystem32rasadhlp.dll'
233	'3944,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
234	'4020,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
235	'4076,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
236	'4076,Wireshark.exe'	'3604,gspawn-win64-helper.exe'
237	'4076,Wireshark.exe'	'cryptnet.dll,C:Windowssystem32cryptnet.dll'
238	'4076,Wireshark.exe'	'3692,dumpcap.exe'
239	'3604,gspawn-win64-helper.exe'	'3704,androiddump.exe'
240	'3692,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
241	'3708,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
242	'4256,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
243	'4256,FoxitReader.exe'	'4292,FoxitReaderUpdater.exe'
244	'4292,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
245	'4472,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
246	'4492,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
247	'4928,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
248	'4964,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
249	'4980,XXX'	'4996,bash.exe'
250	'4996,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
251	'4308,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
252	'4584,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
253	'4200,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
254	'4200,simpress.exe'	'4284,soffice.exe'
255	'4284,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
256	'4284,soffice.exe'	'4304,soffice.bin'
257	'4304,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
258	'5556,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
259	'5556,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
260	'5576,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
261	'5576,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
262	'5492,plugin-container.exe'	'5540,FlashPlayerPlugin_22_0_0_209.exe'
263	'5540,FlashPlayerPlugin_22_0_0_209.exe'	'5616,FlashPlayerPlugin_22_0_0_209.exe'
264	'6044,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

265	'6052,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
266	'5160,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
267	'5516,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
268	'5760,WinRAR.exe'	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
269	'5848,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
270	'5848,SearchProtocolHost.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
271	'5808,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
272	'5808,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
273	'5936,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
274	'5644,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
275	'5944,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
276	'6164,consent.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
277	'6264,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
278	'6300,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
279	'6336,XXX'	'6344,svchost.exe'
280	'6344,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
281	'6500,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
282	'6552,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
283	'6552,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
284	'6552,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
285	'6552,Wireshark.exe'	'netutils.dll,C:Windowssystem32netutils.dll'
286	'6552,Wireshark.exe'	'6244,dumpcap.exe'
287	'6552,Wireshark.exe'	'DUI70.dll,C:Windowssystem32DUI70.dll'
288	'6552,Wireshark.exe'	'6692,dumpcap.exe'
289	'6552,Wireshark.exe'	'6824,dumpcap.exe'
290	'6552,Wireshark.exe'	'6648,dumpcap.exe'
291	'6692,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
292	'6700,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
293	'6824,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
294	'6832,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
295	'6864,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
296	'6648,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
297	'6660,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
298	'6772,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
299	'6772,firefox.exe'	'7464,pingsender.exe'
300	'6772,firefox.exe'	'7148,firefox.exe'
301	'7148,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

302	'8196,sdraw.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
303	'8196,sdraw.exe'	'8208,soffice.exe'
304	'8208,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
305	'8208,soffice.exe'	'8216,soffice.bin'
306	'8216,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
307	'8328,swriter.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
308	'8328,swriter.exe'	'8336,soffice.exe'
309	'8336,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
310	'8336,soffice.exe'	'8344,soffice.bin'
311	'8344,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
312	'8432,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
313	'8804,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
314	'8892,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
315	'8892,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
316	'8912,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
317	'8912,SearchFilterHost.exe'	'MSVCR90.dll,C:WindowsWinSxSamd64_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6161_none_08e61857a83bc251MSVCR90.dll'
318	'8912,SearchFilterHost.exe'	'propertyhdl_x64.dll,C:Program Files (x86)OpenOffice 4programshlxthdlpropertyhdl_x64.dll'
319	'8996,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
320	'9120,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
321	'9100,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
322	'9344,mspaint.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
323	'9344,mspaint.exe'	'OLEACC.dll,C:Windowssystem32OLEACC.dll'
324	'9376,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
325	'10032,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
326	'9828,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
327	'9864,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
328	'11120,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
329	'11120,cmd.exe'	'11232,java.exe'
330	'11128,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
331	'11232,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
332	'11232,java.exe'	'12728,java.exe'
333	'11108,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
334	'11108,firefox.exe'	'11316,firefox.exe'
335	'11108,firefox.exe'	'12756,simpress.exe'
336	'11108,firefox.exe'	'13508,plugin-container.exe'
337	'11316,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

338	'11764,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
339	'11764,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
340	'11764,cmd.exe'	'11788,NETSTAT.EXE'
341	'11772,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
342	'11788,NETSTAT.EXE'	'rasadhlp.dll,C:WindowsSystem32rasadhlp.dll'
343	'11788,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
344	'11844,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
345	'11888,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
346	'11888,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
347	'11888,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
348	'11888,Wireshark.exe'	'12040,dumpcap.exe'
349	'11888,Wireshark.exe'	'14096,dumpcap.exe'
350	'12040,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
351	'12048,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
352	'11944,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
353	'12204,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
354	'12240,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
355	'11840,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
356	'12084,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
357	'12304,XXX'	'12320,bash.exe'
358	'12320,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
359	'12756,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
360	'12756,simpress.exe'	'12780,soffice.exe'
361	'12780,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
362	'12780,soffice.exe'	'12788,soffice.bin'
363	'12788,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
364	'12728,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
365	'12884,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
366	'13508,plugin-container.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
367	'13508,plugin-container.exe'	'13544,FlashPlayerPlugin_22_0_0_209.exe'
368	'13544,FlashPlayerPlugin_22_0_0_209.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
369	'13544,FlashPlayerPlugin_22_0_0_209.exe'	'13568,FlashPlayerPlugin_22_0_0_209.exe'
370	'13568,FlashPlayerPlugin_22_0_0_209.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
371	'14096,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
372	'14104,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
373	'14124,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'

374	'14124,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
375	'14144,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
376	'14144,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
377	'13416,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
378	'13492,slui.exe'	'OLEACC.dll,C:Windowssystem32OLEACC.dll'
379	'13492,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
380	'13700,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
381	'14064,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
382	'13452,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
383	'14016,consent.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
384	'12192,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
385	'14032,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
386	'14896,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
387	'14932,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
388	'14968,regedit.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
389	'15016,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
390	'15036,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
391	'14484,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
392	'14736,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
393	'14736,firefox.exe'	'14476,firefox.exe'
394	'14476,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
395	'15856,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
396	'15888,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
397	'408,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
398	'408,csrss.exe'	'2616,conhost.exe'
399	'416,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
400	'416,wininit.exe'	'504,services.exe'
401	'416,wininit.exe'	'520,lsm.exe'
402	'416,wininit.exe'	'512,lsass.exe'
403	'456,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
404	'504,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
405	'504,services.exe'	'1380,FoxitConnectedPDFService.exe'
406	'504,services.exe'	'620,svchost.exe'
407	'504,services.exe'	'684,VBoxService.exe'
408	'504,services.exe'	'748,svchost.exe'
409	'504,services.exe'	'816,svchost.exe'

410	'504,services.exe'	'880,svchost.exe'
411	'504,services.exe'	'912,svchost.exe'
412	'504,services.exe'	'320,svchost.exe'
413	'504,services.exe'	'1060,svchost.exe'
414	'504,services.exe'	'1200,spoolsv.exe'
415	'504,services.exe'	'1228,svchost.exe'
416	'504,services.exe'	'1348,svchost.exe'
417	'504,services.exe'	'1808,svchost.exe'
418	'504,services.exe'	'1504,taskhost.exe'
419	'504,services.exe'	'2088,sppsvc.exe'
420	'504,services.exe'	'2908,SearchIndexer.exe'
421	'504,services.exe'	'2004,wmpnetwk.exe'
422	'504,services.exe'	'3236,svchost.exe'
423	'504,services.exe'	'4056,svchost.exe'
424	'520,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
425	'512,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
426	'512,lsass.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
427	'620,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
428	'620,svchost.exe'	'2748,WmiPrvSE.exe'
429	'620,svchost.exe'	'2160,dllhost.exe'
430	'620,svchost.exe'	'2676,dllhost.exe'
431	'620,svchost.exe'	'3796,WmiPrvSE.exe'
432	'620,svchost.exe'	'4628,dllhost.exe'
433	'620,svchost.exe'	'4928,dllhost.exe'
434	'684,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
435	'748,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
436	'816,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
437	'816,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
438	'816,svchost.exe'	'netutils.dll,C:Windowssystem32netutils.dll'
439	'816,svchost.exe'	'USERENV.dll,C:WindowsSystem32USERENV.dll'
440	'816,svchost.exe'	'992,audiodg.exe'
441	'880,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
442	'880,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
443	'880,svchost.exe'	'2244,dwm.exe'
444	'912,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
445	'912,svchost.exe'	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
446	'912,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
447	'912,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
448	'912,svchost.exe'	'3408,WMIADAP.exe'
449	'320,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
450	'320,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'

451	'320,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
452	'1060,svchost.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
453	'1200,spoolsv.exe'	'netutils.dll,C:Windowssystem32netutils.dll'
454	'1228,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
455	'1228,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
456	'1348,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
457	'1348,svchost.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
458	'1348,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
459	'1808,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
460	'1504,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
461	'2088,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
462	'2244,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
463	'2236,XXX'	'2272,explorer.exe'
464	'2272,explorer.exe'	'OLEACC.dll,C:Windowssystem32OLEACC.dll'
465	'2272,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
466	'2272,explorer.exe'	'browcli.dll,C:Windowssystem32rowcli.dll'
467	'2272,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
468	'2272,explorer.exe'	'2356,VBoxTray.exe'
469	'2272,explorer.exe'	'2364,MySQLNotifier.exe'
470	'2272,explorer.exe'	'2268,mintty.exe'
471	'2272,explorer.exe'	'2880,taskmgr.exe'
472	'2272,explorer.exe'	'3428,firefox.exe'
473	'2356,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
474	'2364,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
475	'2436,XXX'	'2468,svchost.exe'
476	'2468,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
477	'2388,XXX'	'2600,jusched.exe'
478	'2600,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
479	'2748,WmiPrvSE.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
480	'2748,WmiPrvSE.exe'	'rasadhlp.dll,C:WindowsSystem32rasadhlp.dll'
481	'2748,WmiPrvSE.exe'	'WMI.DLL,C:Windowssystem32WMI.DLL'
482	'2748,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
483	'2908,SearchIndexer.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
484	'2908,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
485	'2908,SearchIndexer.exe'	'2996,SearchProtocolHost.exe'
486	'2908,SearchIndexer.exe'	'3020,SearchFilterHost.exe'

487	'2996,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
488	'3020,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
489	'2004,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
490	'2268,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
491	'2616,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
492	'2716,XXX'	'2704,bash.exe'
493	'2704,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
494	'2540,XXX'	'2836,driver_endpoint_netconn.exe'
495	'2836,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
496	'2880,taskmgr.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
497	'2880,taskmgr.exe'	'2064,taskmgr.exe'
498	'2160,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
499	'2676,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
500	'2064,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
501	'2064,taskmgr.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
502	'2064,taskmgr.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
503	'2064,taskmgr.exe'	'WINMM.dll,C:Windowssystem32WINMM.dll'
504	'2064,taskmgr.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
505	'2620,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
506	'3236,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
507	'3236,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
508	'3236,svchost.exe'	tdh.dll,C:WindowsSystem32dh.dll'
509	'3428,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
510	'3428,firefox.exe'	'3600,firefox.exe'
511	'3600,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
512	'3408,WMIADAP.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
513	'3408,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
514	'3796,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
515	'4628,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
516	'4928,dllhost.exe'	'propsys.dll,C:Windowssystem32propsys.dll'
517	'4056,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'

7.2.8 Zurgop Malware – Instance 2

Table 109: Zurgop Malware Instance 2 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'504,services.exe'
4	'1116,sppsvc.exe'
5	'1220,spoolsv.exe'
6	'1248,svchost.exe'
7	'288,smss.exe'
8	'356,XXX'
9	'364,csrss.exe'
10	'412,XXX'
11	'424,csrss.exe'
12	'460,winlogon.exe'
13	'404,wininit.exe'
14	'528,lsm.exe'
15	'628,svchost.exe'
16	'692,VBoxService.exe'
17	'884,svchost.exe'
18	'836,svchost.exe'
19	'996,audiodg.exe'
20	'756,svchost.exe'
21	'928,svchost.exe'
22	'1856,svchost.exe'
23	'520,lsass.exe'
24	'1408,FoxitConnectedPDFService.exe'
25	'1096,svchost.exe'
26	'1348,svchost.exe'
27	'308,svchost.exe'
28	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
29	'352,XXX'
30	'360,csrss.exe'
31	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
32	'400,wininit.exe'
33	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
34	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
35	'508,services.exe'

36	'wship6.dll,C:WindowsSystem32wship6.dll'
37	'524,lsm.exe'
38	'516,lsass.exe'
39	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
40	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
41	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
42	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
43	'848,svchost.exe'
44	'netutils.dll,C:WindowsSystem32netutils.dll'
45	'1000,audiodg.exe'
46	'892,svchost.exe'
47	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
48	'adsldpc.dll,c:windowssystem32adsldpc.dll'
49	'AVRT.dll,c:windowssystem32AVRT.dll'
50	'HID.DLL,C:WindowsSystem32HID.DLL'
51	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
52	'380,svchost.exe'
53	'vmictimeprovider.dll,C:WindowsSystem32vmictimeprovider.dll'
54	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
55	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
56	'SensApi.dll,C:Windowssystem32SensApi.dll'
57	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
58	'1140,spoolsv.exe'
59	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
60	'1184,svchost.exe'
61	'1332,svchost.exe'
62	'SXS.DLL,C:Windowssystem32SXS.DLL'
63	'1372,FoxitConnectedPDFService.exe'
64	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
65	'1876,svchost.exe'
66	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
67	'1212,taskhost.exe'
68	'midimap.dll,C:Windowssystem32midimap.dll'
69	'1232,XXX'
70	'1596,explorer.exe'
71	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
72	'1988,dwm.exe'
73	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
74	'NaturalLanguage6.dll,C:WindowsSystem32NaturalLanguage6.dll'
75	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
76	tquery.dll,C:Windowssystem32query.dll'

77	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
78	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
79	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
80	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
81	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
82	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
83	'2140,VBoxTray.exe'
84	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
85	'2164,MySQLNotifier.exe'
86	'2204,XXX'
87	'2288,jusched.exe'
88	'2436,WmiPrvSE.exe'
89	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
90	'2608,SearchIndexer.exe'
91	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
92	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
93	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
94	'2820,wmpnetwk.exe'
95	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
96	'provsvc.dll,C:WindowsSystem32provsvc.dll'
97	'2328,sppsvc.exe'
98	'2548,svchost.exe'
99	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
100	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
101	'1852,XXX'
102	'2376,taskmgr.exe'
103	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
104	'DUser.dll,C:Windowssystem32DUser.dll'
105	'iertutil.dll,C:Windowssystem32iertutil.dll'
106	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
107	'1844,WmiPrvSE.exe'
108	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
109	'2856,mintty.exe'
110	'apphelp.dll,C:Windowssystem32apphelp.dll'
111	'2772,conhost.exe'
112	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
113	'596,XXX'
114	'2892,bash.exe'
115	'authz.dll,C:Windowssystem32authz.dll'
116	'1028,XXX'
117	'2072,driver_endpoint_netconn.exe'

118	'2064,SearchFilterHost.exe'
119	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
120	'684,SearchProtocolHost.exe'
121	'3256,cmd.exe'
122	'3264,conhost.exe'
123	'3380,java.exe'
124	'3496,firefox.exe'
125	'3660,firefox.exe'
126	'3160,audiodg.exe'
127	'3580,cmd.exe'
128	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
129	'3740,conhost.exe'
130	'3964,NETSTAT.EXE'
131	'winrnr.dll,C:WindowsSystem32winrnr.dll'
132	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
133	'3200,notepad++.exe'
134	'3100,Wireshark.exe'
135	'3356,dumpcap.exe'
136	'3344,conhost.exe'
137	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
138	'4284,FoxitReader.exe'
139	'4332,FoxitReaderUpdater.exe'
140	'6252,audiodg.exe'
141	'4540,SearchProtocolHost.exe'
142	'4572,SearchFilterHost.exe'
143	'5040,mintty.exe'
144	'5068,conhost.exe'
145	'5088,XXX'
146	'5100,bash.exe'
147	'4728,taskhost.exe'
148	'4900,simpress.exe'
149	'4960,soffice.exe'
150	'5016,soffice.bin'
151	'5340,java.exe'
152	'5308,conhost.exe'
153	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
154	'5216,conhost.exe'
155	'6032,pingsender.exe'
156	'6364,SearchProtocolHost.exe'
157	'profapi.dll,C:Windowssystem32profapi.dll'
158	'6384,SearchFilterHost.exe'

159	'7128,consent.exe'
160	'6692,dllhost.exe'
161	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
162	'6936,dllhost.exe'
163	'7076,dllhost.exe'
164	'6328,dllhost.exe'
165	'IDStore.dll,C:WindowsSystem32IDStore.dll'
166	'6436,dllhost.exe'
167	'6320,XXX'
168	'6296,svchost.exe'
169	'7804,audiodg.exe'
170	'10464,audiodg.exe'
171	'6600,SnippingTool.exe'
172	'2792,wisptis.exe'
173	tpcps.dll,C:Program FilesCommon FilesMicrosoft SharedInkpcps.dll'
174	'7036,mspaint.exe'
175	'oleacc.dll,C:Windowssystem32oleacc.dll'
176	'7056,svchost.exe'
177	'8112,dllhost.exe'
178	'8376,dllhost.exe'
179	'8492,dllhost.exe'
180	'8536,dllhost.exe'
181	'8576,consent.exe'
182	'8692,dllhost.exe'
183	'8732,dllhost.exe'
184	'8832,dllhost.exe'
185	'8884,dllhost.exe'
186	'8576,dllhost.exe'
187	'4364,conhost.exe'
188	'8524,cmd.exe'
189	'8584,dllhost.exe'
190	'8932,FoxitReader.exe'
191	'9308,SearchProtocolHost.exe'
192	'9328,SearchFilterHost.exe'
193	'9428,firefox.exe'
194	'9596,firefox.exe'
195	'9568,dllhost.exe'
196	'9840,XXX'
197	'10020,wordpad.exe'
198	'10236,splwow64.exe'
199	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'

200	'10304,dllhost.exe'
201	'10376,dllhost.exe'
202	'10412,dllhost.exe'
203	'10444,wusa.exe'
204	'10564,dllhost.exe'
205	'10600,xwizard.exe'
206	'10716,slui.exe'
207	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
208	'11584,cmd.exe'
209	'11592,conhost.exe'
210	'11700,java.exe'
211	'11852,firefox.exe'
212	'12020,firefox.exe'
213	'11564,conhost.exe'
214	'12256,cmd.exe'
215	'12100,NETSTAT.EXE'
216	'12340,notepad++.exe'
217	'12372,Wireshark.exe'
218	'12440,gspawn-win64-helper.exe'
219	'12452,androiddump.exe'
220	'msimtf.dll,C:Windowssystem32msimtf.dll'
221	'12520,dumpcap.exe'
222	'12528,conhost.exe'
223	'12620,audiodg.exe'
224	'12992,FoxitReader.exe'
225	'13148,SearchProtocolHost.exe'
226	'13196,SearchFilterHost.exe'
227	'12844,mintty.exe'
228	'12880,conhost.exe'
229	'12884,XXX'
230	'12944,bash.exe'
231	'12788,WmiPrvSE.exe'
232	'12300,SearchProtocolHost.exe'
233	'12516,SearchFilterHost.exe'
234	'13436,simpress.exe'
235	'13444,soffice.exe'
236	'13452,soffice.bin'
237	'13696,svchost.exe'
238	'13916,SearchProtocolHost.exe'
239	'13972,SearchFilterHost.exe'
240	'14272,java.exe'

241	'12652,conhost.exe'
242	'14184,dllhost.exe'
243	'14724,dllhost.exe'
244	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
245	'14828,dllhost.exe'
246	'14960,Wireshark.exe'
247	'15020,gspawn-win64-helper.exe'
248	'15032,androiddump.exe'
249	'15160,dumpcap.exe'
250	'15168,conhost.exe'
251	'15236,simpress.exe'
252	'15244,soffice.exe'
253	'15256,soffice.bin'
254	'2028,taskhost.exe'
255	'2208,userinit.exe'
256	'2216,dwm.exe'
257	'2236,explorer.exe'
258	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
259	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
260	'sbdrop.dll,C:Program FilesWindows Sidebarsbdrop.dll'
261	'2328,VBoxTray.exe'
262	'2340,MySQLNotifier.exe'
263	'2412,XXX'
264	'2456,svchost.exe'
265	'2364,XXX'
266	'2480,jusched.exe'
267	'2684,WmiPrvSE.exe'
268	'2844,SearchIndexer.exe'
269	'2192,mintty.exe'
270	'1928,conhost.exe'
271	'2300,XXX'
272	'2448,bash.exe'
273	'2636,wmpnetwk.exe'
274	'2932,XXX'
275	'2000,driver_endpoint_netconn.exe'
276	'2520,dllhost.exe'
277	'2652,dllhost.exe'
278	'2580,taskmgr.exe'
279	'580,taskmgr.exe'
280	'3856,svchost.exe'
281	'1568,dllhost.exe'

282	'3212,dllhost.exe'
283	'164,taskmgr.exe'
284	'776,taskmgr.exe'
285	'1604,WmiPrvSE.exe'
286	'300,WMIADAP.exe'
287	'MPR.dll,C:Windowssystem32MPR.dll'
288	'3292,dllhost.exe'
289	'3532,dllhost.exe'
290	'3548,ftp.exe'
291	'3572,conhost.exe'
292	'3728,dllhost.exe'
293	'3988,dllhost.exe'
294	'4056,dllhost.exe'
295	'4092,cmd.exe'
296	'2920,conhost.exe'
297	'1084,SearchProtocolHost.exe'
298	'1260,SearchFilterHost.exe'
299	'2904,swriter.exe'
300	'3020,soffice.exe'
301	'2576,soffice.bin'
302	'664,soffice.exe'
303	'1616,soffice.bin'

Table 110: Zurgop Malware Instance 2 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'504,services.exe'	'1116,sppsvc.exe'
4	'504,services.exe'	'1220,spoolsv.exe'
5	'504,services.exe'	'1248,svchost.exe'
6	'504,services.exe'	'628,svchost.exe'
7	'504,services.exe'	'692,VBoxService.exe'
8	'504,services.exe'	'884,svchost.exe'
9	'504,services.exe'	'836,svchost.exe'
10	'504,services.exe'	'756,svchost.exe'
11	'504,services.exe'	'928,svchost.exe'
12	'504,services.exe'	'1856,svchost.exe'
13	'504,services.exe'	'1408,FoxitConnectedPDFService.exe'
14	'504,services.exe'	'1096,svchost.exe'
15	'504,services.exe'	'1348,svchost.exe'
16	'504,services.exe'	'308,svchost.exe'
17	'504,services.exe'	'2028,taskhost.exe'
18	'504,services.exe'	'2844,SearchIndexer.exe'
19	'504,services.exe'	'2636,wmpnetwk.exe'
20	'504,services.exe'	'3856,svchost.exe'
21	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
22	'356,XXX'	'364,csrss.exe'
23	'356,XXX'	'404,wininit.exe'
24	'412,XXX'	'424,csrss.exe'
25	'412,XXX'	'460,winlogon.exe'
26	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
27	'424,csrss.exe'	'2772,conhost.exe'
28	'424,csrss.exe'	'3264,conhost.exe'
29	'424,csrss.exe'	'3740,conhost.exe'
30	'424,csrss.exe'	'3344,conhost.exe'
31	'424,csrss.exe'	'5068,conhost.exe'
32	'424,csrss.exe'	'5308,conhost.exe'
33	'424,csrss.exe'	'5216,conhost.exe'
34	'424,csrss.exe'	'4364,conhost.exe'
35	'424,csrss.exe'	'11592,conhost.exe'
36	'424,csrss.exe'	'11564,conhost.exe'
37	'424,csrss.exe'	'12528,conhost.exe'
38	'424,csrss.exe'	'12880,conhost.exe'
39	'424,csrss.exe'	'12652,conhost.exe'

40	'424,csrss.exe'	'15168,conhost.exe'
41	'424,csrss.exe'	'1928,conhost.exe'
42	'424,csrss.exe'	'3572,conhost.exe'
43	'424,csrss.exe'	'2920,conhost.exe'
44	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
45	'460,winlogon.exe'	'2208,userinit.exe'
46	'404,wininit.exe'	'504,services.exe'
47	'404,wininit.exe'	'528,lsm.exe'
48	'404,wininit.exe'	'520,lsass.exe'
49	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
50	'628,svchost.exe'	'2436,WmiPrvSE.exe'
51	'628,svchost.exe'	'1844,WmiPrvSE.exe'
52	'628,svchost.exe'	'6692,dllhost.exe'
53	'628,svchost.exe'	'6936,dllhost.exe'
54	'628,svchost.exe'	'7076,dllhost.exe'
55	'628,svchost.exe'	'6328,dllhost.exe'
56	'628,svchost.exe'	'6436,dllhost.exe'
57	'628,svchost.exe'	'8112,dllhost.exe'
58	'628,svchost.exe'	'8376,dllhost.exe'
59	'628,svchost.exe'	'8492,dllhost.exe'
60	'628,svchost.exe'	'8536,dllhost.exe'
61	'628,svchost.exe'	'8692,dllhost.exe'
62	'628,svchost.exe'	'8732,dllhost.exe'
63	'628,svchost.exe'	'8832,dllhost.exe'
64	'628,svchost.exe'	'8884,dllhost.exe'
65	'628,svchost.exe'	'8576,dllhost.exe'
66	'628,svchost.exe'	'8584,dllhost.exe'
67	'628,svchost.exe'	'9568,dllhost.exe'
68	'628,svchost.exe'	'10304,dllhost.exe'
69	'628,svchost.exe'	'10376,dllhost.exe'
70	'628,svchost.exe'	'10412,dllhost.exe'
71	'628,svchost.exe'	'10564,dllhost.exe'
72	'628,svchost.exe'	'10716,slui.exe'
73	'628,svchost.exe'	'12788,WmiPrvSE.exe'
74	'628,svchost.exe'	'14184,dllhost.exe'
75	'628,svchost.exe'	'14724,dllhost.exe'
76	'628,svchost.exe'	'14828,dllhost.exe'
77	'628,svchost.exe'	'2684,WmiPrvSE.exe'
78	'628,svchost.exe'	'2520,dllhost.exe'
79	'628,svchost.exe'	'2652,dllhost.exe'
80	'628,svchost.exe'	'1568,dllhost.exe'

81	'628,svchost.exe'	'3212,dllhost.exe'
82	'628,svchost.exe'	'1604,WmiPrvSE.exe'
83	'628,svchost.exe'	'3292,dllhost.exe'
84	'628,svchost.exe'	'3532,dllhost.exe'
85	'628,svchost.exe'	'3728,dllhost.exe'
86	'628,svchost.exe'	'3988,dllhost.exe'
87	'628,svchost.exe'	'4056,dllhost.exe'
88	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
89	'884,svchost.exe'	'2216,dwm.exe'
90	'836,svchost.exe'	'996,audiodg.exe'
91	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
92	'928,svchost.exe'	'adsldpc.dll,c:windowssystem32adsldpc.dll'
93	'928,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
94	'928,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
95	'928,svchost.exe'	'7128,consent.exe'
96	'928,svchost.exe'	'8576,consent.exe'
97	'928,svchost.exe'	'300,WMIADAP.exe'
98	'308,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
99	'308,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
100	'352,XXX'	'360,csrss.exe'
101	'352,XXX'	'400,wininit.exe'
102	'360,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
103	'400,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
104	'400,wininit.exe'	'508,services.exe'
105	'400,wininit.exe'	'524,lsm.exe'
106	'400,wininit.exe'	'516,lsass.exe'
107	'508,services.exe'	'628,svchost.exe'
108	'508,services.exe'	'692,VBoxService.exe'
109	'508,services.exe'	'756,svchost.exe'
110	'508,services.exe'	'928,svchost.exe'
111	'508,services.exe'	'308,svchost.exe'
112	'508,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
113	'508,services.exe'	'848,svchost.exe'
114	'508,services.exe'	'892,svchost.exe'
115	'508,services.exe'	'380,svchost.exe'
116	'508,services.exe'	'1140,spoolsv.exe'
117	'508,services.exe'	'1184,svchost.exe'
118	'508,services.exe'	'1332,svchost.exe'
119	'508,services.exe'	'1372,FoxitConnectedPDFService.exe'
120	'508,services.exe'	'1876,svchost.exe'
121	'508,services.exe'	'1212,taskhost.exe'

122	'508,services.exe'	'2608,SearchIndexer.exe'
123	'508,services.exe'	'2820,wmpnetwk.exe'
124	'508,services.exe'	'2328,sppsvc.exe'
125	'508,services.exe'	'2548,svchost.exe'
126	'508,services.exe'	'4728,taskhost.exe'
127	'508,services.exe'	'7056,svchost.exe'
128	'508,services.exe'	'13696,svchost.exe'
129	'524,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
130	'516,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
131	'848,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
132	'848,svchost.exe'	'1000,audiodg.exe'
133	'848,svchost.exe'	'3160,audiodg.exe'
134	'848,svchost.exe'	'6252,audiodg.exe'
135	'848,svchost.exe'	'7804,audiodg.exe'
136	'848,svchost.exe'	'10464,audiodg.exe'
137	'848,svchost.exe'	'12620,audiodg.exe'
138	'892,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
139	'892,svchost.exe'	'HID.DLL,C:WindowsSystem32HID.DLL'
140	'892,svchost.exe'	'1988,dwm.exe'
141	'892,svchost.exe'	'2792,wisptis.exe'
142	'380,svchost.exe'	'vmictimeprovider.dll,C:WindowsSystem32vmictimeprovider.dll'
143	'380,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
144	'380,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
145	'1140,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
146	'1184,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
147	'1184,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
148	'1332,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
149	'1372,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
150	'1876,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
151	'1212,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
152	'1232,XXX'	'1596,explorer.exe'
153	'1596,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
154	'1596,explorer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
155	'1596,explorer.exe'	'NaturalLanguage6.dll,C:WindowsSystem32NaturalLanguage6.dll'
156	'1596,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
157	'1596,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
158	'1596,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
159	'1596,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
160	'1596,explorer.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
161	'1596,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'

162	'1596,explorer.exe'	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
163	'1596,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
164	'1596,explorer.exe'	'2140,VBoxTray.exe'
165	'1596,explorer.exe'	'2164,MySQLNotifier.exe'
166	'1596,explorer.exe'	'2856,mintty.exe'
167	'1596,explorer.exe'	'3256,cmd.exe'
168	'1596,explorer.exe'	'3496,firefox.exe'
169	'1596,explorer.exe'	'3580,cmd.exe'
170	'1596,explorer.exe'	'3200,notepad++.exe'
171	'1596,explorer.exe'	'3100,Wireshark.exe'
172	'1596,explorer.exe'	'4284,FoxitReader.exe'
173	'1596,explorer.exe'	'5040,mintty.exe'
174	'1596,explorer.exe'	'6600,SnippingTool.exe'
175	'1596,explorer.exe'	'7036,mspaint.exe'
176	'1596,explorer.exe'	'8524,cmd.exe'
177	'1596,explorer.exe'	'8932,FoxitReader.exe'
178	'1596,explorer.exe'	'9428,firefox.exe'
179	'1596,explorer.exe'	'10444,wusa.exe'
180	'1596,explorer.exe'	'10600,xwizard.exe'
181	'1596,explorer.exe'	'11584,cmd.exe'
182	'1596,explorer.exe'	'11852,firefox.exe'
183	'1596,explorer.exe'	'12256,cmd.exe'
184	'1596,explorer.exe'	'12340,notepad++.exe'
185	'1596,explorer.exe'	'12372,Wireshark.exe'
186	'1596,explorer.exe'	'12992,FoxitReader.exe'
187	'1596,explorer.exe'	'12844,mintty.exe'
188	'1596,explorer.exe'	'14960,Wireshark.exe'
189	'1596,explorer.exe'	'15236,simpress.exe'
190	'1988,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
191	'2140,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
192	'2164,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
193	'2204,XXX'	'2288,jusched.exe'
194	'2288,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
195	'2436,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
196	'2608,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
197	'2608,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
198	'2608,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
199	'2608,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
200	'2608,SearchIndexer.exe'	'2064,SearchFilterHost.exe'
201	'2608,SearchIndexer.exe'	'684,SearchProtocolHost.exe'
202	'2608,SearchIndexer.exe'	'4540,SearchProtocolHost.exe'

203	'2608,SearchIndexer.exe'	'4572,SearchFilterHost.exe'
204	'2608,SearchIndexer.exe'	'6364,SearchProtocolHost.exe'
205	'2608,SearchIndexer.exe'	'6384,SearchFilterHost.exe'
206	'2608,SearchIndexer.exe'	'9308,SearchProtocolHost.exe'
207	'2608,SearchIndexer.exe'	'9328,SearchFilterHost.exe'
208	'2608,SearchIndexer.exe'	'13148,SearchProtocolHost.exe'
209	'2608,SearchIndexer.exe'	'13196,SearchFilterHost.exe'
210	'2608,SearchIndexer.exe'	'12300,SearchProtocolHost.exe'
211	'2608,SearchIndexer.exe'	'12516,SearchFilterHost.exe'
212	'2608,SearchIndexer.exe'	'13916,SearchProtocolHost.exe'
213	'2608,SearchIndexer.exe'	'13972,SearchFilterHost.exe'
214	'2820,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
215	'2820,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
216	'2328,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
217	'2548,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
218	'2548,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
219	'1852,XXX'	'2376,taskmgr.exe'
220	'2376,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
221	'2376,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
222	'2376,taskmgr.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
223	'2376,taskmgr.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
224	'1844,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
225	'2856,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
226	'2772,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
227	'596,XXX'	'2892,bash.exe'
228	'2892,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
229	'1028,XXX'	'2072,driver_endpoint_netconn.exe'
230	'2072,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
231	'2064,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
232	'684,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
233	'3256,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
234	'3256,cmd.exe'	'3380,java.exe'
235	'3264,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
236	'3380,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
237	'3380,java.exe'	'5340,java.exe'
238	'3496,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
239	'3496,firefox.exe'	'3660,firefox.exe'
240	'3496,firefox.exe'	'4900,simpress.exe'
241	'3496,firefox.exe'	'6032,pingsender.exe'
242	'3660,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
243	'3580,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'

244	'3580,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
245	'3580,cmd.exe'	'3964,NETSTAT.EXE'
246	'3740,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
247	'3964,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
248	'3964,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
249	'3200,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
250	'3100,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
251	'3100,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
252	'3100,Wireshark.exe'	'3356,dumpcap.exe'
253	'3356,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
254	'3344,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
255	'4284,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
256	'4284,FoxitReader.exe'	'4332,FoxitReaderUpdater.exe'
257	'4332,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
258	'4540,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
259	'4572,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
260	'5040,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
261	'5068,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
262	'5088,XXX'	'5100,bash.exe'
263	'5100,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
264	'4728,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
265	'4900,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
266	'4900,simpress.exe'	'4960,soffice.exe'
267	'4960,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
268	'4960,soffice.exe'	'5016,soffice.bin'
269	'5016,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
270	'5340,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
271	'5308,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
272	'5216,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
273	'6032,pingsender.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
274	'6364,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
275	'6364,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
276	'6384,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
277	'6384,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
278	'6692,dllhost.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
279	'6936,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
280	'7076,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
281	'6328,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
282	'6436,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
283	'6320,XXX'	'6296,svchost.exe'
284	'6296,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

285	'6600,SnippingTool.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
286	'2792,wisptis.exe'	tpcps.dll,C:Program FilesCommon FilesMicrosoft SharedInkpcps.dll'
287	'7036,mspaint.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
288	'7036,mspaint.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
289	'7056,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
290	'8112,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
291	'8376,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
292	'8492,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
293	'8536,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
294	'8692,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
295	'8732,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
296	'8832,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
297	'8884,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
298	'8576,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
299	'4364,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
300	'8524,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
301	'8524,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
302	'8584,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
303	'8932,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
304	'9308,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
305	'9308,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
306	'9328,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
307	'9328,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
308	'9428,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
309	'9428,firefox.exe'	'9596,firefox.exe'
310	'9596,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
311	'9568,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
312	'9840,XXX'	'10020,wordpad.exe'
313	'10020,wordpad.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
314	'10020,wordpad.exe'	'10236,splwow64.exe'
315	'10236,splwow64.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
316	'10236,splwow64.exe'	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
317	'10304,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
318	'10376,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
319	'10412,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
320	'10444,wusa.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
321	'10564,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
322	'10600,xwizard.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
323	'10716,slui.exe'	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
324	'11584,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
325	'11584,cmd.exe'	'11700,java.exe'

326	'11592,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
327	'11700,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
328	'11700,java.exe'	'14272,java.exe'
329	'11852,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
330	'11852,firefox.exe'	'12020,firefox.exe'
331	'11852,firefox.exe'	'13436,simpress.exe'
332	'12020,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
333	'11564,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
334	'12256,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
335	'12256,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
336	'12256,cmd.exe'	'12100,NETSTAT.EXE'
337	'12100,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
338	'12100,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
339	'12340,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
340	'12372,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
341	'12372,Wireshark.exe'	'12440,gspawn-win64-helper.exe'
342	'12372,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
343	'12372,Wireshark.exe'	'12520,dumpcap.exe'
344	'12440,gspawn-win64-helper.exe'	'12452,androiddump.exe'
345	'12520,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
346	'12528,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
347	'12992,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
348	'13148,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
349	'13196,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
350	'12844,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
351	'12880,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
352	'12884,XXX'	'12944,bash.exe'
353	'12944,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
354	'12788,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
355	'12300,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
356	'12516,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
357	'13436,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
358	'13436,simpress.exe'	'13444,soffice.exe'
359	'13444,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
360	'13444,soffice.exe'	'13452,soffice.bin'
361	'13452,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
362	'13696,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
363	'13916,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
364	'13916,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
365	'13972,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
366	'13972,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'

367	'14272,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
368	'12652,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
369	'14184,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
370	'14724,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
371	'14828,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
372	'14960,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
373	'14960,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
374	'14960,Wireshark.exe'	'15020,gspawn-win64-helper.exe'
375	'14960,Wireshark.exe'	'15160,dumpcap.exe'
376	'15020,gspawn-win64-helper.exe'	'15032,androiddump.exe'
377	'15160,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
378	'15168,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
379	'15236,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
380	'15236,simpress.exe'	'15244,soffice.exe'
381	'15244,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
382	'15244,soffice.exe'	'15256,soffice.bin'
383	'15256,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
384	'2028,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
385	'2208,userinit.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
386	'2208,userinit.exe'	'2236,explorer.exe'
387	'2216,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
388	'2236,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
389	'2236,explorer.exe'	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
390	'2236,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
391	'2236,explorer.exe'	'sbdrop.dll,C:Program FilesWindows Sidebarsbdrop.dll'
392	'2236,explorer.exe'	'2328,VBoxTray.exe'
393	'2236,explorer.exe'	'2340,MySQLNotifier.exe'
394	'2236,explorer.exe'	'2192,mintty.exe'
395	'2236,explorer.exe'	'2580,taskmgr.exe'
396	'2236,explorer.exe'	'164,taskmgr.exe'
397	'2236,explorer.exe'	'3548,ftp.exe'
398	'2236,explorer.exe'	'4092,cmd.exe'
399	'2236,explorer.exe'	'2904,swriter.exe'
400	'2236,explorer.exe'	'664,soffice.exe'
401	'2328,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
402	'2340,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
403	'2412,XXX'	'2456,svchost.exe'
404	'2456,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
405	'2364,XXX'	'2480,jusched.exe'
406	'2480,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
407	'2844,SearchIndexer.exe'	'1084,SearchProtocolHost.exe'

408	'2844,SearchIndexer.exe'	'1260,SearchFilterHost.exe'
409	'2192,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
410	'1928,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
411	'2300,XXX'	'2448,bash.exe'
412	'2448,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
413	'2932,XXX'	'2000,driver_endpoint_netconn.exe'
414	'2000,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
415	'2580,taskmgr.exe'	'580,taskmgr.exe'
416	'2580,taskmgr.exe'	'MPR.dll,C:Windowssystem32MPR.dll'
417	'164,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
418	'164,taskmgr.exe'	'776,taskmgr.exe'
419	'3292,dllhost.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
420	'3532,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
421	'3548,ftp.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
422	'3572,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
423	'3728,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
424	'3988,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
425	'4056,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
426	'4092,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
427	'2920,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
428	'1084,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
429	'2904,swriter.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
430	'2904,swriter.exe'	'3020,soffice.exe'
431	'3020,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
432	'3020,soffice.exe'	'2576,soffice.bin'
433	'2576,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
434	'664,soffice.exe'	'1616,soffice.bin'

7.2.9 Carperb Malware – Instance 1

Table 111: Carperb Malware Instance 1 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,svchost.exe'
6	'360,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'412,XXX'
9	'424,csrss.exe'
10	'400,wininit.exe'
11	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'508,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'524,lsm.exe'
17	'516,lsass.exe'
18	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
19	'wkscli.dll,C:Windowssystem32wkscli.dll'
20	'624,svchost.exe'
21	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
22	'688,VBoxService.exe'
23	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
24	'752,svchost.exe'
25	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
26	'848,svchost.exe'
27	'netutils.dll,C:WindowsSystem32netutils.dll'
28	'winrnr.dll,C:WindowsSystem32winrnr.dll'
29	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
30	'896,svchost.exe'
31	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
32	'936,svchost.exe'
33	'AVRT.dll,c:windowssystem32AVRT.dll'
34	'rasman.dll,C:Windowssystem32rasman.dll'
35	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'

36	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
37	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
38	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
39	'320,svchost.exe'
40	'SensApi.dll,C:Windowssystem32SensApi.dll'
41	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
42	'1156,spoolsv.exe'
43	'1204,svchost.exe'
44	'1360,svchost.exe'
45	'SXS.DLL,C:Windowssystem32SXS.DLL'
46	'1408,FoxitConnectedPDFService.exe'
47	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
48	'1936,svchost.exe'
49	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
50	'1496,sppsvc.exe'
51	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
52	'1248,svchost.exe'
53	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
54	'1468,SearchIndexer.exe'
55	'NLSLexicons002a.dll,C:WindowsSystem32NLSLexicons002a.dll'
56	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
57	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
58	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
59	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
60	'1520,taskhost.exe'
61	'midimap.dll,C:Windowssystem32midimap.dll'
62	'2188,dwm.exe'
63	'2176,XXX'
64	'2208,explorer.exe'
65	'eappcfg.dll,C:Windowssystem32eappcfg.dll'
66	thumbcache.dll,C:Windowssystem32humbcache.dll'
67	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
68	tquery.dll,C:Windowssystem32query.dll'
69	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
70	'docprop.dll,C:Windowssystem32docprop.dll'
71	'sxproxy.dll,C:Windowssystem32sxproxy.dll'
72	'DfsShlEx.dll,C:Windowssystem32DfsShlEx.dll'
73	'shacct.dll,C:WindowsSystem32shacct.dll'
74	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
75	'dxgi.dll,C:Windowssystem32dxgi.dll'
76	'fdWNet.dll,C:Windowssystem32fdWNet.dll'

77	'icm32.dll,C:Windowssystem32icm32.dll'
78	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
79	'wab32res.dll,C:Program FilesCommon FilesSystemwab32res.dll'
80	'2296,VBoxTray.exe'
81	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
82	'2304,MySQLNotifier.exe'
83	'2320,XXX'
84	'2436,jusched.exe'
85	'2620,WmiPrvSE.exe'
86	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
87	'2984,wmpnetwk.exe'
88	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
89	'provsvc.dll,C:WindowsSystem32provsvc.dll'
90	'2920,mintty.exe'
91	'apphelp.dll,C:Windowssystem32apphelp.dll'
92	'1424,conhost.exe'
93	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
94	'2084,XXX'
95	'960,bash.exe'
96	'authz.dll,C:Windowssystem32authz.dll'
97	'1216,XXX'
98	'2536,taskmgr.exe'
99	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
100	'2860,audiodg.exe'
101	'DUser.dll,C:Windowssystem32DUser.dll'
102	'2864,XXX'
103	'2600,driver_endpoint_netconn.exe'
104	'1244,audiodg.exe'
105	'3452,taskhost.exe'
106	'1228,cmd.exe'
107	'3344,conhost.exe'
108	'3720,java.exe'
109	'696,firefox.exe'
110	'1868,firefox.exe'
111	'4060,cmd.exe'
112	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
113	'2804,conhost.exe'
114	'1956,NETSTAT.EXE'
115	'4056,notepad++.exe'
116	'4120,Wireshark.exe'
117	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'

118	'4260,dumpcap.exe'
119	'4268,conhost.exe'
120	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
121	'4708,FoxitReader.exe'
122	'4736,FoxitReaderUpdater.exe'
123	'4944,SearchProtocolHost.exe'
124	'4976,SearchFilterHost.exe'
125	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
126	'4644,mintty.exe'
127	'4696,conhost.exe'
128	'4748,XXX'
129	'5020,bash.exe'
130	'4676,simpress.exe'
131	'4444,soffice.exe'
132	'4328,soffice.bin'
133	'5892,java.exe'
134	'5904,conhost.exe'
135	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
136	'5288,plugin-container.exe'
137	'5340,FlashPlayerPlugin_22_0_0_209.exe'
138	'5368,FlashPlayerPlugin_22_0_0_209.exe'
139	'5124,SearchProtocolHost.exe'
140	'profapi.dll,C:Windowssystem32profapi.dll'
141	'2940,SearchFilterHost.exe'
142	'5660,conhost.exe'
143	'5664,dumpcap.exe'
144	'6024,dllhost.exe'
145	'6264,dllhost.exe'
146	'6320,consent.exe'
147	'6424,dllhost.exe'
148	'IDStore.dll,C:WindowsSystem32IDStore.dll'
149	'6464,dllhost.exe'
150	'6500,AAA.exe'
151	'6508,svchost.exe'
152	'6516,svchost.exe'
153	'6744,svchost.exe'
154	'7100,audiodg.exe'
155	'8444,firefox.exe'
156	'10504,pingsender.exe'
157	'10712,conhost.exe'
158	'11016,audiodg.exe'

159	'13752,audiodg.exe'
160	'7248,dllhost.exe'
161	'7600,dllhost.exe'
162	'7904,dllhost.exe'
163	'7180,dllhost.exe'
164	'8176,dllhost.exe'
165	'7568,dllhost.exe'
166	'7764,dllhost.exe'
167	'8208,SearchProtocolHost.exe'
168	'slc.dll,C:Windowssystem32slc.dll'
169	'8228,SearchFilterHost.exe'
170	'8612,firefox.exe'
171	'8328,dllhost.exe'
172	'1736,dllhost.exe'
173	'9120,slui.exe'
174	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
175	'8848,dllhost.exe'
176	'9236,dllhost.exe'
177	'9284,dllhost.exe'
178	'9528,dllhost.exe'
179	'9580,dllhost.exe'
180	'10044,dllhost.exe'
181	'9320,dllhost.exe'
182	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
183	'9424,SearchProtocolHost.exe'
184	'9436,SearchFilterHost.exe'
185	'shell32.dll,C:Windowssystem32shell32.dll'
186	'9772,dllhost.exe'
187	'9916,mspaint.exe'
188	'oleacc.dll,C:Windowssystem32oleacc.dll'
189	'SAMLIB.dll,C:Windowssystem32SAMLIB.dll'
190	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
191	'9952,svchost.exe'
192	'10528,dllhost.exe'
193	'msxml6.dll,C:WindowsSystem32msxml6.dll'
194	'10768,SearchProtocolHost.exe'
195	'10788,SearchFilterHost.exe'
196	'10868,dllhost.exe'
197	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
198	'11080,firefox.exe'
199	'11292,firefox.exe'

200	'11832,soffice.exe'
201	'11844,soffice.bin'
202	'12168,dllhost.exe'
203	'11668,notepad.exe'
204	'12000,notepad.exe'
205	'11636,dllhost.exe'
206	'12460,dllhost.exe'
207	'12760,dllhost.exe'
208	'12500,dllhost.exe'
209	'12620,SearchProtocolHost.exe'
210	'12648,SearchFilterHost.exe'
211	'12664,splwow64.exe'
212	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
213	'12824,dllhost.exe'
214	'13088,dllhost.exe'
215	'13380,WmiPrvSE.exe'
216	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
217	'13704,dllhost.exe'
218	'13992,dllhost.exe'
219	'13580,dllhost.exe'
220	'13880,dllhost.exe'
221	'14240,dllhost.exe'
222	'13796,mstsc.exe'
223	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
224	'14668,taskhost.exe'
225	'15040,soffice.exe'
226	'15048,soffice.bin'
227	'15164,taskmgr.exe'
228	'15256,dllhost.exe'
229	'15304,dllhost.exe'
230	'15336,taskmgr.exe'
231	'15588,audiodg.exe'
232	'15904,dllhost.exe'
233	'16016,conhost.exe'
234	'16032,cmd.exe'
235	'16140,java.exe'
236	'15836,firefox.exe'
237	'16088,firefox.exe'
238	'17096,cmd.exe'
239	'17104,conhost.exe'
240	'17124,NETSTAT.EXE'

241	'17188,notepad++.exe'
242	'16820,FoxitReader.exe'
243	'17420,mintty.exe'
244	'17456,conhost.exe'
245	'17472,XXX'
246	'17488,bash.exe'
247	'18128,simpress.exe'
248	'18140,soffice.exe'
249	'18148,soffice.bin'
250	'18260,svchost.exe'

Table 112: Carperb Malware Instance 1 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'352,svchost.exe'	'360,csrss.exe'
5	'352,svchost.exe'	'400,wininit.exe'
6	'352,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
7	'352,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
8	'352,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
9	'360,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
10	'412,XXX'	'424,csrss.exe'
11	'412,XXX'	'460,winlogon.exe'
12	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
13	'424,csrss.exe'	'1424,conhost.exe'
14	'424,csrss.exe'	'3344,conhost.exe'
15	'424,csrss.exe'	'2804,conhost.exe'
16	'424,csrss.exe'	'4268,conhost.exe'
17	'424,csrss.exe'	'4696,conhost.exe'
18	'424,csrss.exe'	'5904,conhost.exe'
19	'424,csrss.exe'	'5660,conhost.exe'
20	'424,csrss.exe'	'10712,conhost.exe'
21	'424,csrss.exe'	'16016,conhost.exe'
22	'424,csrss.exe'	'17104,conhost.exe'
23	'424,csrss.exe'	'17456,conhost.exe'
24	'400,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
25	'400,wininit.exe'	'508,services.exe'
26	'400,wininit.exe'	'524,lsm.exe'
27	'400,wininit.exe'	'516,lsass.exe'
28	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
29	'508,services.exe'	'352,svchost.exe'
30	'508,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
31	'508,services.exe'	'624,svchost.exe'
32	'508,services.exe'	'688,VBoxService.exe'
33	'508,services.exe'	'752,svchost.exe'
34	'508,services.exe'	'848,svchost.exe'
35	'508,services.exe'	'896,svchost.exe'
36	'508,services.exe'	'936,svchost.exe'

37	'508,services.exe'	'320,svchost.exe'
38	'508,services.exe'	'1156,spoolsv.exe'
39	'508,services.exe'	'1204,svchost.exe'
40	'508,services.exe'	'1360,svchost.exe'
41	'508,services.exe'	'1408,FoxitConnectedPDFService.exe'
42	'508,services.exe'	'1936,svchost.exe'
43	'508,services.exe'	'1496,sppsvc.exe'
44	'508,services.exe'	'1248,svchost.exe'
45	'508,services.exe'	'1468,SearchIndexer.exe'
46	'508,services.exe'	'1520,taskhost.exe'
47	'508,services.exe'	'2984,wmpnetwk.exe'
48	'508,services.exe'	'3452,taskhost.exe'
49	'508,services.exe'	'6744,svchost.exe'
50	'508,services.exe'	'9952,svchost.exe'
51	'508,services.exe'	'14668,taskhost.exe'
52	'508,services.exe'	'18260,svchost.exe'
53	'524,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
54	'516,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
55	'516,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
56	'624,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
57	'624,svchost.exe'	'2620,WmiPrvSE.exe'
58	'624,svchost.exe'	'6024,dllhost.exe'
59	'624,svchost.exe'	'6264,dllhost.exe'
60	'624,svchost.exe'	'6424,dllhost.exe'
61	'624,svchost.exe'	'6464,dllhost.exe'
62	'624,svchost.exe'	'7248,dllhost.exe'
63	'624,svchost.exe'	'7600,dllhost.exe'
64	'624,svchost.exe'	'7904,dllhost.exe'
65	'624,svchost.exe'	'7180,dllhost.exe'
66	'624,svchost.exe'	'8176,dllhost.exe'
67	'624,svchost.exe'	'7568,dllhost.exe'
68	'624,svchost.exe'	'7764,dllhost.exe'
69	'624,svchost.exe'	'8328,dllhost.exe'
70	'624,svchost.exe'	'1736,dllhost.exe'
71	'624,svchost.exe'	'9120,slui.exe'
72	'624,svchost.exe'	'8848,dllhost.exe'
73	'624,svchost.exe'	'9236,dllhost.exe'
74	'624,svchost.exe'	'9284,dllhost.exe'
75	'624,svchost.exe'	'9528,dllhost.exe'
76	'624,svchost.exe'	'9580,dllhost.exe'
77	'624,svchost.exe'	'10044,dllhost.exe'

78	'624,svchost.exe'	'9320,dllhost.exe'
79	'624,svchost.exe'	'9772,dllhost.exe'
80	'624,svchost.exe'	'10528,dllhost.exe'
81	'624,svchost.exe'	'10868,dllhost.exe'
82	'624,svchost.exe'	'12168,dllhost.exe'
83	'624,svchost.exe'	'11636,dllhost.exe'
84	'624,svchost.exe'	'12460,dllhost.exe'
85	'624,svchost.exe'	'12760,dllhost.exe'
86	'624,svchost.exe'	'12500,dllhost.exe'
87	'624,svchost.exe'	'12824,dllhost.exe'
88	'624,svchost.exe'	'13088,dllhost.exe'
89	'624,svchost.exe'	'13380,WmiPrvSE.exe'
90	'624,svchost.exe'	'13704,dllhost.exe'
91	'624,svchost.exe'	'13992,dllhost.exe'
92	'624,svchost.exe'	'13580,dllhost.exe'
93	'624,svchost.exe'	'13880,dllhost.exe'
94	'624,svchost.exe'	'14240,dllhost.exe'
95	'624,svchost.exe'	'15256,dllhost.exe'
96	'624,svchost.exe'	'15304,dllhost.exe'
97	'624,svchost.exe'	'15904,dllhost.exe'
98	'688,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
99	'752,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
100	'848,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
101	'848,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
102	'848,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
103	'848,svchost.exe'	'2860,audiodg.exe'
104	'848,svchost.exe'	'1244,audiodg.exe'
105	'848,svchost.exe'	'7100,audiodg.exe'
106	'848,svchost.exe'	'11016,audiodg.exe'
107	'848,svchost.exe'	'13752,audiodg.exe'
108	'848,svchost.exe'	'15588,audiodg.exe'
109	'896,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
110	'896,svchost.exe'	'2188,dwm.exe'
111	'936,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
112	'936,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
113	'936,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
114	'936,svchost.exe'	'6320,consent.exe'
115	'320,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
116	'320,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
117	'1156,spoolsv.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
118	'1204,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'

119	'1360,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
120	'1408,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
121	'1936,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
122	'1496,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
123	'1248,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
124	'1468,SearchIndexer.exe'	'NLSLexicons002a.dll,C:WindowsSystem32NLSLexicons002a.dll'
125	'1468,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
126	'1468,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
127	'1468,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
128	'1468,SearchIndexer.exe'	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
129	'1468,SearchIndexer.exe'	'4944,SearchProtocolHost.exe'
130	'1468,SearchIndexer.exe'	'4976,SearchFilterHost.exe'
131	'1468,SearchIndexer.exe'	'5124,SearchProtocolHost.exe'
132	'1468,SearchIndexer.exe'	'2940,SearchFilterHost.exe'
133	'1468,SearchIndexer.exe'	'8208,SearchProtocolHost.exe'
134	'1468,SearchIndexer.exe'	'8228,SearchFilterHost.exe'
135	'1468,SearchIndexer.exe'	'9424,SearchProtocolHost.exe'
136	'1468,SearchIndexer.exe'	'9436,SearchFilterHost.exe'
137	'1468,SearchIndexer.exe'	'10768,SearchProtocolHost.exe'
138	'1468,SearchIndexer.exe'	'10788,SearchFilterHost.exe'
139	'1468,SearchIndexer.exe'	'12620,SearchProtocolHost.exe'
140	'1468,SearchIndexer.exe'	'12648,SearchFilterHost.exe'
141	'1520,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
142	'2188,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
143	'2176,XXX'	'2208,explorer.exe'
144	'2208,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
145	'2208,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
146	'2208,explorer.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
147	'2208,explorer.exe'	'eappcfg.dll,C:Windowssystem32eappcfg.dll'
148	'2208,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
149	'2208,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
150	'2208,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
151	'2208,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
152	'2208,explorer.exe'	'docprop.dll,C:Windowssystem32docprop.dll'
153	'2208,explorer.exe'	'sxproxy.dll,C:Windowssystem32sxproxy.dll'
154	'2208,explorer.exe'	'DfsShlEx.dll,C:Windowssystem32DfsShlEx.dll'
155	'2208,explorer.exe'	'shacct.dll,C:WindowsSystem32shacct.dll'
156	'2208,explorer.exe'	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
157	'2208,explorer.exe'	'dxgi.dll,C:Windowssystem32dxgi.dll'
158	'2208,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
159	'2208,explorer.exe'	'icm32.dll,C:Windowssystem32icm32.dll'

160	'2208,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
161	'2208,explorer.exe'	'wab32res.dll,C:Program FilesCommon FilesSystemwab32res.dll'
162	'2208,explorer.exe'	'2296,VBoxTray.exe'
163	'2208,explorer.exe'	'2304,MySQLNotifier.exe'
164	'2208,explorer.exe'	'2920,mintty.exe'
165	'2208,explorer.exe'	'1228,cmd.exe'
166	'2208,explorer.exe'	'696,firefox.exe'
167	'2208,explorer.exe'	'4060,cmd.exe'
168	'2208,explorer.exe'	'4056,notepad++.exe'
169	'2208,explorer.exe'	'4120,Wireshark.exe'
170	'2208,explorer.exe'	'4708,FoxitReader.exe'
171	'2208,explorer.exe'	'4644,mintty.exe'
172	'2208,explorer.exe'	'6500,AAA.exe'
173	'2208,explorer.exe'	'8444,firefox.exe'
174	'2208,explorer.exe'	'9916,mspaint.exe'
175	'2208,explorer.exe'	'11080,firefox.exe'
176	'2208,explorer.exe'	'11832,soffice.exe'
177	'2208,explorer.exe'	'11668,notepad.exe'
178	'2208,explorer.exe'	'12000,notepad.exe'
179	'2208,explorer.exe'	'13796,mstsc.exe'
180	'2208,explorer.exe'	'15040,soffice.exe'
181	'2208,explorer.exe'	'15164,taskmgr.exe'
182	'2208,explorer.exe'	'16032,cmd.exe'
183	'2208,explorer.exe'	'15836,firefox.exe'
184	'2208,explorer.exe'	'17096,cmd.exe'
185	'2208,explorer.exe'	'17188,notepad++.exe'
186	'2208,explorer.exe'	'16820,FoxitReader.exe'
187	'2208,explorer.exe'	'17420,mintty.exe'
188	'2296,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
189	'2304,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
190	'2320,XXX'	'2436,jusched.exe'
191	'2436,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
192	'2620,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
193	'2984,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
194	'2984,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
195	'2920,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
196	'1424,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
197	'2084,XXX'	'960,bash.exe'
198	'960,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
199	'1216,XXX'	'2536,taskmgr.exe'
200	'2536,taskmgr.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'

201	'2536,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
202	'2536,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
203	'2864,XXX'	'2600,driver_endpoint_netconn.exe'
204	'2600,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
205	'3452,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
206	'1228,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
207	'1228,cmd.exe'	'3720,java.exe'
208	'3344,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
209	'3720,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
210	'3720,java.exe'	'5892,java.exe'
211	'696,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
212	'696,firefox.exe'	'1868,firefox.exe'
213	'696,firefox.exe'	'4676,simpress.exe'
214	'696,firefox.exe'	'5288,plugin-container.exe'
215	'1868,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
216	'4060,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
217	'4060,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
218	'4060,cmd.exe'	'1956,NETSTAT.EXE'
219	'2804,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
220	'1956,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
221	'1956,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
222	'4056,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
223	'4120,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
224	'4120,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
225	'4120,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
226	'4120,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
227	'4120,Wireshark.exe'	'4260,dumpcap.exe'
228	'4120,Wireshark.exe'	'5664,dumpcap.exe'
229	'4260,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
230	'4268,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
231	'4708,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
232	'4708,FoxitReader.exe'	'4736,FoxitReaderUpdater.exe'
233	'4736,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
234	'4944,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
235	'4976,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
236	'4644,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
237	'4696,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
238	'4748,XXX'	'5020,bash.exe'
239	'5020,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
240	'4676,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
241	'4676,simpress.exe'	'4444,soffice.exe'

242	'4444,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
243	'4444,soffice.exe'	'4328,soffice.bin'
244	'4328,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
245	'5892,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
246	'5904,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
247	'5288,plugin-container.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
248	'5288,plugin-container.exe'	'5340,FlashPlayerPlugin_22_0_0_209.exe'
249	'5340,FlashPlayerPlugin_22_0_0_209.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
250	'5340,FlashPlayerPlugin_22_0_0_209.exe'	'5368,FlashPlayerPlugin_22_0_0_209.exe'
251	'5368,FlashPlayerPlugin_22_0_0_209.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
252	'5124,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
253	'2940,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
254	'5660,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
255	'5664,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
256	'6024,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
257	'6264,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
258	'6320,consent.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
259	'6424,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
260	'6464,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
261	'6500,AAA.exe'	'6508,svchost.exe'
262	'6500,AAA.exe'	'6516,svchost.exe'
263	'6508,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
264	'6516,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
265	'6744,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
266	'8444,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
267	'8444,firefox.exe'	'10504,pingsender.exe'
268	'8444,firefox.exe'	'8612,firefox.exe'
269	'7248,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
270	'7600,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
271	'7904,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
272	'7180,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
273	'8176,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
274	'7568,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
275	'7764,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
276	'8208,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
277	'8228,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
278	'8612,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
279	'8328,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
280	'1736,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
281	'9120,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'

282	'8848,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
283	'9236,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
284	'9284,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
285	'9528,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
286	'9580,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
287	'10044,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
288	'9320,dllhost.exe'	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
289	'9424,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
290	'9436,SearchFilterHost.exe'	'shell32.dll,C:Windowssystem32shell32.dll'
291	'9772,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
292	'9916,mspaint.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
293	'9916,mspaint.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
294	'9916,mspaint.exe'	'SAMLIB.dll,C:Windowssystem32SAMLIB.dll'
295	'9916,mspaint.exe'	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
296	'9952,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
297	'10528,dllhost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
298	'10768,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
299	'10788,SearchFilterHost.exe'	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
300	'10868,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
301	'11080,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
302	'11080,firefox.exe'	'11292,firefox.exe'
303	'11292,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
304	'11832,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
305	'11832,soffice.exe'	'11844,soffice.bin'
306	'11844,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
307	'11844,soffice.bin'	'12664,splwow64.exe'
308	'12168,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
309	'11668,notepad.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
310	'12000,notepad.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
311	'11636,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
312	'12460,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
313	'12760,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
314	'12500,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
315	'12620,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
316	'12648,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
317	'12664,splwow64.exe'	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
318	'12824,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
319	'13088,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
320	'13380,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
321	'13704,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
322	'13992,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'

323	'13580,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
324	'13880,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
325	'14240,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
326	'13796,mstsc.exe'	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
327	'14668,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
328	'15040,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
329	'15040,soffice.exe'	'15048,soffice.bin'
330	'15048,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
331	'15164,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
332	'15164,taskmgr.exe'	'15336,taskmgr.exe'
333	'15256,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
334	'15304,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
335	'15336,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
336	'15904,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
337	'16016,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
338	'16032,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
339	'16032,cmd.exe'	'16140,java.exe'
340	'16140,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
341	'15836,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
342	'15836,firefox.exe'	'16088,firefox.exe'
343	'15836,firefox.exe'	'18128,simpress.exe'
344	'16088,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
345	'17096,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
346	'17096,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
347	'17096,cmd.exe'	'17124,NETSTAT.EXE'
348	'17104,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
349	'17124,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
350	'17124,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
351	'17188,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
352	'16820,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
353	'17420,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
354	'17456,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
355	'17472,XXX'	'17488,bash.exe'
356	'17488,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
357	'18128,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
358	'18128,simpress.exe'	'18140,soffice.exe'
359	'18140,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
360	'18140,soffice.exe'	'18148,soffice.bin'
361	'18148,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
362	'18260,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'

7.2.10 Carperb Malware – Instance 2

Table 113: Carperb Malware Instance 2 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,XXX'
6	'360,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'400,wininit.exe'
9	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
10	'412,XXX'
11	'424,csrss.exe'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'508,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'524,lsm.exe'
17	'516,lsass.exe'
18	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
19	'628,svchost.exe'
20	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
21	'692,VBoxService.exe'
22	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
23	'756,svchost.exe'
24	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
25	'848,svchost.exe'
26	'netutils.dll,C:WindowsSystem32netutils.dll'
27	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
28	'896,svchost.exe'
29	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
30	'HID.DLL,C:WindowsSystem32HID.DLL'
31	'1008,audiodg.exe'
32	'936,svchost.exe'
33	'appinfo.dll,c:windowssystem32appinfo.dll'
34	'AVRT.dll,c:windowssystem32AVRT.dll'
35	tschannel.dll,C:Windowssystem32schannel.dll'

36	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
37	'364,svchost.exe'
38	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
39	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
40	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
41	'828,svchost.exe'
42	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
43	'1152,spoolsv.exe'
44	'1200,svchost.exe'
45	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
46	'1352,svchost.exe'
47	'SXS.DLL,C:Windowssystem32SXS.DLL'
48	'1412,FoxitConnectedPDFService.exe'
49	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
50	'1904,svchost.exe'
51	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
52	'976,sppsvc.exe'
53	'1652,svchost.exe'
54	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
55	'1648,SearchIndexer.exe'
56	'NLSLexicons002a.dll,C:WindowsSystem32NLSLexicons002a.dll'
57	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
58	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
59	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
60	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
61	'ktmw32.dll,C:Windowssystem32ktmw32.dll'
62	'1664,WmiPrvSE.exe'
63	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
64	'2348,dwm.exe'
65	'2340,XXX'
66	'2368,explorer.exe'
67	tquery.dll,C:Windowssystem32query.dll'
68	'thumbcache.dll,C:Windowssystem32humbcache.dll'
69	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
70	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
71	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
72	'zipfldr.dll,C:Windowssystem32zipfldr.dll'

73	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
74	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
75	'DfsShlEx.dll,C:Windowssystem32DfsShlEx.dll'
76	'LOGONCLI.DLL,C:Windowssystem32LOGONCLI.DLL'
77	'dxgi.dll,C:Windowssystem32dxgi.dll'
78	'sensapi.dll,C:Windowssystem32sensapi.dll'
79	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
80	'2084,taskhost.exe'
81	'midimap.dll,C:Windowssystem32midimap.dll'
82	'2448,VBoxTray.exe'
83	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
84	'2456,MySQLNotifier.exe'
85	'2472,XXX'
86	'2764,jusched.exe'
87	'1020,wmpnetwk.exe'
88	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
89	'provsvc.dll,C:WindowsSystem32provsvc.dll'
90	'2688,XXX'
91	'2068,taskmgr.exe'
92	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
93	'2724,mintty.exe'
94	'apphelp.dll,C:Windowssystem32apphelp.dll'
95	'2580,conhost.exe'
96	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
97	'2912,XXX'
98	'3720,bash.exe'
99	'authz.dll,C:Windowssystem32authz.dll'
100	'2056,XXX'
101	'212,driver_endpoint_netconn.exe'
102	'304,audiodg.exe'
103	'2080,cmd.exe'
104	'3196,java.exe'
105	'3272,conhost.exe'
106	'2468,java.exe'
107	'3904,firefox.exe'
108	'2924,firefox.exe'
109	'2652,cmd.exe'
110	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
111	'1112,conhost.exe'
112	'3556,NETSTAT.EXE'
113	'winrnr.dll,C:WindowsSystem32winrnr.dll'

114	'3256,notepad++.exe'
115	'4008,Wireshark.exe'
116	'4152,gspawn-win64-helper.exe'
117	'4164,androiddump.exe'
118	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
119	'4232,dumpcap.exe'
120	'4240,conhost.exe'
121	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
122	'4644,FoxitReader.exe'
123	'4680,FoxitReaderUpdater.exe'
124	'4964,SearchProtocolHost.exe'
125	'4992,SearchFilterHost.exe'
126	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
127	'4464,mintty.exe'
128	'4540,conhost.exe'
129	'4580,XXX'
130	'4576,bash.exe'
131	'4872,simpress.exe'
132	'4888,soffice.exe'
133	'4612,soffice.bin'
134	'5540,firefox.exe'
135	'5924,java.exe'
136	'5928,conhost.exe'
137	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
138	'5520,dumpcap.exe'
139	'5524,conhost.exe'
140	'5936,dllhost.exe'
141	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
142	'5648,dllhost.exe'
143	'5460,SearchProtocolHost.exe'
144	'VERSION.dll,C:Windowssystem32VERSION.dll'
145	'5052,SearchFilterHost.exe'
146	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
147	'6268,consent.exe'
148	'6340,dllhost.exe'
149	'IDStore.dll,C:WindowsSystem32IDStore.dll'
150	'6376,dllhost.exe'
151	'6408,AAA.exe'
152	'6420,svchost.exe'
153	'6428,svchost.exe'
154	'6436,explorer.exe'

155	'8968,audiodg.exe'
156	'13124,audiodg.exe'
157	'7144,dllhost.exe'
158	'5372,SearchProtocolHost.exe'
159	'profapi.dll,C:Windowssystem32profapi.dll'
160	'6712,SearchFilterHost.exe'
161	'6916,svchost.exe'
162	'7204,FoxitReader.exe'
163	'7368,SearchProtocolHost.exe'
164	'7388,SearchFilterHost.exe'
165	'7472,taskmgr.exe'
166	'7668,soffice.exe'
167	'7676,soffice.bin'
168	'7980,taskeng.exe'
169	'8020,MySQLInstallerConsole.exe'
170	'System.Configuration.ni.dll,C:WindowsassemblyNativeImages_v4.0.30319_64System.Configuration11581b5eba4b3ff58441c638ab66c742System.Configuration.ni.dll'
171	'8028,conhost.exe'
172	'msi.dll,C:Windowssystem32msi.dll'
173	'8068,csc.exe'
174	'8076,cvtres.exe'
175	'8216,mspaint.exe'
176	'oleacc.dll,C:Windowssystem32oleacc.dll'
177	'DUser.dll,C:Windowssystem32DUser.dll'
178	'8252,svchost.exe'
179	'8716,notepad.exe'
180	'8212,dllhost.exe'
181	'9116,dllhost.exe'
182	'9040,dllhost.exe'
183	'9184,dllhost.exe'
184	'9584,taskhost.exe'
185	'9644,notepad++.exe'
186	'10020,slui.exe'
187	'9392,calc.exe'
188	'9412,WinRAR.exe'
189	'msimg32.dll,C:Windowssystem32msimg32.dll'
190	'9096,SearchProtocolHost.exe'
191	'9704,SearchFilterHost.exe'
192	'10900,soffice.exe'
193	'10908,soffice.bin'
194	'11032,firefox.exe'

195	'11212,firefox.exe'
196	'11492,audiodg.exe'
197	'12004,WmiPrvSE.exe'
198	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
199	'12388,Wireshark.exe'
200	'12448,gspawn-win64-helper.exe'
201	'12460,androiddump.exe'
202	'msimtf.dll,C:Windowssystem32msimtf.dll'
203	'12524,dumpcap.exe'
204	'12532,conhost.exe'
205	'12908,dumpcap.exe'
206	'12916,conhost.exe'
207	'11028,cmd.exe'
208	'12356,conhost.exe'
209	'12448,java.exe'
210	'12672,firefox.exe'
211	'12864,firefox.exe'
212	'13720,cmd.exe'
213	'13728,conhost.exe'
214	'13744,NETSTAT.EXE'
215	'13808,notepad++.exe'
216	'13848,Wireshark.exe'
217	'13988,dumpcap.exe'
218	'13996,conhost.exe'
219	'14052,FoxitReader.exe'
220	'14164,mintty.exe'
221	'14328,conhost.exe'
222	'13452,XXX'
223	'13448,bash.exe'
224	'15004,simpress.exe'
225	'15012,soffice.exe'
226	'15020,soffice.bin'
227	'14324,SearchProtocolHost.exe'
228	'14788,SearchFilterHost.exe'
229	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
230	'15076,WinRAR.exe'
231	'imagehlp.dll,C:Windowssystem32imagehlp.dll'
232	'15436,mspaint.exe'
233	'16064,audiodg.exe'
234	'15464,svchost.exe'
235	'15588,StikyNot.exe'

236	'15644,SearchProtocolHost.exe'
237	'15972,mstsc.exe'
238	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
239	'16356,XXX'
240	'16364,javaw.exe'
241	'15636,jucheck.exe'
242	'15632,XXX'
243	'15596,jp2launcher.exe'
244	'16284,SnippingTool.exe'
245	'16324,wisptis.exe'
246	tpcps.dll,C:Program FilesCommon FilesMicrosoft SharedInkpcps.dll'
247	'15884,xpsrchvw.exe'
248	'15564,java.exe'
249	'15556,conhost.exe'
250	'15888,SearchProtocolHost.exe'
251	'16168,SearchFilterHost.exe'
252	'17084,dumpcap.exe'
253	'17092,conhost.exe'
254	'17164,firefox.exe'
255	'17396,firefox.exe'
256	'17512,taskmgr.exe'
257	'17752,taskmgr.exe'
258	'17848,dllhost.exe'
259	'17892,dllhost.exe'
260	'17924,taskmgr.exe'

Table 114: Carperb Malware Instance 2 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'352,XXX'	'360,csrss.exe'
5	'352,XXX'	'400,wininit.exe'
6	'360,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'400,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
8	'400,wininit.exe'	'508,services.exe'
9	'400,wininit.exe'	'524,lsm.exe'
10	'400,wininit.exe'	'516,lsass.exe'
11	'412,XXX'	'424,csrss.exe'
12	'412,XXX'	'460,winlogon.exe'
13	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
14	'424,csrss.exe'	'2580,conhost.exe'
15	'424,csrss.exe'	'3272,conhost.exe'
16	'424,csrss.exe'	'1112,conhost.exe'
17	'424,csrss.exe'	'4240,conhost.exe'
18	'424,csrss.exe'	'4540,conhost.exe'
19	'424,csrss.exe'	'5928,conhost.exe'
20	'424,csrss.exe'	'5524,conhost.exe'
21	'424,csrss.exe'	'8028,conhost.exe'
22	'424,csrss.exe'	'12532,conhost.exe'
23	'424,csrss.exe'	'12916,conhost.exe'
24	'424,csrss.exe'	'12356,conhost.exe'
25	'424,csrss.exe'	'13728,conhost.exe'
26	'424,csrss.exe'	'13996,conhost.exe'
27	'424,csrss.exe'	'14328,conhost.exe'
28	'424,csrss.exe'	'15556,conhost.exe'
29	'424,csrss.exe'	'17092,conhost.exe'
30	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
31	'508,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
32	'508,services.exe'	'628,svchost.exe'
33	'508,services.exe'	'692,VBoxService.exe'
34	'508,services.exe'	'756,svchost.exe'
35	'508,services.exe'	'848,svchost.exe'
36	'508,services.exe'	'896,svchost.exe'
37	'508,services.exe'	'936,svchost.exe'
38	'508,services.exe'	'364,svchost.exe'

39	'508,services.exe'	'828,svchost.exe'
40	'508,services.exe'	'1152,spoolsv.exe'
41	'508,services.exe'	'1200,svchost.exe'
42	'508,services.exe'	'1352,svchost.exe'
43	'508,services.exe'	'1412,FoxitConnectedPDFService.exe'
44	'508,services.exe'	'1904,svchost.exe'
45	'508,services.exe'	'976,sppsvc.exe'
46	'508,services.exe'	'1652,svchost.exe'
47	'508,services.exe'	'1648,SearchIndexer.exe'
48	'508,services.exe'	'2084,taskhost.exe'
49	'508,services.exe'	'1020,wmpnetwk.exe'
50	'508,services.exe'	'6916,svchost.exe'
51	'508,services.exe'	'8252,svchost.exe'
52	'508,services.exe'	'9584,taskhost.exe'
53	'508,services.exe'	'15464,svchost.exe'
54	'524,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
55	'516,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
56	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
57	'628,svchost.exe'	'1664,WmiPrvSE.exe'
58	'628,svchost.exe'	'5936,dllhost.exe'
59	'628,svchost.exe'	'5648,dllhost.exe'
60	'628,svchost.exe'	'6340,dllhost.exe'
61	'628,svchost.exe'	'6376,dllhost.exe'
62	'628,svchost.exe'	'7144,dllhost.exe'
63	'628,svchost.exe'	'8212,dllhost.exe'
64	'628,svchost.exe'	'9116,dllhost.exe'
65	'628,svchost.exe'	'9040,dllhost.exe'
66	'628,svchost.exe'	'9184,dllhost.exe'
67	'628,svchost.exe'	'10020,slui.exe'
68	'628,svchost.exe'	'12004,WmiPrvSE.exe'
69	'628,svchost.exe'	'17848,dllhost.exe'
70	'628,svchost.exe'	'17892,dllhost.exe'
71	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
72	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
73	'848,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
74	'848,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
75	'848,svchost.exe'	'1008,audiodg.exe'
76	'848,svchost.exe'	'304,audiodg.exe'
77	'848,svchost.exe'	'8968,audiodg.exe'
78	'848,svchost.exe'	'13124,audiodg.exe'
79	'848,svchost.exe'	'11492,audiodg.exe'

80	'848,svchost.exe'	'16064,audiodg.exe'
81	'896,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
82	'896,svchost.exe'	'HID.DLL,C:WindowsSystem32HID.DLL'
83	'896,svchost.exe'	'2348,dwm.exe'
84	'896,svchost.exe'	'16324,wisptis.exe'
85	'936,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
86	'936,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
87	'936,svchost.exe'	tschannel.dll,C:Windowssystem32schannel.dll'
88	'936,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
89	'936,svchost.exe'	'6268,consent.exe'
90	'936,svchost.exe'	'7980,taskeng.exe'
91	'364,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
92	'364,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
93	'364,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
94	'828,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
95	'1152,spoolsv.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
96	'1200,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
97	'1200,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
98	'1352,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
99	'1412,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
100	'1904,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
101	'976,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
102	'1652,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
103	'1648,SearchIndexer.exe'	'NLSLexicons002a.dll,C:WindowsSystem32NLSLexicons002a.dll'
104	'1648,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
105	'1648,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
106	'1648,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
107	'1648,SearchIndexer.exe'	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
108	'1648,SearchIndexer.exe'	'ktmw32.dll,C:Windowssystem32ktmw32.dll'
109	'1648,SearchIndexer.exe'	'4964,SearchProtocolHost.exe'
110	'1648,SearchIndexer.exe'	'4992,SearchFilterHost.exe'
111	'1648,SearchIndexer.exe'	'5460,SearchProtocolHost.exe'
112	'1648,SearchIndexer.exe'	'5052,SearchFilterHost.exe'
113	'1648,SearchIndexer.exe'	'5372,SearchProtocolHost.exe'
114	'1648,SearchIndexer.exe'	'6712,SearchFilterHost.exe'

115	'1648,SearchIndexer.exe'	'7368,SearchProtocolHost.exe'
116	'1648,SearchIndexer.exe'	'7388,SearchFilterHost.exe'
117	'1648,SearchIndexer.exe'	'9096,SearchProtocolHost.exe'
118	'1648,SearchIndexer.exe'	'9704,SearchFilterHost.exe'
119	'1648,SearchIndexer.exe'	'14324,SearchProtocolHost.exe'
120	'1648,SearchIndexer.exe'	'14788,SearchFilterHost.exe'
121	'1648,SearchIndexer.exe'	'15644,SearchProtocolHost.exe'
122	'1648,SearchIndexer.exe'	'15888,SearchProtocolHost.exe'
123	'1648,SearchIndexer.exe'	'16168,SearchFilterHost.exe'
124	'1664,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
125	'2348,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
126	'2340,XXX'	'2368,explorer.exe'
127	'2368,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
128	'2368,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
129	'2368,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
130	'2368,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
131	'2368,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
132	'2368,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
133	'2368,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
134	'2368,explorer.exe'	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
135	'2368,explorer.exe'	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
136	'2368,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
137	'2368,explorer.exe'	'DfsShlEx.dll,C:Windowssystem32DfsShlEx.dll'
138	'2368,explorer.exe'	'LOGONCLI.DLL,C:Windowssystem32LOGONCLI.DLL'
139	'2368,explorer.exe'	'dxgi.dll,C:Windowssystem32dxgi.dll'
140	'2368,explorer.exe'	'sensapi.dll,C:Windowssystem32sensapi.dll'
141	'2368,explorer.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
142	'2368,explorer.exe'	'2448,VBoxTray.exe'
143	'2368,explorer.exe'	'2456,MySQLNotifier.exe'
144	'2368,explorer.exe'	'2724,mintty.exe'
145	'2368,explorer.exe'	'2080,cmd.exe'
146	'2368,explorer.exe'	'3904,firefox.exe'
147	'2368,explorer.exe'	'2652,cmd.exe'
148	'2368,explorer.exe'	'3256,notepad++.exe'
149	'2368,explorer.exe'	'4008,Wireshark.exe'
150	'2368,explorer.exe'	'4644,FoxitReader.exe'
151	'2368,explorer.exe'	'4464,mintty.exe'

152	'2368,explorer.exe'	'5540,firefox.exe'
153	'2368,explorer.exe'	'6408,AAA.exe'
154	'2368,explorer.exe'	'7204,FoxitReader.exe'
155	'2368,explorer.exe'	'7472,taskmgr.exe'
156	'2368,explorer.exe'	'7668,soffice.exe'
157	'2368,explorer.exe'	'8216,mspaint.exe'
158	'2368,explorer.exe'	'8716,notepad.exe'
159	'2368,explorer.exe'	'9644,notepad++.exe'
160	'2368,explorer.exe'	'9392,calc.exe'
161	'2368,explorer.exe'	'9412,WinRAR.exe'
162	'2368,explorer.exe'	'10900,soffice.exe'
163	'2368,explorer.exe'	'11032,firefox.exe'
164	'2368,explorer.exe'	'12388,Wireshark.exe'
165	'2368,explorer.exe'	'11028,cmd.exe'
166	'2368,explorer.exe'	'12672,firefox.exe'
167	'2368,explorer.exe'	'13720,cmd.exe'
168	'2368,explorer.exe'	'13808,notepad++.exe'
169	'2368,explorer.exe'	'13848,Wireshark.exe'
170	'2368,explorer.exe'	'14052,FoxitReader.exe'
171	'2368,explorer.exe'	'14164,mintty.exe'
172	'2368,explorer.exe'	'15076,WinRAR.exe'
173	'2368,explorer.exe'	'15436,mspaint.exe'
174	'2368,explorer.exe'	'15588,StikyNot.exe'
175	'2368,explorer.exe'	'15972,mstsc.exe'
176	'2368,explorer.exe'	'16284,SnippingTool.exe'
177	'2368,explorer.exe'	'15884,xpsrchvw.exe'
178	'2368,explorer.exe'	'17164,firefox.exe'
179	'2368,explorer.exe'	'17512,taskmgr.exe'
180	'2368,explorer.exe'	'17752,taskmgr.exe'
181	'2084,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
182	'2448,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
183	'2456,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
184	'2472,XXX'	'2764,jusched.exe'
185	'2764,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
186	'1020,wmpnetwk.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
187	'1020,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
188	'1020,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
189	'2688,XXX'	'2068,taskmgr.exe'
190	'2068,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
191	'2724,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'

192	'2580,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
193	'2912,XXX'	'3720,bash.exe'
194	'3720,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
195	'2056,XXX'	'212,driver_endpoint_netconn.exe'
196	'212,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
197	'2080,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
198	'2080,cmd.exe'	'3196,java.exe'
199	'2080,cmd.exe'	'2468,java.exe'
200	'3272,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
201	'2468,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
202	'2468,java.exe'	'5924,java.exe'
203	'3904,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
204	'3904,firefox.exe'	'2924,firefox.exe'
205	'3904,firefox.exe'	'4872,simpress.exe'
206	'2924,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
207	'2652,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
208	'2652,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
209	'2652,cmd.exe'	'3556,NETSTAT.EXE'
210	'1112,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
211	'3556,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
212	'3556,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
213	'3256,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
214	'4008,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
215	'4008,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
216	'4008,Wireshark.exe'	'4152,gspawn-win64-helper.exe'
217	'4008,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
218	'4008,Wireshark.exe'	'4232,dumpcap.exe'
219	'4008,Wireshark.exe'	'5520,dumpcap.exe'
220	'4152,gspawn-win64-helper.exe'	'4164,androiddump.exe'
221	'4232,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
222	'4240,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
223	'4644,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
224	'4644,FoxitReader.exe'	'4680,FoxitReaderUpdater.exe'
225	'4680,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
226	'4964,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
227	'4992,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
228	'4464,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
229	'4540,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'

230	'4580,XXX'	'4576,bash.exe'
231	'4576,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
232	'4872,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
233	'4872,simpress.exe'	'4888,soffice.exe'
234	'4888,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
235	'4888,soffice.exe'	'4612,soffice.bin'
236	'4612,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
237	'5924,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
238	'5928,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
239	'5520,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
240	'5524,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
241	'5936,dllhost.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
242	'5648,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
243	'5460,SearchProtocolHost.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
244	'5052,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
245	'6268,consent.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
246	'6340,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
247	'6376,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
248	'6408,AAA.exe'	'6420,svchost.exe'
249	'6408,AAA.exe'	'6428,svchost.exe'
250	'6408,AAA.exe'	'6436,explorer.exe'
251	'6420,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
252	'6428,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
253	'7144,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
254	'5372,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
255	'5372,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
256	'6712,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
257	'6712,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
258	'6916,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
259	'7204,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
260	'7368,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
261	'7368,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
262	'7388,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
263	'7388,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
264	'7472,taskmgr.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
265	'7668,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

266	'7668,soffice.exe'	'7676,soffice.bin'
267	'7676,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
268	'7980,taskeng.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
269	'7980,taskeng.exe'	'8020,MySQLInstallerConsole.exe'
270	'8020,MySQLInstallerConsole.exe'	'System.Configuration.ni.dll,C:WindowsassemblyNativeImages_v4.0.30319_64System.Configuration11581b5eba4b3ff58441c638ab66c742System.Configuration.ni.dll'
271	'8020,MySQLInstallerConsole.exe'	'msi.dll,C:Windowssystem32msi.dll'
272	'8020,MySQLInstallerConsole.exe'	'8068,csc.exe'
273	'8028,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
274	'8068,csc.exe'	'8076,cvtres.exe'
275	'8216,mspaint.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
276	'8216,mspaint.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
277	'8252,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
278	'8716,notepad.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
279	'8212,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
280	'9116,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
281	'9040,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
282	'9184,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
283	'9584,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
284	'9644,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
285	'10020,slui.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
286	'9392,calc.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
287	'9412,WinRAR.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
288	'9412,WinRAR.exe'	'msimg32.dll,C:Windowssystem32msimg32.dll'
289	'9096,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
290	'9704,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
291	'10900,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
292	'10900,soffice.exe'	'10908,soffice.bin'
293	'10908,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
294	'11032,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
295	'11032,firefox.exe'	'11212,firefox.exe'
296	'11212,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
297	'12004,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
298	'12388,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
299	'12388,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
300	'12388,Wireshark.exe'	'12448,gspawn-win64-helper.exe'
301	'12388,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'

302	'12388,Wireshark.exe'	'12524,dumpcap.exe'
303	'12388,Wireshark.exe'	'12908,dumpcap.exe'
304	'12448,gspawn-win64-helper.exe'	'12460,androiddump.exe'
305	'12448,gspawn-win64-helper.exe'	'15564,java.exe'
306	'12524,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
307	'12532,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
308	'12908,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
309	'12916,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
310	'11028,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
311	'11028,cmd.exe'	'12448,java.exe'
312	'12356,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
313	'12448,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
314	'12672,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
315	'12672,firefox.exe'	'12864,firefox.exe'
316	'12672,firefox.exe'	'15004,simpress.exe'
317	'12864,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
318	'13720,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
319	'13720,cmd.exe'	'13744,NETSTAT.EXE'
320	'13728,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
321	'13744,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
322	'13744,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
323	'13808,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
324	'13848,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
325	'13848,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
326	'13848,Wireshark.exe'	'13988,dumpcap.exe'
327	'13848,Wireshark.exe'	'17084,dumpcap.exe'
328	'13988,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
329	'13996,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
330	'14052,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
331	'14164,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
332	'14328,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
333	'13452,XXX'	'13448,bash.exe'
334	'13448,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
335	'15004,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
336	'15004,simpress.exe'	'15012,soffice.exe'

337	'15012,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
338	'15012,soffice.exe'	'15020,soffice.bin'
339	'15020,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
340	'14324,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
341	'14324,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
342	'14788,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
343	'14788,SearchFilterHost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
344	'15076,WinRAR.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
345	'15076,WinRAR.exe'	'imagehlp.dll,C:Windowssystem32imagehlp.dll'
346	'15464,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
347	'15644,SearchProtocolHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
348	'15972,mstsc.exe'	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
349	'16356,XXX'	'16364,javaw.exe'
350	'16364,javaw.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
351	'16364,javaw.exe'	'15636,jucheck.exe'
352	'15632,XXX'	'15596,jp2launcher.exe'
353	'15596,jp2launcher.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
354	'16284,SnippingTool.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
355	'16324,wisptis.exe'	tpcps.dll,C:Program FilesCommon FilesMicrosoft SharedInkpcps.dll'
356	'15564,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
357	'15556,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
358	'15888,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
359	'16168,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
360	'17084,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
361	'17092,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
362	'17164,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
363	'17164,firefox.exe'	'17396,firefox.exe'
364	'17396,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
365	'17512,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
366	'17752,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
367	'17752,taskmgr.exe'	'17924,taskmgr.exe'
368	'17848,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
369	'17892,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
370	'17924,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
371	'17924,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'

7.2.11 Alina Malware – Instance 1

Table 115: Alina Malware Instance 1 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'356,XXX'
6	'368,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'408,wininit.exe'
9	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
10	'416,XXX'
11	'428,csrss.exe'
12	'464,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'508,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'532,lsm.exe'
17	'524,lsass.exe'
18	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
19	'wkscli.dll,C:Windowssystem32wkscli.dll'
20	'636,svchost.exe'
21	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
22	'700,VBoxService.exe'
23	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
24	'764,svchost.exe'
25	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
26	'856,svchost.exe'
27	'netutils.dll,C:WindowsSystem32netutils.dll'
28	'winrnr.dll,C:WindowsSystem32winrnr.dll'
29	'1008,audiodg.exe'
30	'900,svchost.exe'
31	'credssp.dll,C:WindowsSystem32credssp.dll'
32	'940,svchost.exe'
33	'wer.dll,C:Windowssystem32wer.dll'
34	'rasman.dll,C:Windowssystem32rasman.dll'
35	'AVRT.dll,c:windowssystem32AVRT.dll'
36	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'

37	'384,svchost.exe'
38	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
39	'vmictimeprovider.dll,C:WindowsSystem32vmictimeprovider.dll'
40	'dsrole.dll,C:Windowssystem32dsrole.dll'
41	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
42	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
43	'1000,svchost.exe'
44	'SensApi.dll,C:Windowssystem32SensApi.dll'
45	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
46	'1156,spoolsv.exe'
47	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
48	'1204,svchost.exe'
49	'1356,svchost.exe'
50	'SXS.DLL,C:Windowssystem32SXS.DLL'
51	'1400,FoxitConnectedPDFService.exe'
52	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
53	'1880,svchost.exe'
54	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
55	'1780,dwm.exe'
56	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
57	'1328,XXX'
58	'1612,explorer.exe'
59	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
60	'thumbcache.dll,C:Windowssystem32humbcache.dll'
61	'sbdrop.dll,C:Program FilesWindows Sidebarsbdrop.dll'
62	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
63	tquery.dll,C:Windowssystem32query.dll'
64	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
65	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
66	'docprop.dll,C:Windowssystem32docprop.dll'
67	'sxproxy.dll,C:Windowssystem32sxproxy.dll'
68	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
69	'dxgi.dll,C:Windowssystem32dxgi.dll'
70	'2056,taskhost.exe'
71	'midimap.dll,C:Windowssystem32midimap.dll'
72	'2156,VBoxTray.exe'
73	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
74	'2176,MySQLNotifier.exe'
75	'2220,dllhost.exe'

76	'2272,jusched.exe'
77	'2428,WmiPrvSE.exe'
78	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
79	'2656,SearchIndexer.exe'
80	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
81	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
82	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
83	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
84	'2724,SearchProtocolHost.exe'
85	'slc.dll,C:Windowssystem32slc.dll'
86	'apphelp.dll,C:Windowssystem32apphelp.dll'
87	'2744,SearchFilterHost.exe'
88	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
89	'2852,wmpnetwk.exe'
90	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
91	'2316,sppsvc.exe'
92	'2268,svchost.exe'
93	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
94	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
95	'332,XXX'
96	'3268,taskmgr.exe'
97	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
98	'1332,mintty.exe'
99	'836,conhost.exe'
100	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
101	'2760,XXX'
102	'2524,bash.exe'
103	'authz.dll,C:Windowssystem32authz.dll'
104	'3672,XXX'
105	'3928,driver_endpoint_netconn.exe'
106	'1640,SearchFilterHost.exe'
107	'3728,SearchProtocolHost.exe'
108	'profapi.dll,C:WindowsSystem32profapi.dll'
109	'1832,WMIADAP.exe'
110	'PSAPI.DLL,C:Windowssystem32PSAPI.DLL'
111	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
112	'1860,WmiPrvSE.exe'
113	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
114	'1444,conhost.exe'
115	'2844,sdclt.exe'
116	'3292,sc.exe'

117	'3588,wsqmcons.exe'
118	'2940,taskhost.exe'
119	'3204,SearchProtocolHost.exe'
120	'3892,SearchFilterHost.exe'
121	'3572,cmd.exe'
122	'1968,conhost.exe'
123	'3700,java.exe'
124	'3520,firefox.exe'
125	'2756,firefox.exe'
126	'4312,cmd.exe'
127	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
128	'4320,conhost.exe'
129	'4348,NETSTAT.EXE'
130	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
131	'4412,notepad++.exe'
132	'4464,Wireshark.exe'
133	'4524,gspawn-win64-helper.exe'
134	'4536,androiddump.exe'
135	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
136	'5828,audiodg.exe'
137	'DUI70.dll,C:Windowssystem32DUI70.dll'
138	'4600,dumpcap.exe'
139	'4608,conhost.exe'
140	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
141	'4324,firefox.exe'
142	'4448,FoxitReader.exe'
143	'4536,FoxitReaderUpdater.exe'
144	'4792,SearchProtocolHost.exe'
145	'4824,SearchFilterHost.exe'
146	'5032,mintty.exe'
147	'5080,conhost.exe'
148	'2612,XXX'
149	'4124,bash.exe'
150	'5192,taskhost.exe'
151	'5676,simpress.exe'
152	'5684,soffice.exe'
153	'5692,soffice.bin'
154	'5424,java.exe'
155	'5416,conhost.exe'
156	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
157	'5980,SearchProtocolHost.exe'

158	'5136,SearchFilterHost.exe'
159	'5944,conhost.exe'
160	'5948,dumpcap.exe'
161	'6156,SearchProtocolHost.exe'
162	'6176,SearchFilterHost.exe'
163	'6484,dllhost.exe'
164	'6616,dllhost.exe'
165	'6660,consent.exe'
166	'6740,dllhost.exe'
167	'IDStore.dll,C:WindowsSystem32IDStore.dll'
168	'6780,dllhost.exe'
169	'6816,3_4.exe'
170	'6880,dwm.exe'
171	'7892,notepad++.exe'
172	'7944,SearchProtocolHost.exe'
173	'7300,SearchFilterHost.exe'
174	'7316,calc.exe'
175	'oleacc.dll,C:Windowssystem32oleacc.dll'
176	'7252,XXX'
177	'7796,driver_endpoint_netconn.exe'
178	'2168,dllhost.exe'
179	'3592,svchost.exe'
180	'3736,dllhost.exe'
181	'3484,dllhost.exe'
182	'4052,dllhost.exe'
183	'3980,dllhost.exe'
184	'4268,dllhost.exe'
185	'4372,dllhost.exe'
186	'3708,dllhost.exe'
187	'5284,consent.exe'
188	'5424,dllhost.exe'
189	'5276,dllhost.exe'
190	'4624,regedit.exe'
191	'5148,dllhost.exe'
192	'6596,firefox.exe'
193	'5180,firefox.exe'
194	'7136,soffice.exe'
195	'6700,soffice.bin'
196	'4724,FoxitReader.exe'
197	'3152,firefox.exe'
198	'3536,firefox.exe'

199	'1888,slui.exe'
200	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
201	'364,csrss.exe'
202	'404,wininit.exe'
203	'512,services.exe'
204	'520,lsass.exe'
205	'528,lsm.exe'
206	'628,svchost.exe'
207	'692,VBoxService.exe'
208	'756,svchost.exe'
209	'828,svchost.exe'
210	'USERENV.dll,C:WindowsSystem32USERENV.dll'
211	'876,svchost.exe'
212	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
213	'992,audiodg.exe'
214	'908,svchost.exe'
215	'appinfo.dll,c:windowssystem32appinfo.dll'
216	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
217	'320,svchost.exe'
218	'1028,svchost.exe'
219	'1224,spoolsv.exe'
220	'1252,svchost.exe'
221	'1384,svchost.exe'
222	'1412,FoxitConnectedPDFService.exe'
223	'1904,svchost.exe'
224	'2096,sppsvc.exe'
225	'2104,taskhost.exe'
226	'2304,userinit.exe'
227	'2312,dwm.exe'
228	'2336,explorer.exe'
229	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
230	'WSCAPI.dll,C:WindowsSystem32WSCAPI.dll'
231	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
232	'MLANG.dll,C:Windowssystem32MLANG.dll'
233	'2416,VBoxTray.exe'
234	'2432,MySQLNotifier.exe'
235	'2532,dwm.exe'
236	'2540,XXX'
237	'2616,jusched.exe'
238	'2772,WmiPrvSE.exe'
239	'3060,mintty.exe'

240	'2056,conhost.exe'
241	'2248,bash.exe'
242	'2288,SearchIndexer.exe'
243	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
244	'2656,SearchProtocolHost.exe'
245	'2648,SearchFilterHost.exe'
246	'2972,wmpnetwk.exe'
247	'2208,XXX'
248	'1544,driver_endpoint_netconn.exe'
249	'2196,taskmgr.exe'
250	'2568,adobeflash.exe'
251	'2216,dllhost.exe'
252	'3016,taskmgr.exe'
253	'3344,svchost.exe'
254	'WS2_32.dll,C:Windowssystem32WS2_32.dll'
255	'3524,cmd.exe'
256	'3532,conhost.exe'
257	'3584,Wireshark.exe'
258	'msls31.dll,C:WindowsSystem32msls31.dll'
259	'msimtf.dll,C:Windowssystem32msimtf.dll'
260	'3724,dumpcap.exe'
261	'3732,conhost.exe'
262	'3860,dumpcap.exe'
263	'3868,conhost.exe'
264	'3972,soffice.exe'
265	'3992,soffice.bin'
266	'4048,WMIADAP.exe'
267	'4076,WmiPrvSE.exe'
268	'3316,firefox.exe'
269	'3772,firefox.exe'
270	'5072,cmd.exe'
271	'5104,java.exe'
272	'4508,java.exe'
273	'5044,firefox.exe'
274	'5164,firefox.exe'
275	'5640,cmd.exe'
276	'5648,conhost.exe'
277	'5680,NETSTAT.EXE'
278	'5756,notepad++.exe'
279	'6936,audiodg.exe'
280	'6016,FoxitReader.exe'

281	'5444,SearchProtocolHost.exe'
282	'5452,SearchFilterHost.exe'
283	'5892,mintty.exe'
284	'5964,conhost.exe'
285	'5708,bash.exe'
286	'6428,wermgr.exe'
287	'6488,taskhost.exe'
288	'6684,simpress.exe'
289	'6692,soffice.exe'
290	'7720,java.exe'
291	'7728,conhost.exe'
292	'7948,SearchProtocolHost.exe'
293	'7968,SearchFilterHost.exe'
294	'412,csrss.exe'
295	'420,wininit.exe'
296	'460,winlogon.exe'
297	'524,lsm.exe'
298	'516,lsass.exe'
299	'624,svchost.exe'
300	'688,VBoxService.exe'
301	'752,svchost.exe'
302	'832,svchost.exe'
303	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
304	'868,svchost.exe'
305	'896,svchost.exe'
306	'304,svchost.exe'
307	'308,svchost.exe'
308	'1204,spoolsv.exe'
309	'1236,svchost.exe'
310	'1352,svchost.exe'
311	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
312	'1868,svchost.exe'
313	'2012,sppsvc.exe'
314	'1136,taskhost.exe'
315	'2136,userinit.exe'
316	'2144,dwm.exe'
317	'2168,explorer.exe'
318	'browcli.dll,C:Windowssystem32rowcli.dll'
319	'wdi.dll,C:Windowssystem32wdi.dll'
320	'mtxoci.dll,C:Windowssystem32mtxoci.dll'
321	'zipfldr.dll,C:Windowssystem32zipfldr.dll'

322	'SearchFolder.dll,C:Windowssystem32SearchFolder.dll'
323	'shacct.dll,C:WindowsSystem32shacct.dll'
324	'2256,VBoxTray.exe'
325	'2264,MySQLNotifier.exe'
326	'2348,dwm.exe'
327	'2372,adobeflash.exe'
328	'2384,XXX'
329	'2460,jusched.exe'
330	'2576,WmiPrvSE.exe'
331	'2864,mintty.exe'
332	'2900,conhost.exe'
333	'2916,XXX'
334	'2932,bash.exe'
335	'2084,SearchIndexer.exe'
336	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
337	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
338	'2120,SearchProtocolHost.exe'
339	'2220,SearchFilterHost.exe'
340	'2420,wmpnetwk.exe'
341	'iertutil.dll,C:Windowssystem32iertutil.dll'
342	'2952,XXX'
343	'3032,driver_endpoint_netconn.exe'
344	'3008,taskmgr.exe'
345	'944,desktop.exe'
346	'2496,dllhost.exe'
347	'2840,dllhost.exe'
348	'2808,taskmgr.exe'
349	'3284,svchost.exe'
350	'4620,audiodg.exe'
351	'4624,audiodg.exe'
352	'3548,WMIADAP.exe'
353	'3576,WmiPrvSE.exe'
354	'4064,firefox.exe'
355	'3320,firefox.exe'
356	'4404,sdraw.exe'
357	'4412,soffice.exe'
358	'4420,soffice.bin'
359	'4784,Wireshark.exe'
360	'5216,dumpcap.exe'
361	'5224,conhost.exe'
362	'5752,dllhost.exe'

363	'5900,dllhost.exe'
364	'5932,dllhost.exe'
365	'6132,firefox.exe'
366	'5292,firefox.exe'
367	'5888,dllhost.exe'
368	'5692,dllhost.exe'
369	'6300,dllhost.exe'
370	'6336,dllhost.exe'
371	'6368,mmc.exe'
372	'wevtapi.dll,C:Windowssystem32wevtapi.dll'
373	'COMDLG32.dll,C:Windowssystem32COMDLG32.dll'
374	'RichEd20.DLL,C:Windowssystem32RichEd20.DLL'
375	'System.Web.ni.dll,C:WindowsassemblyNativeImages_v2.0.50727_64System.Webea5a0e7af3956d40caeffaab3bb8b753System.Web.ni.dll'
376	'6644,dumpcap.exe'
377	'6660,conhost.exe'
378	'6868,mspaint.exe'
379	'6916,svchost.exe'
380	'7084,FoxitReader.exe'
381	'6596,SearchProtocolHost.exe'
382	'6512,SearchFilterHost.exe'
383	'6476,notepad++.exe'
384	'7572,firefox.exe'
385	'7740,firefox.exe'
386	'8016,dllhost.exe'
387	'8384,dllhost.exe'
388	'8532,SearchProtocolHost.exe'
389	'8556,SearchFilterHost.exe'
390	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
391	'msxml6.dll,C:WindowsSystem32msxml6.dll'
392	'ehtrace.dll,C:Windowsehomeehtrace.dll'
393	'8568,dllhost.exe'
394	'8784,dllhost.exe'
395	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
396	'9016,XXX'
397	'9036,setup_wm.exe'
398	'9188,unregmp2.exe'
399	'8256,wmplayer.exe'
400	'9228,dllhost.exe'
401	'9652,dllhost.exe'

Table 116: Alina Malware Instance 1 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'356,XXX'	'368,csrss.exe'
5	'356,XXX'	'408,wininit.exe'
6	'356,XXX'	'364,csrss.exe'
7	'356,XXX'	'404,wininit.exe'
8	'356,XXX'	'420,wininit.exe'
9	'368,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
10	'368,csrss.exe'	'1444,conhost.exe'
11	'408,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
12	'408,wininit.exe'	'508,services.exe'
13	'408,wininit.exe'	'532,lsm.exe'
14	'408,wininit.exe'	'524,lsass.exe'
15	'416,XXX'	'428,csrss.exe'
16	'416,XXX'	'464,winlogon.exe'
17	'428,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
18	'428,csrss.exe'	'836,conhost.exe'
19	'428,csrss.exe'	'1968,conhost.exe'
20	'428,csrss.exe'	'4320,conhost.exe'
21	'428,csrss.exe'	'4608,conhost.exe'
22	'428,csrss.exe'	'5080,conhost.exe'
23	'428,csrss.exe'	'5416,conhost.exe'
24	'428,csrss.exe'	'5944,conhost.exe'
25	'428,csrss.exe'	'2056,conhost.exe'
26	'428,csrss.exe'	'3532,conhost.exe'
27	'428,csrss.exe'	'3732,conhost.exe'
28	'428,csrss.exe'	'3868,conhost.exe'
29	'428,csrss.exe'	'5648,conhost.exe'
30	'428,csrss.exe'	'5964,conhost.exe'
31	'428,csrss.exe'	'7728,conhost.exe'
32	'464,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
33	'464,winlogon.exe'	'2304,userinit.exe'
34	'508,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
35	'508,services.exe'	'636,svchost.exe'
36	'508,services.exe'	'700,VBoxService.exe'
37	'508,services.exe'	'764,svchost.exe'
38	'508,services.exe'	'856,svchost.exe'
39	'508,services.exe'	'900,svchost.exe'

40	'508,services.exe'	'940,svchost.exe'
41	'508,services.exe'	'384,svchost.exe'
42	'508,services.exe'	'1000,svchost.exe'
43	'508,services.exe'	'1156,spoolsv.exe'
44	'508,services.exe'	'1204,svchost.exe'
45	'508,services.exe'	'1356,svchost.exe'
46	'508,services.exe'	'1400,FoxitConnectedPDFService.exe'
47	'508,services.exe'	'1880,svchost.exe'
48	'508,services.exe'	'2056,taskhost.exe'
49	'508,services.exe'	'2656,SearchIndexer.exe'
50	'508,services.exe'	'2852,wmpnetwk.exe'
51	'508,services.exe'	'2316,sppsvc.exe'
52	'508,services.exe'	'2268,svchost.exe'
53	'508,services.exe'	'2844,sdclt.exe'
54	'508,services.exe'	'3292,sc.exe'
55	'508,services.exe'	'3588,wsqmcons.exe'
56	'508,services.exe'	'2940,taskhost.exe'
57	'508,services.exe'	'5192,taskhost.exe'
58	'508,services.exe'	'3592,svchost.exe'
59	'508,services.exe'	'624,svchost.exe'
60	'508,services.exe'	'688,VBoxService.exe'
61	'508,services.exe'	'752,svchost.exe'
62	'508,services.exe'	'832,svchost.exe'
63	'508,services.exe'	'868,svchost.exe'
64	'508,services.exe'	'896,svchost.exe'
65	'508,services.exe'	'304,svchost.exe'
66	'508,services.exe'	'308,svchost.exe'
67	'508,services.exe'	'1204,spoolsv.exe'
68	'508,services.exe'	'1236,svchost.exe'
69	'508,services.exe'	'1352,svchost.exe'
70	'508,services.exe'	'1868,svchost.exe'
71	'508,services.exe'	'2012,sppsvc.exe'
72	'508,services.exe'	'1136,taskhost.exe'
73	'508,services.exe'	'2084,SearchIndexer.exe'
74	'508,services.exe'	'2420,wmpnetwk.exe'
75	'508,services.exe'	'3284,svchost.exe'
76	'508,services.exe'	'6916,svchost.exe'
77	'532,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
78	'524,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
79	'524,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
80	'636,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'

81	'636,svchost.exe'	'2428,WmiPrvSE.exe'
82	'636,svchost.exe'	'1860,WmiPrvSE.exe'
83	'636,svchost.exe'	'6484,dllhost.exe'
84	'636,svchost.exe'	'6616,dllhost.exe'
85	'636,svchost.exe'	'6740,dllhost.exe'
86	'636,svchost.exe'	'6780,dllhost.exe'
87	'636,svchost.exe'	'2168,dllhost.exe'
88	'636,svchost.exe'	'3736,dllhost.exe'
89	'636,svchost.exe'	'3484,dllhost.exe'
90	'636,svchost.exe'	'4052,dllhost.exe'
91	'636,svchost.exe'	'3980,dllhost.exe'
92	'636,svchost.exe'	'4268,dllhost.exe'
93	'636,svchost.exe'	'4372,dllhost.exe'
94	'636,svchost.exe'	'3708,dllhost.exe'
95	'636,svchost.exe'	'5424,dllhost.exe'
96	'636,svchost.exe'	'5276,dllhost.exe'
97	'636,svchost.exe'	'5148,dllhost.exe'
98	'636,svchost.exe'	'1888,slui.exe'
99	'700,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
100	'764,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
101	'856,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
102	'856,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
103	'856,svchost.exe'	'1008,audiodg.exe'
104	'856,svchost.exe'	'5828,audiodg.exe'
105	'900,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
106	'900,svchost.exe'	'1780,dwm.exe'
107	'940,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
108	'940,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
109	'940,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
110	'940,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
111	'940,svchost.exe'	'1832,WMIADAP.exe'
112	'940,svchost.exe'	'6660,consent.exe'
113	'940,svchost.exe'	'5284,consent.exe'
114	'384,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
115	'384,svchost.exe'	'vmictimeprovider.dll,C:WindowsSystem32vmictimeprovider.dll'
116	'384,svchost.exe'	'dsrole.dll,C:Windowssystem32dsrole.dll'
117	'384,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
118	'384,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
119	'1000,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
120	'1000,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
121	'1000,svchost.exe'	'2248,bash.exe'

122	'1156,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
123	'1204,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
124	'1204,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
125	'1356,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
126	'1400,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
127	'1880,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
128	'1780,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
129	'1328,XXX'	'1612,explorer.exe'
130	'1612,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
131	'1612,explorer.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
132	'1612,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
133	'1612,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
134	'1612,explorer.exe'	'sbdrop.dll,C:Program FilesWindows Sidebarsbdrop.dll'
135	'1612,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
136	'1612,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
137	'1612,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
138	'1612,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
139	'1612,explorer.exe'	'docprop.dll,C:Windowssystem32docprop.dll'
140	'1612,explorer.exe'	'sxproxy.dll,C:Windowssystem32sxproxy.dll'
141	'1612,explorer.exe'	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
142	'1612,explorer.exe'	'dxgi.dll,C:Windowssystem32dxgi.dll'
143	'1612,explorer.exe'	'2156,VBoxTray.exe'
144	'1612,explorer.exe'	'2176,MySQLNotifier.exe'
145	'1612,explorer.exe'	'1332,mintty.exe'
146	'1612,explorer.exe'	'3572,cmd.exe'
147	'1612,explorer.exe'	'3520,firefox.exe'
148	'1612,explorer.exe'	'4312,cmd.exe'
149	'1612,explorer.exe'	'4412,notepad++.exe'
150	'1612,explorer.exe'	'4464,Wireshark.exe'
151	'1612,explorer.exe'	'4324,firefox.exe'
152	'1612,explorer.exe'	'4448,FoxitReader.exe'
153	'1612,explorer.exe'	'5032,mintty.exe'
154	'1612,explorer.exe'	'6816,3_4.exe'
155	'1612,explorer.exe'	'7892,notepad++.exe'
156	'1612,explorer.exe'	'7316,calc.exe'
157	'1612,explorer.exe'	'4624,regedit.exe'
158	'1612,explorer.exe'	'6596,firefox.exe'
159	'1612,explorer.exe'	'7136,soffice.exe'
160	'1612,explorer.exe'	'3152,firefox.exe'
161	'2056,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
162	'2156,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'

163	'2176,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
164	'2220,dllhost.exe'	'2272,jusched.exe'
165	'2220,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
166	'2272,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
167	'2428,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
168	'2428,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
169	'2656,SearchIndexer.exe'	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
170	'2656,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
171	'2656,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
172	'2656,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
173	'2656,SearchIndexer.exe'	'2724,SearchProtocolHost.exe'
174	'2656,SearchIndexer.exe'	'2744,SearchFilterHost.exe'
175	'2656,SearchIndexer.exe'	'1640,SearchFilterHost.exe'
176	'2656,SearchIndexer.exe'	'3728,SearchProtocolHost.exe'
177	'2656,SearchIndexer.exe'	'3204,SearchProtocolHost.exe'
178	'2656,SearchIndexer.exe'	'3892,SearchFilterHost.exe'
179	'2656,SearchIndexer.exe'	'4792,SearchProtocolHost.exe'
180	'2656,SearchIndexer.exe'	'4824,SearchFilterHost.exe'
181	'2656,SearchIndexer.exe'	'5980,SearchProtocolHost.exe'
182	'2656,SearchIndexer.exe'	'5136,SearchFilterHost.exe'
183	'2656,SearchIndexer.exe'	'6156,SearchProtocolHost.exe'
184	'2656,SearchIndexer.exe'	'6176,SearchFilterHost.exe'
185	'2656,SearchIndexer.exe'	'7944,SearchProtocolHost.exe'
186	'2656,SearchIndexer.exe'	'7300,SearchFilterHost.exe'
187	'2724,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
188	'2724,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
189	'2744,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
190	'2852,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
191	'2316,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
192	'2268,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
193	'2268,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'

194	'332,XXX'	'3268,taskmgr.exe'
195	'3268,taskmgr.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
196	'3268,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
197	'1332,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
198	'836,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
199	'2760,XXX'	'2524,bash.exe'
200	'2524,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
201	'3672,XXX'	'3928,driver_endpoint_netconn.exe'
202	'3928,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
203	'1640,SearchFilterHost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
204	'3728,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
205	'1832,WMIADAP.exe'	'PSAPI.DLL,C:Windowssystem32PSAPI.DLL'
206	'1832,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
207	'1860,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
208	'2940,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
209	'3204,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
210	'3892,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
211	'3572,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
212	'3572,cmd.exe'	'3700,java.exe'
213	'1968,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
214	'3700,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
215	'3700,java.exe'	'5424,java.exe'
216	'3520,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
217	'3520,firefox.exe'	'2756,firefox.exe'
218	'3520,firefox.exe'	'5676,simpress.exe'
219	'2756,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
220	'4312,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
221	'4312,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
222	'4312,cmd.exe'	'4348,NETSTAT.EXE'
223	'4320,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
224	'4348,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
225	'4348,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
226	'4412,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
227	'4412,notepad++.exe'	'4420,soffice.bin'
228	'4464,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
229	'4464,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
230	'4464,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
231	'4464,Wireshark.exe'	'4524,gspawn-win64-helper.exe'
232	'4464,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'

233	'4464,Wireshark.exe'	'DUI70.dll,C:Windowssystem32DUI70.dll'
234	'4464,Wireshark.exe'	'4600,dumpcap.exe'
235	'4464,Wireshark.exe'	'5948,dumpcap.exe'
236	'4524,gspawn-win64-helper.exe'	'4536,androiddump.exe'
237	'4600,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
238	'4608,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
239	'4448,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
240	'4448,FoxitReader.exe'	'4536,FoxitReaderUpdater.exe'
241	'4536,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
242	'4792,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
243	'4824,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
244	'5032,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
245	'5080,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
246	'5080,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
247	'2612,XXX'	'4124,bash.exe'
248	'4124,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
249	'5192,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
250	'5676,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
251	'5676,simpress.exe'	'5684,soffice.exe'
252	'5684,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
253	'5684,soffice.exe'	'5692,soffice.bin'
254	'5692,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
255	'5424,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
256	'5416,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
257	'5980,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
258	'5980,SearchProtocolHost.exe'	'5708,bash.exe'
259	'5136,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
260	'5944,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
261	'5948,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
262	'6156,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
263	'6176,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
264	'6484,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
265	'6616,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
266	'6660,consent.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
267	'6740,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
268	'6780,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
269	'6816,3_4.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

270	'6816,3_4.exe'	'6880,dwm.exe'
271	'6880,dwm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
272	'7944,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
273	'7300,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
274	'7316,calc.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
275	'7252,XXX'	'7796,driver_endpoint_netconn.exe'
276	'7796,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
277	'2168,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
278	'2168,dllhost.exe'	'2256,VBoxTray.exe'
279	'2168,dllhost.exe'	'2264,MySQLNotifier.exe'
280	'2168,dllhost.exe'	'2348,dwm.exe'
281	'2168,dllhost.exe'	'2372,adobeflash.exe'
282	'2168,dllhost.exe'	'2864,mintty.exe'
283	'2168,dllhost.exe'	'3008,taskmgr.exe'
284	'2168,dllhost.exe'	'4064,firefox.exe'
285	'2168,dllhost.exe'	'4404,sdraw.exe'
286	'2168,dllhost.exe'	'4784,Wireshark.exe'
287	'2168,dllhost.exe'	'6132,firefox.exe'
288	'2168,dllhost.exe'	'6368,mmc.exe'
289	'2168,dllhost.exe'	'6868,mspaint.exe'
290	'2168,dllhost.exe'	'7084,FoxitReader.exe'
291	'2168,dllhost.exe'	'6476,notepad++.exe'
292	'2168,dllhost.exe'	'7572,firefox.exe'
293	'3592,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
294	'3736,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
295	'3484,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
296	'4052,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
297	'3980,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
298	'4268,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
299	'4372,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
300	'3708,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
301	'5424,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
302	'5276,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
303	'4624,regedit.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
304	'5148,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
305	'6596,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
306	'6596,firefox.exe'	'5180,firefox.exe'
307	'6596,firefox.exe'	'4724,FoxitReader.exe'
308	'5180,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
309	'7136,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

310	'7136,soffice.exe'	'6700,soffice.bin'
311	'6700,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
312	'4724,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
313	'3152,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
314	'3152,firefox.exe'	'3536,firefox.exe'
315	'3536,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
316	'1888,slui.exe'	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
317	'364,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
318	'404,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
319	'404,wininit.exe'	'512,services.exe'
320	'404,wininit.exe'	'520,lsass.exe'
321	'404,wininit.exe'	'528,lsm.exe'
322	'404,wininit.exe'	'412,csrss.exe'
323	'404,wininit.exe'	'460,winlogon.exe'
324	'512,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
325	'512,services.exe'	'628,svchost.exe'
326	'512,services.exe'	'692,VBoxService.exe'
327	'512,services.exe'	'756,svchost.exe'
328	'512,services.exe'	'828,svchost.exe'
329	'512,services.exe'	'876,svchost.exe'
330	'512,services.exe'	'908,svchost.exe'
331	'512,services.exe'	'320,svchost.exe'
332	'512,services.exe'	'1028,svchost.exe'
333	'512,services.exe'	'1224,spoolsv.exe'
334	'512,services.exe'	'1252,svchost.exe'
335	'512,services.exe'	'1384,svchost.exe'
336	'512,services.exe'	'1412,FoxitConnectedPDFService.exe'
337	'512,services.exe'	'1904,svchost.exe'
338	'512,services.exe'	'2096,sppsvc.exe'
339	'512,services.exe'	'2104,taskhost.exe'
340	'512,services.exe'	'2288,SearchIndexer.exe'
341	'512,services.exe'	'2972,wmpnetwk.exe'
342	'512,services.exe'	'3344,svchost.exe'
343	'512,services.exe'	'6428,wermgr.exe'
344	'512,services.exe'	'6488,taskhost.exe'
345	'520,lsass.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
346	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
347	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
348	'628,svchost.exe'	'2220,dllhost.exe'
349	'628,svchost.exe'	'2772,WmiPrvSE.exe'
350	'628,svchost.exe'	'2216,dllhost.exe'

351	'628,svchost.exe'	'4076,WmiPrvSE.exe'
352	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
353	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
354	'828,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
355	'828,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
356	'828,svchost.exe'	'USERENV.dll,C:WindowsSystem32USERENV.dll'
357	'828,svchost.exe'	'992,audiodg.exe'
358	'828,svchost.exe'	'6936,audiodg.exe'
359	'876,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
360	'876,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
361	'876,svchost.exe'	'2312,dwm.exe'
362	'908,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
363	'908,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
364	'908,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
365	'908,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
366	'908,svchost.exe'	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
367	'908,svchost.exe'	'4048,WMIADAP.exe'
368	'320,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
369	'1028,svchost.exe'	'PSAPI.DLL,C:Windowssystem32PSAPI.DLL'
370	'1224,spoolsv.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
371	'1252,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
372	'1252,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
373	'1384,svchost.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
374	'1384,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
375	'1412,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
376	'1904,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
377	'2096,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
378	'2104,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
379	'2304,userinit.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
380	'2304,userinit.exe'	'2336,explorer.exe'
381	'2312,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
382	'2336,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
383	'2336,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
384	'2336,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
385	'2336,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
386	'2336,explorer.exe'	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
387	'2336,explorer.exe'	'WSCAPI.dll,C:WindowsSystem32WSCAPI.dll'
388	'2336,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
389	'2336,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
390	'2336,explorer.exe'	'2416,VBoxTray.exe'
391	'2336,explorer.exe'	'2432,MySQLNotifier.exe'

392	'2336,explorer.exe'	'2532,dwm.exe'
393	'2336,explorer.exe'	'3060,mintty.exe'
394	'2336,explorer.exe'	'2196,taskmgr.exe'
395	'2336,explorer.exe'	'3524,cmd.exe'
396	'2336,explorer.exe'	'3584,Wireshark.exe'
397	'2336,explorer.exe'	'3972,soffice.exe'
398	'2336,explorer.exe'	'3316,firefox.exe'
399	'2336,explorer.exe'	'5072,cmd.exe'
400	'2336,explorer.exe'	'5044,firefox.exe'
401	'2336,explorer.exe'	'5640,cmd.exe'
402	'2336,explorer.exe'	'5756,notepad++.exe'
403	'2336,explorer.exe'	'6016,FoxitReader.exe'
404	'2336,explorer.exe'	'5892,mintty.exe'
405	'2416,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
406	'2432,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
407	'2532,dwm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
408	'2532,dwm.exe'	'2568,adobeflash.exe'
409	'2540,XXX'	'2616,jusched.exe'
410	'2616,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
411	'2772,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
412	'2772,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
413	'3060,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
414	'2056,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
415	'2248,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
416	'2288,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
417	'2288,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
418	'2288,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
419	'2288,SearchIndexer.exe'	'2656,SearchProtocolHost.exe'
420	'2288,SearchIndexer.exe'	'2648,SearchFilterHost.exe'
421	'2288,SearchIndexer.exe'	'5444,SearchProtocolHost.exe'
422	'2288,SearchIndexer.exe'	'5452,SearchFilterHost.exe'
423	'2288,SearchIndexer.exe'	'7948,SearchProtocolHost.exe'
424	'2288,SearchIndexer.exe'	'7968,SearchFilterHost.exe'
425	'2656,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
426	'2648,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
427	'2972,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'

428	'2208,XXX'	'1544,driver_endpoint_netconn.exe'
429	'1544,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
430	'2196,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
431	'2196,taskmgr.exe'	'3016,taskmgr.exe'
432	'2568,adobeflash.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
433	'2216,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
434	'3016,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
435	'3344,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
436	'3344,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
437	'3344,svchost.exe'	'WS2_32.dll,C:Windowssystem32WS2_32.dll'
438	'3524,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
439	'3532,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
440	'3584,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
441	'3584,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
442	'3584,Wireshark.exe'	'msls31.dll,C:WindowsSystem32msls31.dll'
443	'3584,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
444	'3584,Wireshark.exe'	'3724,dumpcap.exe'
445	'3584,Wireshark.exe'	'3860,dumpcap.exe'
446	'3724,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
447	'3732,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
448	'3860,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
449	'3868,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
450	'3972,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
451	'3972,soffice.exe'	'3992,soffice.bin'
452	'3992,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
453	'4048,WMIADAP.exe'	'PSAPI.DLL,C:Windowssystem32PSAPI.DLL'
454	'4048,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
455	'4076,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
456	'3316,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
457	'3316,firefox.exe'	'3772,firefox.exe'
458	'3772,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
459	'5072,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
460	'5072,cmd.exe'	'5104,java.exe'
461	'5072,cmd.exe'	'4508,java.exe'
462	'4508,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
463	'4508,java.exe'	'7720,java.exe'
464	'5044,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
465	'5044,firefox.exe'	'5164,firefox.exe'
466	'5044,firefox.exe'	'6684,simpress.exe'
467	'5164,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
468	'5640,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'

469	'5640,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
470	'5640,cmd.exe'	'5680,NETSTAT.EXE'
471	'5648,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
472	'5680,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
473	'5680,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
474	'5756,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
475	'6016,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
476	'5444,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
477	'5452,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
478	'5892,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
479	'5964,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
480	'5708,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
481	'6488,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
482	'6684,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
483	'6684,simpress.exe'	'6692,soffice.exe'
484	'6692,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
485	'6692,soffice.exe'	'6700,soffice.bin'
486	'7720,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
487	'7728,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
488	'7948,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
489	'7968,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
490	'412,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
491	'412,csrss.exe'	'2900,conhost.exe'
492	'412,csrss.exe'	'5224,conhost.exe'
493	'412,csrss.exe'	'6660,conhost.exe'
494	'420,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
495	'420,wininit.exe'	'508,services.exe'
496	'420,wininit.exe'	'524,lsm.exe'
497	'420,wininit.exe'	'516,lsass.exe'
498	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
499	'460,winlogon.exe'	'2136,userinit.exe'
500	'524,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
501	'516,lsass.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
502	'624,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
503	'624,svchost.exe'	'2576,WmiPrvSE.exe'
504	'624,svchost.exe'	'2496,dllhost.exe'
505	'624,svchost.exe'	'2840,dllhost.exe'
506	'624,svchost.exe'	'3576,WmiPrvSE.exe'
507	'624,svchost.exe'	'5752,dllhost.exe'
508	'624,svchost.exe'	'5900,dllhost.exe'

509	'624,svchost.exe'	'5932,dllhost.exe'
510	'624,svchost.exe'	'5888,dllhost.exe'
511	'624,svchost.exe'	'5692,dllhost.exe'
512	'624,svchost.exe'	'6300,dllhost.exe'
513	'624,svchost.exe'	'6336,dllhost.exe'
514	'624,svchost.exe'	'8016,dllhost.exe'
515	'624,svchost.exe'	'8384,dllhost.exe'
516	'624,svchost.exe'	'8568,dllhost.exe'
517	'624,svchost.exe'	'8784,dllhost.exe'
518	'624,svchost.exe'	'9228,dllhost.exe'
519	'624,svchost.exe'	'9652,dllhost.exe'
520	'688,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
521	'752,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
522	'832,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
523	'832,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
524	'832,svchost.exe'	'USERENV.dll,C:WindowsSystem32USERENV.dll'
525	'832,svchost.exe'	'992,audiodg.exe'
526	'832,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
527	'832,svchost.exe'	'4620,audiodg.exe'
528	'832,svchost.exe'	'4624,audiodg.exe'
529	'868,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
530	'868,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
531	'868,svchost.exe'	'2144,dwm.exe'
532	'896,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
533	'896,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
534	'896,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
535	'896,svchost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
536	'896,svchost.exe'	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
537	'896,svchost.exe'	'3548,WMIADAP.exe'
538	'304,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
539	'304,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
540	'304,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
541	'308,svchost.exe'	'PSAPI.DLL,C:Windowssystem32PSAPI.DLL'
542	'1204,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
543	'1236,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
544	'1236,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
545	'1352,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
546	'1352,svchost.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
547	'1352,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
548	'1352,svchost.exe'	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
549	'1868,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'

550	'2012,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
551	'1136,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
552	'2136,userinit.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
553	'2136,userinit.exe'	'2168,explorer.exe'
554	'2144,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
555	'2168,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
556	'2168,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
557	'2168,explorer.exe'	'dsrole.dll,C:Windowssystem32dsrole.dll'
558	'2168,explorer.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
559	'2168,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
560	'2168,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
561	'2168,explorer.exe'	'dxgi.dll,C:Windowssystem32dxgi.dll'
562	'2168,explorer.exe'	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
563	'2168,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
564	'2168,explorer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
565	'2168,explorer.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
566	'2168,explorer.exe'	'browcli.dll,C:Windowssystem32rowcli.dll'
567	'2168,explorer.exe'	'wdi.dll,C:Windowssystem32wdi.dll'
568	'2168,explorer.exe'	'mtxoci.dll,C:Windowssystem32mtxoci.dll'
569	'2168,explorer.exe'	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
570	'2168,explorer.exe'	'SearchFolder.dll,C:Windowssystem32SearchFolder.dll'
571	'2168,explorer.exe'	'shacct.dll,C:WindowsSystem32shacct.dll'
572	'2256,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
573	'2264,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
574	'2348,dwm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
575	'2348,dwm.exe'	'944,desktop.exe'
576	'2372,adobeflash.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
577	'2384,XXX'	'2460,jusched.exe'
578	'2460,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
579	'2576,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
580	'2576,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
581	'2864,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
582	'2900,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
583	'2916,XXX'	'2932,bash.exe'
584	'2932,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
585	'2084,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
586	'2084,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
587	'2084,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
588	'2084,SearchIndexer.exe'	'ElsLad.dll,C:Windowssystem32ElsLad.dll'

589	'2084,SearchIndexer.exe'	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
590	'2084,SearchIndexer.exe'	'2120,SearchProtocolHost.exe'
591	'2084,SearchIndexer.exe'	'2220,SearchFilterHost.exe'
592	'2084,SearchIndexer.exe'	'6596,SearchProtocolHost.exe'
593	'2084,SearchIndexer.exe'	'6512,SearchFilterHost.exe'
594	'2084,SearchIndexer.exe'	'8532,SearchProtocolHost.exe'
595	'2084,SearchIndexer.exe'	'8556,SearchFilterHost.exe'
596	'2120,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
597	'2220,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
598	'2420,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
599	'2420,wmpnetwk.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
600	'2952,XXX'	'3032,driver_endpoint_netconn.exe'
601	'3032,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
602	'3008,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
603	'3008,taskmgr.exe'	'2808,taskmgr.exe'
604	'944,desktop.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
605	'2496,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
606	'2840,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
607	'2808,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
608	'3284,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
609	'3284,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
610	'3284,svchost.exe'	'WS2_32.dll,C:Windowssystem32WS2_32.dll'
611	'3548,WMIADAP.exe'	'PSAPI.DLL,C:Windowssystem32PSAPI.DLL'
612	'3548,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
613	'3576,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
614	'4064,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
615	'4064,firefox.exe'	'3320,firefox.exe'
616	'3320,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
617	'4404,sdraw.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
618	'4404,sdraw.exe'	'4412,soffice.exe'
619	'4412,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
620	'4420,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
621	'4784,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
622	'4784,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
623	'4784,Wireshark.exe'	'5216,dumpcap.exe'
624	'4784,Wireshark.exe'	'6644,dumpcap.exe'
625	'5216,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'

626	'5224,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
627	'5752,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
628	'5900,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
629	'5932,dllhost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
630	'6132,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
631	'6132,firefox.exe'	'5292,firefox.exe'
632	'5292,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
633	'5888,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
634	'5692,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
635	'6300,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
636	'6336,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
637	'6368,mmc.exe'	'wevtapi.dll,C:Windowssystem32wevtapi.dll'
638	'6368,mmc.exe'	'COMDLG32.dll,C:Windowssystem32COMDLG32.dll'
639	'6368,mmc.exe'	'RichEd20.DLL,C:Windowssystem32RichEd20.DLL'
640	'6368,mmc.exe'	'System.Web.ni.dll,C:WindowsassemblyNativeImages_v2.0.50727_64System.Webea5a0e7af3956d40caeffaab3bb8b753System.Web.ni.dll'
641	'6644,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
642	'6660,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
643	'6868,mspaint.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
644	'6916,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
645	'7084,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
646	'6596,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
647	'6512,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
648	'6476,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
649	'7572,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
650	'7572,firefox.exe'	'7740,firefox.exe'
651	'7740,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
652	'8016,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
653	'8384,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
654	'8532,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
655	'8532,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
656	'8532,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
657	'8532,SearchProtocolHost.exe'	'ehtrace.dll,C:Windowsehomeehtrace.dll'
658	'8556,SearchFilterHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
659	'8556,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
660	'8556,SearchFilterHost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
661	'8568,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
662	'8784,dllhost.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'

663	'8784,dllhost.exe'	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
664	'9016,XXX'	'9036,setup_wm.exe'
665	'9036,setup_wm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
666	'9036,setup_wm.exe'	'9188,unregmp2.exe'
667	'9036,setup_wm.exe'	'8256,wmplayer.exe'
668	'8256,wmplayer.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
669	'9228,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
670	'9652,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'

7.2.12 Alina Malware – Instance 2

Table 117: Alina Malware Instance 2 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'356,XXX'
6	'364,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'404,wininit.exe'
9	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
10	'416,XXX'
11	'428,csrss.exe'
12	'464,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'508,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'532,lsm.exe'
17	'524,lsass.exe'
18	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
19	'636,svchost.exe'
20	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
21	'700,VBoxService.exe'
22	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
23	'764,svchost.exe'
24	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
25	'856,svchost.exe'
26	'netutils.dll,C:WindowsSystem32netutils.dll'
27	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
28	'904,svchost.exe'
29	'credssp.dll,C:WindowsSystem32credssp.dll'
30	'940,svchost.exe'
31	'AVRT.dll,c:windowssystem32AVRT.dll'
32	'wer.dll,C:Windowssystem32wer.dll'
33	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
34	'HID.DLL,C:WindowsSystem32HID.DLL'
35	'380,svchost.exe'

36	'dsrole.dll,C:Windowssystem32dsrole.dll'
37	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
38	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
39	'652,svchost.exe'
40	'SensApi.dll,C:Windowssystem32SensApi.dll'
41	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
42	'1196,spoolsv.exe'
43	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
44	'1228,svchost.exe'
45	'1352,svchost.exe'
46	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
47	'1396,FoxitConnectedPDFService.exe'
48	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
49	'1880,svchost.exe'
50	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
51	'1992,dwm.exe'
52	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
53	'1516,XXX'
54	'1148,explorer.exe'
55	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
56	thumbcache.dll,C:Windowssystem32humbcache.dll'
57	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
58	'tquery.dll,C:Windowssystem32query.dll'
59	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
60	'DfsShlEx.dll,C:Windowssystem32DfsShlEx.dll'
61	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
62	'1156,taskhost.exe'
63	'midimap.dll,C:Windowssystem32midimap.dll'
64	'2132,VBoxTray.exe'
65	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
66	'2152,MySQLNotifier.exe'
67	'2168,XXX'
68	'2248,jusched.exe'
69	'2440,WmiPrvSE.exe'
70	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
71	'2632,SearchIndexer.exe'
72	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
73	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
74	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'

75	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
76	'2856,wmpnetwk.exe'
77	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
78	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
79	'provsvc.dll,C:WindowsSystem32provsvc.dll'
80	'3048,sppsvc.exe'
81	'2412,svchost.exe'
82	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
83	'3040,XXX'
84	'628,taskmgr.exe'
85	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
86	'3208,mintty.exe'
87	'apphelp.dll,C:Windowssystem32apphelp.dll'
88	'3436,conhost.exe'
89	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
90	'3452,XXX'
91	'3200,bash.exe'
92	'authz.dll,C:Windowssystem32authz.dll'
93	'3768,audiodg.exe'
94	'3772,svchost.exe'
95	'defragproxy.dll,C:Windowssystem32defragproxy.dll'
96	'3780,XXX'
97	'3800,driver_endpoint_netconn.exe'
98	'3212,cmd.exe'
99	'3492,java.exe'
100	'3788,conhost.exe'
101	'880,java.exe'
102	'3584,firefox.exe'
103	'1548,firefox.exe'
104	'2708,cmd.exe'
105	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
106	'3156,conhost.exe'
107	'2508,NETSTAT.EXE'
108	'winrnr.dll,C:WindowsSystem32winrnr.dll'
109	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
110	'3708,notepad++.exe'
111	'620,gspawn-win64-helper.exe'
112	'2660,androiddump.exe'
113	'996,Wireshark.exe'
114	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
115	'IconCodecService.dll,C:Windowssystem32IconCodecService.dll'

116	'DUI70.dll,C:Windowssystem32DUI70.dll'
117	'1688,dumpcap.exe'
118	'3572,conhost.exe'
119	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
120	'1976,FoxitReader.exe'
121	'3616,FoxitReaderUpdater.exe'
122	'4376,audiodg.exe'
123	'4256,SearchProtocolHost.exe'
124	'4276,SearchFilterHost.exe'
125	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
126	'4684,mintty.exe'
127	'4724,conhost.exe'
128	'4740,XXX'
129	'4756,bash.exe'
130	'4852,SearchProtocolHost.exe'
131	'4868,SearchFilterHost.exe'
132	'4652,simpress.exe'
133	'4716,soffice.exe'
134	'4804,soffice.bin'
135	'5984,java.exe'
136	'5992,conhost.exe'
137	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
138	'5300,SearchProtocolHost.exe'
139	'profapi.dll,C:Windowssystem32profapi.dll'
140	'5368,SearchFilterHost.exe'
141	'SXS.DLL,C:Windowssystem32SXS.DLL'
142	'5524,dumpcap.exe'
143	'5556,conhost.exe'
144	'5996,consent.exe'
145	'5896,dllhost.exe'
146	'5184,dllhost.exe'
147	'IDStore.dll,C:WindowsSystem32IDStore.dll'
148	'5308,dllhost.exe'
149	'5444,3_4.exe'
150	'5516,jusched.exe'
151	'5480,firefox.exe'
152	'7060,XXX'
153	'7072,driver_endpoint_netconn.exe'
154	'1020,audiodg.exe'
155	'1876,consent.exe'
156	'420,dllhost.exe'

157	'3552,dllhost.exe'
158	'1136,cmd.exe'
159	'1820,conhost.exe'
160	'1800,slui.exe'
161	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
162	'3740,soffice.exe'
163	'3300,soffice.bin'
164	'2704,taskhost.exe'
165	'5000,notepad++.exe'
166	'4940,dllhost.exe'
167	'4896,SearchProtocolHost.exe'
168	'4380,SearchFilterHost.exe'
169	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
170	'4768,dllhost.exe'
171	'6092,dllhost.exe'
172	'4204,mip.exe'
173	'mraut.DLL,C:Program FilesCommon Filesmicrosoft sharedinkmraut.DLL'
174	'6000,wisptis.exe'
175	tpcps.dll,C:Program FilesCommon FilesMicrosoft SharedInkpcps.dll'
176	'6320,audiodg.exe'
177	'5116,FoxitReader.exe'
178	'3364,SearchProtocolHost.exe'
179	'3956,SearchFilterHost.exe'
180	'4812,powershell.exe'
181	'4840,conhost.exe'
182	'5792,firefox.exe'
183	'6072,firefox.exe'
184	'5292,WmiPrvSE.exe'
185	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
186	'2692,soffice.exe'
187	'2756,soffice.bin'
188	'5392,sbase.exe'
189	'4788,soffice.exe'
190	'4960,soffice.bin'
191	'6848,simpress.exe'
192	'6800,soffice.exe'
193	'3752,soffice.bin'
194	'4040,splwow64.exe'
195	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
196	'6348,SnippingTool.exe'

197	'2576,SearchProtocolHost.exe'
198	'7172,SearchFilterHost.exe'
199	'7352,firefox.exe'
200	'7832,pingsender.exe'
201	'7844,conhost.exe'
202	'7520,firefox.exe'
203	'7288,dllhost.exe'
204	'7220,dllhost.exe'
205	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
206	'8244,SearchProtocolHost.exe'
207	'8264,SearchFilterHost.exe'
208	'mlang.dll,C:Windowssystem32mlang.dll'
209	'8444,dllhost.exe'
210	'8560,firefox.exe'
211	'8724,firefox.exe'
212	'360,XXX'
213	'368,csrss.exe'
214	'408,wininit.exe'
215	'psbase.dll,C:Windowssystem32psbase.dll'
216	'wkscli.dll,C:Windowssystem32wkscli.dll'
217	'832,svchost.exe'
218	'USERENV.dll,C:WindowsSystem32USERENV.dll'
219	'888,svchost.exe'
220	'1004,audiodg.exe'
221	'936,svchost.exe'
222	'appinfo.dll,c:windowssystem32appinfo.dll'
223	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
224	'rasman.dll,C:Windowssystem32rasman.dll'
225	'384,svchost.exe'
226	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
227	'1028,svchost.exe'
228	'psapi.dll,C:Windowssystem32psapi.dll'
229	'1220,spoolsv.exe'
230	'1252,svchost.exe'
231	'1372,svchost.exe'
232	'1400,FoxitConnectedPDFService.exe'
233	'1868,svchost.exe'
234	'1608,taskhost.exe'
235	'2008,sppsvc.exe'
236	'2240,userinit.exe'
237	'2248,dwm.exe'

238	'2272,explorer.exe'
239	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
240	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
241	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
242	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
243	'browcli.dll,C:Windowssystem32rowcli.dll'
244	'docprop.dll,C:Windowssystem32docprop.dll'
245	'sxproxy.dll,C:Windowssystem32sxproxy.dll'
246	'sbdrop.dll,C:Program FilesWindows Sidebarsbdrop.dll'
247	'2364,VBoxTray.exe'
248	'2372,MySQLNotifier.exe'
249	'2452,jusched.exe'
250	'2464,XXX'
251	'2600,jusched.exe'
252	'2732,WmiPrvSE.exe'
253	'WMI.DLL,C:Windowssystem32WMI.DLL'
254	'2900,SearchIndexer.exe'
255	'2988,SearchProtocolHost.exe'
256	'3008,SearchFilterHost.exe'
257	'1312,mintty.exe'
258	'2148,conhost.exe'
259	'2128,XXX'
260	'1124,bash.exe'
261	'2552,wmpnetwk.exe'
262	'2548,XXX'
263	'2624,driver_endpoint_netconn.exe'
264	'2728,taskmgr.exe'
265	'2800,win-firewall.exe'
266	'2264,dllhost.exe'
267	'2332,dllhost.exe'
268	'2864,taskmgr.exe'
269	'3272,cmd.exe'
270	'3284,conhost.exe'
271	'3388,java.exe'
272	'3564,svchost.exe'
273	'WS2_32.dll,C:Windowssystem32WS2_32.dll'
274	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
275	taskschd.dll,C:Windowssystem32askschd.dll'
276	'6192,audiodg.exe'
277	'3768,java.exe'
278	'3776,conhost.exe'

279	'3832,cmd.exe'
280	'3840,conhost.exe'
281	'3912,cmd.exe'
282	'3920,conhost.exe'
283	'4024,java.exe'
284	'3160,firefox.exe'
285	'3548,firefox.exe'
286	'4308,cmd.exe'
287	'4316,conhost.exe'
288	'4332,NETSTAT.EXE'
289	'4400,notepad++.exe'
290	'4440,Wireshark.exe'
291	'msimtf.dll,C:Windowssystem32msimtf.dll'
292	'4584,dumpcap.exe'
293	'4592,conhost.exe'
294	'4760,WMIADAP.exe'
295	'4820,WmiPrvSE.exe'
296	'4808,FoxitReader.exe'
297	'5068,SearchProtocolHost.exe'
298	'3256,SearchFilterHost.exe'
299	'4564,mintty.exe'
300	'4696,conhost.exe'
301	'4728,XXX'
302	'4732,bash.exe'
303	'5576,simpress.exe'
304	'5600,soffice.exe'
305	'5612,soffice.bin'
306	'5960,svchost.exe'
307	'5204,java.exe'
308	'5508,conhost.exe'
309	'6412,iexplore.exe'
310	'6496,iexplore.exe'
311	'7032,dumpcap.exe'
312	'7040,conhost.exe'
313	'7080,SearchProtocolHost.exe'
314	'7100,SearchFilterHost.exe'
315	'7140,iexplore.exe'
316	'6300,iexplore.exe'
317	'6932,SearchProtocolHost.exe'
318	'6964,SearchFilterHost.exe'
319	'7660,firefox.exe'

320	'7228,dllhost.exe'
321	'7652,dllhost.exe'
322	'7956,svchost.exe'
323	'8380,SearchProtocolHost.exe'
324	'8404,SearchFilterHost.exe'
325	'8592,soffice.exe'
326	'8600,soffice.bin'
327	'292,smss.exe'
328	'632,svchost.exe'
329	'696,VBoxService.exe'
330	'760,svchost.exe'
331	'884,svchost.exe'
332	'932,svchost.exe'
333	'mspatcha.dll,c:windowssystem32mspatcha.dll'
334	'364,svchost.exe'
335	'1216,spoolsv.exe'
336	'1248,svchost.exe'
337	'1368,svchost.exe'
338	'upnphost.dll,c:windowssystem32upnphost.dll'
339	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
340	'1340,sppsvc.exe'
341	'1044,taskhost.exe'
342	'2164,userinit.exe'
343	'2172,dwm.exe'
344	'2196,explorer.exe'
345	'SearchFolder.dll,C:Windowssystem32SearchFolder.dll'
346	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
347	'puiobj.dll,C:Windowssystem32puiobj.dll'
348	'2284,VBoxTray.exe'
349	'2292,MySQLNotifier.exe'
350	'2356,jusched.exe'
351	'2368,win-firewall.exe'
352	'2380,XXX'
353	'2484,jusched.exe'
354	'2600,WmiPrvSE.exe'
355	'2952,mintty.exe'
356	'2996,conhost.exe'
357	'3012,XXX'
358	'3028,bash.exe'
359	'1084,SearchIndexer.exe'
360	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'

361	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
362	'NLSLexicons0010.dll,C:WindowsSystem32NLSLexicons0010.dll'
363	'2252,SearchProtocolHost.exe'
364	'2440,SearchFilterHost.exe'
365	'2420,wmpnetwk.exe'
366	'iertutil.dll,C:Windowssystem32iertutil.dll'
367	'1096,XXX'
368	'3056,driver_endpoint_netconn.exe'
369	'116,taskmgr.exe'
370	'2032,jucheck.exe'
371	'1992,dllhost.exe'
372	'2632,dllhost.exe'
373	'2112,taskmgr.exe'
374	'3296,svchost.exe'
375	tdh.dll,C:WindowsSystem32dh.dll'
376	'3472,firefox.exe'
377	'3668,firefox.exe'
378	'4012,WMIADAP.exe'
379	'4040,WmiPrvSE.exe'
380	'3268,cmd.exe'
381	'3280,conhost.exe'
382	'4120,simpress.exe'
383	'4128,soffice.exe'
384	'4136,soffice.bin'
385	'4348,StikyNot.exe'
386	'4464,audiodg.exe'
387	'7324,pingsender.exe'
388	'4408,SearchProtocolHost.exe'
389	'4428,SearchFilterHost.exe'
390	'rtffilt.dll,C:Windowssystem32rtffilt.dll'
391	'4468,SearchProtocolHost.exe'
392	'4956,dllhost.exe'
393	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
394	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
395	'5232,XXX'
396	'5256,setup_wm.exe'
397	'5412,wmplayer.exe'
398	'5928,SearchProtocolHost.exe'
399	'ehtrace.dll,C:Windowsehomeehtrace.dll'
400	'5948,SearchFilterHost.exe'

401	'msxml6.dll,C:WindowsSystem32msxml6.dll'
402	'4900,SearchProtocolHost.exe'
403	'5156,SearchFilterHost.exe'
404	'ksuser.dll,C:WindowsSystem32ksuser.dll'
405	'5316,xpsrchvw.exe'
406	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'
407	'6684,SearchProtocolHost.exe'
408	'slc.dll,C:Windowssystem32slc.dll'
409	'6704,SearchFilterHost.exe'
410	'6416,firefox.exe'
411	'7224,dllhost.exe'
412	'7516,cmd.exe'
413	'7524,conhost.exe'
414	'7636,java.exe'
415	'7764,firefox.exe'
416	'7928,firefox.exe'
417	'7468,cmd.exe'
418	'7476,conhost.exe'
419	'7508,NETSTAT.EXE'
420	'7596,notepad++.exe'
421	'7460,Wireshark.exe'
422	'8240,dumpcap.exe'
423	'8248,conhost.exe'
424	'8528,FoxitReader.exe'
425	'8728,SearchProtocolHost.exe'
426	'8748,SearchFilterHost.exe'
427	'8216,mintty.exe'
428	'8288,conhost.exe'
429	'8312,XXX'
430	'8328,bash.exe'
431	'8500,firefox.exe'
432	'8968,simpress.exe'
433	'9092,soffice.exe'
434	'9052,soffice.bin'
435	'8948,svchost.exe'
436	'9936,java.exe'
437	'9944,conhost.exe'
438	'9304,splwow64.exe'
439	'9388,gswin32c.exe'
440	'9392,conhost.exe'
441	'9460,CPWSave.exe'

442	'9468,CPWSave.exe'
443	'9748,SearchProtocolHost.exe'
444	'9780,SearchFilterHost.exe'
445	'10192,dumpcap.exe'
446	'10216,conhost.exe'

Table 118: Alina Malware Instance 2 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'4,System'	'292,smss.exe'
4	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'356,XXX'	'364,csrss.exe'
6	'356,XXX'	'404,wininit.exe'
7	'364,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'404,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
9	'404,wininit.exe'	'508,services.exe'
10	'404,wininit.exe'	'532,lsm.exe'
11	'404,wininit.exe'	'524,lsass.exe'
12	'416,XXX'	'428,csrss.exe'
13	'416,XXX'	'464,winlogon.exe'
14	'428,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
15	'428,csrss.exe'	'3436,conhost.exe'
16	'428,csrss.exe'	'3788,conhost.exe'
17	'428,csrss.exe'	'3156,conhost.exe'
18	'428,csrss.exe'	'3572,conhost.exe'
19	'428,csrss.exe'	'4724,conhost.exe'
20	'428,csrss.exe'	'5992,conhost.exe'
21	'428,csrss.exe'	'5556,conhost.exe'
22	'428,csrss.exe'	'1820,conhost.exe'
23	'428,csrss.exe'	'4840,conhost.exe'
24	'428,csrss.exe'	'7844,conhost.exe'
25	'428,csrss.exe'	'2148,conhost.exe'
26	'428,csrss.exe'	'3284,conhost.exe'
27	'428,csrss.exe'	'3776,conhost.exe'
28	'428,csrss.exe'	'3840,conhost.exe'
29	'428,csrss.exe'	'3920,conhost.exe'
30	'428,csrss.exe'	'4316,conhost.exe'
31	'428,csrss.exe'	'4592,conhost.exe'
32	'428,csrss.exe'	'4696,conhost.exe'
33	'428,csrss.exe'	'5508,conhost.exe'
34	'428,csrss.exe'	'7040,conhost.exe'
35	'428,csrss.exe'	'2996,conhost.exe'
36	'428,csrss.exe'	'3280,conhost.exe'
37	'428,csrss.exe'	'7524,conhost.exe'
38	'428,csrss.exe'	'7476,conhost.exe'
39	'428,csrss.exe'	'8248,conhost.exe'

40	'428,csrss.exe'	'8288,conhost.exe'
41	'428,csrss.exe'	'9944,conhost.exe'
42	'428,csrss.exe'	'10216,conhost.exe'
43	'464,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
44	'464,winlogon.exe'	'2240,userinit.exe'
45	'464,winlogon.exe'	'2164,userinit.exe'
46	'508,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
47	'508,services.exe'	'636,svchost.exe'
48	'508,services.exe'	'700,VBoxService.exe'
49	'508,services.exe'	'764,svchost.exe'
50	'508,services.exe'	'856,svchost.exe'
51	'508,services.exe'	'904,svchost.exe'
52	'508,services.exe'	'940,svchost.exe'
53	'508,services.exe'	'380,svchost.exe'
54	'508,services.exe'	'652,svchost.exe'
55	'508,services.exe'	'1196,spoolsv.exe'
56	'508,services.exe'	'1228,svchost.exe'
57	'508,services.exe'	'1352,svchost.exe'
58	'508,services.exe'	'1396,FoxitConnectedPDFService.exe'
59	'508,services.exe'	'1880,svchost.exe'
60	'508,services.exe'	'1156,taskhost.exe'
61	'508,services.exe'	'2632,SearchIndexer.exe'
62	'508,services.exe'	'2856,wmpnetwk.exe'
63	'508,services.exe'	'3048,sppsvc.exe'
64	'508,services.exe'	'2412,svchost.exe'
65	'508,services.exe'	'3772,svchost.exe'
66	'508,services.exe'	'2704,taskhost.exe'
67	'508,services.exe'	'832,svchost.exe'
68	'508,services.exe'	'888,svchost.exe'
69	'508,services.exe'	'936,svchost.exe'
70	'508,services.exe'	'384,svchost.exe'
71	'508,services.exe'	'1028,svchost.exe'
72	'508,services.exe'	'1220,spoolsv.exe'
73	'508,services.exe'	'1252,svchost.exe'
74	'508,services.exe'	'1372,svchost.exe'
75	'508,services.exe'	'1400,FoxitConnectedPDFService.exe'
76	'508,services.exe'	'1868,svchost.exe'
77	'508,services.exe'	'1608,taskhost.exe'
78	'508,services.exe'	'2008,sppsvc.exe'
79	'508,services.exe'	'2900,SearchIndexer.exe'
80	'508,services.exe'	'2552,wmpnetwk.exe'

81	'508,services.exe'	'3564,svchost.exe'
82	'508,services.exe'	'5960,svchost.exe'
83	'508,services.exe'	'7956,svchost.exe'
84	'508,services.exe'	'632,svchost.exe'
85	'508,services.exe'	'696,VBoxService.exe'
86	'508,services.exe'	'760,svchost.exe'
87	'508,services.exe'	'884,svchost.exe'
88	'508,services.exe'	'932,svchost.exe'
89	'508,services.exe'	'364,svchost.exe'
90	'508,services.exe'	'1216,spoolsv.exe'
91	'508,services.exe'	'1248,svchost.exe'
92	'508,services.exe'	'1368,svchost.exe'
93	'508,services.exe'	'1340,sppsvc.exe'
94	'508,services.exe'	'1044,taskhost.exe'
95	'508,services.exe'	'1084,SearchIndexer.exe'
96	'508,services.exe'	'2420,wmpnetwk.exe'
97	'508,services.exe'	'3296,svchost.exe'
98	'508,services.exe'	'8948,svchost.exe'
99	'532,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
100	'524,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
101	'524,lsass.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
102	'524,lsass.exe'	'psbase.dll,C:Windowssystem32psbase.dll'
103	'524,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
104	'636,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
105	'636,svchost.exe'	'2440,WmiPrvSE.exe'
106	'636,svchost.exe'	'5896,dllhost.exe'
107	'636,svchost.exe'	'5184,dllhost.exe'
108	'636,svchost.exe'	'5308,dllhost.exe'
109	'636,svchost.exe'	'420,dllhost.exe'
110	'636,svchost.exe'	'3552,dllhost.exe'
111	'636,svchost.exe'	'1800,slui.exe'
112	'636,svchost.exe'	'4940,dllhost.exe'
113	'636,svchost.exe'	'4768,dllhost.exe'
114	'636,svchost.exe'	'6092,dllhost.exe'
115	'636,svchost.exe'	'5292,WmiPrvSE.exe'
116	'636,svchost.exe'	'7288,dllhost.exe'
117	'636,svchost.exe'	'7220,dllhost.exe'
118	'636,svchost.exe'	'8444,dllhost.exe'
119	'636,svchost.exe'	'2732,WmiPrvSE.exe'
120	'636,svchost.exe'	'2264,dllhost.exe'
121	'636,svchost.exe'	'2332,dllhost.exe'

122	'636,svchost.exe'	'4820,WmiPrvSE.exe'
123	'636,svchost.exe'	'7228,dllhost.exe'
124	'636,svchost.exe'	'7652,dllhost.exe'
125	'700,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
126	'764,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
127	'856,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
128	'856,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
129	'856,svchost.exe'	'3768,audiodg.exe'
130	'856,svchost.exe'	'4376,audiodg.exe'
131	'856,svchost.exe'	'1020,audiodg.exe'
132	'856,svchost.exe'	'6320,audiodg.exe'
133	'904,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
134	'904,svchost.exe'	'HID.DLL,C:WindowsSystem32HID.DLL'
135	'904,svchost.exe'	'1992,dwm.exe'
136	'904,svchost.exe'	'6000,wisptis.exe'
137	'940,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
138	'940,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
139	'940,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
140	'940,svchost.exe'	'5996,consent.exe'
141	'940,svchost.exe'	'1876,consent.exe'
142	'380,svchost.exe'	'dsrole.dll,C:Windowssystem32dsrole.dll'
143	'380,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
144	'380,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
145	'380,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
146	'380,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
147	'652,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
148	'652,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
149	'1196,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
150	'1228,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
151	'1352,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
152	'1396,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
153	'1880,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
154	'1992,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
155	'1516,XXX'	'1148,explorer.exe'
156	'1148,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
157	'1148,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
158	'1148,explorer.exe'	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
159	'1148,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
160	'1148,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
161	'1148,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'

162	'1148,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
163	'1148,explorer.exe'	'DfsShlEx.dll,C:Windowssystem32DfsShlEx.dll'
164	'1148,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
165	'1148,explorer.exe'	'2132,VBoxTray.exe'
166	'1148,explorer.exe'	'2152,MySQLNotifier.exe'
167	'1148,explorer.exe'	'3208,mintty.exe'
168	'1148,explorer.exe'	'3212,cmd.exe'
169	'1148,explorer.exe'	'3584,firefox.exe'
170	'1148,explorer.exe'	'2708,cmd.exe'
171	'1148,explorer.exe'	'3708,notepad++.exe'
172	'1148,explorer.exe'	'996,Wireshark.exe'
173	'1148,explorer.exe'	'1976,FoxitReader.exe'
174	'1148,explorer.exe'	'4684,mintty.exe'
175	'1148,explorer.exe'	'5444,3_4.exe'
176	'1148,explorer.exe'	'1136,cmd.exe'
177	'1148,explorer.exe'	'3740,soffice.exe'
178	'1148,explorer.exe'	'5000,notepad++.exe'
179	'1148,explorer.exe'	'4204,mip.exe'
180	'1148,explorer.exe'	'5116,FoxitReader.exe'
181	'1148,explorer.exe'	'4812,powershell.exe'
182	'1148,explorer.exe'	'5792,firefox.exe'
183	'1148,explorer.exe'	'2692,soffice.exe'
184	'1148,explorer.exe'	'5392,sbase.exe'
185	'1148,explorer.exe'	'6848,simpress.exe'
186	'1148,explorer.exe'	'6348,SnippingTool.exe'
187	'1148,explorer.exe'	'8560,firefox.exe'
188	'1156,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
189	'2132,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
190	'2152,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
191	'2168,XXX'	'2248,jusched.exe'
192	'2248,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
193	'2440,WmiPrvSE.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
194	'2440,WmiPrvSE.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
195	'2440,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
196	'2440,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
197	'2632,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
198	'2632,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
199	'2632,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
200	'2632,SearchIndexer.exe'	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'

201	'2632,SearchIndexer.exe'	'4256,SearchProtocolHost.exe'
202	'2632,SearchIndexer.exe'	'4276,SearchFilterHost.exe'
203	'2632,SearchIndexer.exe'	'4852,SearchProtocolHost.exe'
204	'2632,SearchIndexer.exe'	'4868,SearchFilterHost.exe'
205	'2632,SearchIndexer.exe'	'5300,SearchProtocolHost.exe'
206	'2632,SearchIndexer.exe'	'5368,SearchFilterHost.exe'
207	'2632,SearchIndexer.exe'	'4896,SearchProtocolHost.exe'
208	'2632,SearchIndexer.exe'	'4380,SearchFilterHost.exe'
209	'2632,SearchIndexer.exe'	'3364,SearchProtocolHost.exe'
210	'2632,SearchIndexer.exe'	'3956,SearchFilterHost.exe'
211	'2632,SearchIndexer.exe'	'2576,SearchProtocolHost.exe'
212	'2632,SearchIndexer.exe'	'7172,SearchFilterHost.exe'
213	'2632,SearchIndexer.exe'	'8244,SearchProtocolHost.exe'
214	'2632,SearchIndexer.exe'	'8264,SearchFilterHost.exe'
215	'2856,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
216	'2856,wmpnetwk.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
217	'2856,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
218	'3048,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
219	'2412,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
220	'3040,XXX'	'628,taskmgr.exe'
221	'628,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
222	'3208,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
223	'3436,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
224	'3452,XXX'	'3200,bash.exe'
225	'3200,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
226	'3772,svchost.exe'	'defragproxy.dll,C:Windowssystem32defragproxy.dll'
227	'3780,XXX'	'3800,driver_endpoint_netconn.exe'
228	'3800,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
229	'3212,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
230	'3212,cmd.exe'	'3492,java.exe'
231	'3212,cmd.exe'	'880,java.exe'
232	'3788,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
233	'880,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
234	'880,java.exe'	'5984,java.exe'
235	'3584,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

236	'3584,firefox.exe'	'1548,firefox.exe'
237	'3584,firefox.exe'	'4652,simpress.exe'
238	'3584,firefox.exe'	'5480,firefox.exe'
239	'1548,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
240	'2708,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
241	'2708,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
242	'2708,cmd.exe'	'2508,NETSTAT.EXE'
243	'3156,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
244	'2508,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
245	'2508,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
246	'3708,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
247	'620,gspawn-win64-helper.exe'	'2660,androiddump.exe'
248	'996,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
249	'996,Wireshark.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
250	'996,Wireshark.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
251	'996,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
252	'996,Wireshark.exe'	'620,gspawn-win64-helper.exe'
253	'996,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
254	'996,Wireshark.exe'	'IconCodecService.dll,C:Windowssystem32IconCodecService.dll'
255	'996,Wireshark.exe'	'DUI70.dll,C:Windowssystem32DUI70.dll'
256	'996,Wireshark.exe'	'1688,dumpcap.exe'
257	'996,Wireshark.exe'	'5524,dumpcap.exe'
258	'1688,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
259	'3572,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
260	'1976,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
261	'1976,FoxitReader.exe'	'3616,FoxitReaderUpdater.exe'
262	'3616,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
263	'4256,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
264	'4276,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
265	'4684,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
266	'4724,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
267	'4740,XXX'	'4756,bash.exe'
268	'4756,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
269	'4852,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
270	'4868,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
271	'4652,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
272	'4652,simpress.exe'	'4716,soffice.exe'
273	'4716,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
274	'4716,soffice.exe'	'4804,soffice.bin'

275	'4804,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
276	'5984,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
277	'5992,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
278	'5300,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
279	'5368,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
280	'5524,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
281	'5556,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
282	'5896,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
283	'5184,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
284	'5308,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
285	'5444,3_4.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
286	'5444,3_4.exe'	'5516,jusched.exe'
287	'5516,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
288	'5480,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
289	'7060,XXX'	'7072,driver_endpoint_netconn.exe'
290	'7072,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
291	'420,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
292	'3552,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
293	'1136,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
294	'1136,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
295	'1820,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
296	'1800,slui.exe'	'WindowsCodecs.dll,C:WindowsSystem32WindowsCodecs.dll'
297	'3740,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
298	'3740,soffice.exe'	'3300,soffice.bin'
299	'3300,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
300	'3300,soffice.bin'	'4040,splwow64.exe'
301	'2704,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
302	'5000,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
303	'4940,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
304	'4896,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
305	'4380,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
306	'4768,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
307	'6092,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
308	'4204,mip.exe'	'mraut.DLL,C:Program FilesCommon Filesmicrosoft sharedinkmraut.DLL'
309	'6000,wisptis.exe'	tpcps.dll,C:Program FilesCommon FilesMicrosoft SharedInkpcps.dll'
310	'5116,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
311	'5116,FoxitReader.exe'	'7352,firefox.exe'
312	'3364,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'

313	'3956,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
314	'4812,powershell.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
315	'4840,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
316	'5792,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
317	'5792,firefox.exe'	'6072,firefox.exe'
318	'6072,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
319	'5292,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
320	'2692,soffice.exe'	'2756,soffice.bin'
321	'5392,sbase.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
322	'5392,sbase.exe'	'4788,soffice.exe'
323	'4788,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
324	'4788,soffice.exe'	'4960,soffice.bin'
325	'4960,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
326	'6848,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
327	'6848,simpress.exe'	'6800,soffice.exe'
328	'6800,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
329	'6800,soffice.exe'	'3752,soffice.bin'
330	'3752,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
331	'4040,splwow64.exe'	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
332	'6348,SnippingTool.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
333	'6348,SnippingTool.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
334	'2576,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
335	'2576,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
336	'7172,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
337	'7172,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
338	'7352,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
339	'7352,firefox.exe'	'7832,pingsender.exe'
340	'7352,firefox.exe'	'7520,firefox.exe'
341	'7520,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
342	'7288,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
343	'7220,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
344	'8244,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
345	'8264,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
346	'8264,SearchFilterHost.exe'	'mlang.dll,C:Windowssystem32mlang.dll'
347	'8444,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
348	'8560,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
349	'8560,firefox.exe'	'8724,firefox.exe'
350	'8724,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

351	'360,XXX'	'368,csrss.exe'
352	'360,XXX'	'408,wininit.exe'
353	'368,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
354	'368,csrss.exe'	'9392,conhost.exe'
355	'408,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
356	'408,wininit.exe'	'508,services.exe'
357	'408,wininit.exe'	'532,lsm.exe'
358	'408,wininit.exe'	'524,lsass.exe'
359	'832,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
360	'832,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
361	'832,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
362	'832,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
363	'832,svchost.exe'	'USERENV.dll,C:WindowsSystem32USERENV.dll'
364	'832,svchost.exe'	'1004,audiodg.exe'
365	'832,svchost.exe'	'6192,audiodg.exe'
366	'832,svchost.exe'	'4464,audiodg.exe'
367	'888,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
368	'888,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
369	'888,svchost.exe'	'2248,dwm.exe'
370	'936,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
371	'936,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
372	'936,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
373	'936,svchost.exe'	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
374	'936,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
375	'936,svchost.exe'	'4760,WMIADAP.exe'
376	'384,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
377	'384,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
378	'384,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
379	'1028,svchost.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
380	'1220,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
381	'1252,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
382	'1252,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
383	'1372,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
384	'1372,svchost.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
385	'1372,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
386	'1400,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
387	'1868,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
388	'1608,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
389	'2008,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
390	'2240,userinit.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
391	'2240,userinit.exe'	'2272,explorer.exe'

392	'2248,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
393	'2272,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
394	'2272,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
395	'2272,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
396	'2272,explorer.exe'	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
397	'2272,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
398	'2272,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
399	'2272,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
400	'2272,explorer.exe'	'browcli.dll,C:Windowssystem32rowcli.dll'
401	'2272,explorer.exe'	'docprop.dll,C:Windowssystem32docprop.dll'
402	'2272,explorer.exe'	'sxproxy.dll,C:Windowssystem32sxproxy.dll'
403	'2272,explorer.exe'	'sbdrop.dll,C:Program FilesWindows Sidebarsbdrop.dll'
404	'2272,explorer.exe'	'2364,VBoxTray.exe'
405	'2272,explorer.exe'	'2372,MySQLNotifier.exe'
406	'2272,explorer.exe'	'2452,jusched.exe'
407	'2272,explorer.exe'	'1312,mintty.exe'
408	'2272,explorer.exe'	'2728,taskmgr.exe'
409	'2272,explorer.exe'	'3272,cmd.exe'
410	'2272,explorer.exe'	'3832,cmd.exe'
411	'2272,explorer.exe'	'3912,cmd.exe'
412	'2272,explorer.exe'	'3160,firefox.exe'
413	'2272,explorer.exe'	'4308,cmd.exe'
414	'2272,explorer.exe'	'4400,notepad++.exe'
415	'2272,explorer.exe'	'4440,Wireshark.exe'
416	'2272,explorer.exe'	'4808,FoxitReader.exe'
417	'2272,explorer.exe'	'4564,mintty.exe'
418	'2272,explorer.exe'	'6412,iexplore.exe'
419	'2272,explorer.exe'	'8592,soffice.exe'
420	'2364,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
421	'2372,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
422	'2452,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
423	'2452,jusched.exe'	'2800,win-firewall.exe'
424	'2464,XXX'	'2600,jusched.exe'
425	'2600,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
426	'2732,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
427	'2732,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
428	'2732,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
429	'2732,WmiPrvSE.exe'	'WMI.DLL,C:Windowssystem32WMI.DLL'
430	'2900,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
431	'2900,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'

432	'2900,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
433	'2900,SearchIndexer.exe'	'2988,SearchProtocolHost.exe'
434	'2900,SearchIndexer.exe'	'3008,SearchFilterHost.exe'
435	'2900,SearchIndexer.exe'	'5068,SearchProtocolHost.exe'
436	'2900,SearchIndexer.exe'	'3256,SearchFilterHost.exe'
437	'2900,SearchIndexer.exe'	'7080,SearchProtocolHost.exe'
438	'2900,SearchIndexer.exe'	'7100,SearchFilterHost.exe'
439	'2900,SearchIndexer.exe'	'6932,SearchProtocolHost.exe'
440	'2900,SearchIndexer.exe'	'6964,SearchFilterHost.exe'
441	'2900,SearchIndexer.exe'	'8380,SearchProtocolHost.exe'
442	'2900,SearchIndexer.exe'	'8404,SearchFilterHost.exe'
443	'2988,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
444	'3008,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
445	'1312,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
446	'2148,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
447	'2128,XXX'	'1124,bash.exe'
448	'1124,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
449	'2552,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
450	'2548,XXX'	'2624,driver_endpoint_netconn.exe'
451	'2624,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
452	'2728,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
453	'2728,taskmgr.exe'	'2864,taskmgr.exe'
454	'2800,win-firewall.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
455	'2264,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
456	'2332,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
457	'2864,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
458	'2864,taskmgr.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
459	'3272,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
460	'3272,cmd.exe'	'3388,java.exe'
461	'3284,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
462	'3388,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
463	'3388,java.exe'	'3768,java.exe'
464	'3564,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
465	'3564,svchost.exe'	'WS2_32.dll,C:Windowssystem32WS2_32.dll'
466	'3564,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'

467	'3564,svchost.exe'	'taskschd.dll,C:Windowssystem32askschd.dll'
468	'3768,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
469	'3776,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
470	'3832,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
471	'3840,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
472	'3912,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
473	'3912,cmd.exe'	'4024,java.exe'
474	'3920,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
475	'4024,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
476	'4024,java.exe'	'5204,java.exe'
477	'3160,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
478	'3160,firefox.exe'	'3548,firefox.exe'
479	'3160,firefox.exe'	'5576,simpress.exe'
480	'3160,firefox.exe'	'7660,firefox.exe'
481	'3548,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
482	'4308,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
483	'4308,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
484	'4308,cmd.exe'	'4332,NETSTAT.EXE'
485	'4316,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
486	'4332,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
487	'4332,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
488	'4400,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
489	'4440,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
490	'4440,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
491	'4440,Wireshark.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
492	'4440,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
493	'4440,Wireshark.exe'	'4584,dumpcap.exe'
494	'4440,Wireshark.exe'	'7032,dumpcap.exe'
495	'4584,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
496	'4592,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
497	'4760,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
498	'4760,WMIADAP.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
499	'4820,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
500	'4808,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
501	'5068,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
502	'3256,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
503	'4564,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
504	'4696,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
505	'4728,XXX'	'4732,bash.exe'
506	'4732,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'

507	'5576,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
508	'5576,simpress.exe'	'5600,soffice.exe'
509	'5600,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
510	'5600,soffice.exe'	'5612,soffice.bin'
511	'5612,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
512	'5960,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
513	'5204,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
514	'5508,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
515	'6412,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
516	'6412,iexplore.exe'	'6496,iexplore.exe'
517	'6412,iexplore.exe'	'7140,iexplore.exe'
518	'6412,iexplore.exe'	'6300,iexplore.exe'
519	'6496,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
520	'7032,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
521	'7040,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
522	'7080,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
523	'7100,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
524	'7140,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
525	'6300,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
526	'6932,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
527	'6964,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
528	'7660,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
529	'7228,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
530	'7652,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
531	'7956,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
532	'8380,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
533	'8380,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
534	'8404,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
535	'8404,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
536	'8592,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
537	'8592,soffice.exe'	'8600,soffice.bin'
538	'8600,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
539	'292,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
540	'632,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
541	'632,svchost.exe'	'2600,WmiPrvSE.exe'
542	'632,svchost.exe'	'1992,dllhost.exe'
543	'632,svchost.exe'	'2632,dllhost.exe'

544	'632,svchost.exe'	'4040,WmiPrvSE.exe'
545	'632,svchost.exe'	'4956,dllhost.exe'
546	'632,svchost.exe'	'7224,dllhost.exe'
547	'696,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
548	'760,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
549	'884,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
550	'884,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
551	'884,svchost.exe'	'2172,dwm.exe'
552	'932,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
553	'932,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
554	'932,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
555	'932,svchost.exe'	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
556	'932,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
557	'932,svchost.exe'	'mspatcha.dll,c:windowssystem32mspatcha.dll'
558	'932,svchost.exe'	'4012,WMIADAP.exe'
559	'364,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
560	'364,svchost.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
561	'1216,spoolsv.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
562	'1216,spoolsv.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
563	'1216,spoolsv.exe'	'9388,gswin32c.exe'
564	'1216,spoolsv.exe'	'9460,CPWSave.exe'
565	'1248,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
566	'1248,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
567	'1368,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
568	'1368,svchost.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
569	'1368,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
570	'1368,svchost.exe'	'upnphost.dll,c:windowssystem32upnphost.dll'
571	'1368,svchost.exe'	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
572	'1340,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
573	'1044,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
574	'2164,userinit.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
575	'2164,userinit.exe'	'2196,explorer.exe'
576	'2172,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
577	'2196,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
578	'2196,explorer.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
579	'2196,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
580	'2196,explorer.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
581	'2196,explorer.exe'	'mlang.dll,C:Windowssystem32mlang.dll'
582	'2196,explorer.exe'	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
583	'2196,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
584	'2196,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'

585	'2196,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
586	'2196,explorer.exe'	'browcli.dll,C:Windowssystem32rowcli.dll'
587	'2196,explorer.exe'	'sbdrop.dll,C:Program FilesWindows Sidebarsbdrop.dll'
588	'2196,explorer.exe'	'SearchFolder.dll,C:Windowssystem32SearchFolder.dll'
589	'2196,explorer.exe'	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
590	'2196,explorer.exe'	'puiobj.dll,C:Windowssystem32puiobj.dll'
591	'2196,explorer.exe'	'2284,VBoxTray.exe'
592	'2196,explorer.exe'	'2292,MySQLNotifier.exe'
593	'2196,explorer.exe'	'2356,jusched.exe'
594	'2196,explorer.exe'	'2368,win-firewall.exe'
595	'2196,explorer.exe'	'2952,mintty.exe'
596	'2196,explorer.exe'	'116,taskmgr.exe'
597	'2196,explorer.exe'	'3472,firefox.exe'
598	'2196,explorer.exe'	'3268,cmd.exe'
599	'2196,explorer.exe'	'4120,simpress.exe'
600	'2196,explorer.exe'	'4348,StikyNot.exe'
601	'2196,explorer.exe'	'5316,xpsrchvw.exe'
602	'2196,explorer.exe'	'7516,cmd.exe'
603	'2196,explorer.exe'	'7764,firefox.exe'
604	'2196,explorer.exe'	'7468,cmd.exe'
605	'2196,explorer.exe'	'7596,notepad++.exe'
606	'2196,explorer.exe'	'7460,Wireshark.exe'
607	'2196,explorer.exe'	'8528,FoxitReader.exe'
608	'2196,explorer.exe'	'8216,mintty.exe'
609	'2196,explorer.exe'	'8500,firefox.exe'
610	'2284,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
611	'2292,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
612	'2356,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
613	'2356,jusched.exe'	'2032,jucheck.exe'
614	'2368,win-firewall.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
615	'2380,XXX'	'2484,jusched.exe'
616	'2484,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
617	'2600,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
618	'2600,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
619	'2952,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
620	'2996,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
621	'3012,XXX'	'3028,bash.exe'
622	'3028,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
623	'1084,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
624	'1084,SearchIndexer.exe'	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'

625	'1084,SearchIndexer.exe'	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
626	'1084,SearchIndexer.exe'	'NLSLexicons0010.dll,C:WindowsSystem32NLSLexicons0010.dll'
627	'1084,SearchIndexer.exe'	'2252,SearchProtocolHost.exe'
628	'1084,SearchIndexer.exe'	'2440,SearchFilterHost.exe'
629	'1084,SearchIndexer.exe'	'4408,SearchProtocolHost.exe'
630	'1084,SearchIndexer.exe'	'4428,SearchFilterHost.exe'
631	'1084,SearchIndexer.exe'	'4468,SearchProtocolHost.exe'
632	'1084,SearchIndexer.exe'	'5928,SearchProtocolHost.exe'
633	'1084,SearchIndexer.exe'	'5948,SearchFilterHost.exe'
634	'1084,SearchIndexer.exe'	'4900,SearchProtocolHost.exe'
635	'1084,SearchIndexer.exe'	'5156,SearchFilterHost.exe'
636	'1084,SearchIndexer.exe'	'6684,SearchProtocolHost.exe'
637	'1084,SearchIndexer.exe'	'6704,SearchFilterHost.exe'
638	'1084,SearchIndexer.exe'	'8728,SearchProtocolHost.exe'
639	'1084,SearchIndexer.exe'	'8748,SearchFilterHost.exe'
640	'1084,SearchIndexer.exe'	'9748,SearchProtocolHost.exe'
641	'1084,SearchIndexer.exe'	'9780,SearchFilterHost.exe'
642	'2252,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
643	'2440,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
644	'2420,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
645	'2420,wmpnetwk.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
646	'1096,XXX'	'3056,driver_endpoint_netconn.exe'
647	'3056,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
648	'116,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
649	'116,taskmgr.exe'	'2112,taskmgr.exe'
650	'2032,jucheck.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
651	'1992,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
652	'2632,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
653	'2112,taskmgr.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
654	'2112,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
655	'3296,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
656	'3296,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'

657	'3296,svchost.exe'	tdh.dll,C:WindowsSystem32dh.dll'
658	'3472,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
659	'3472,firefox.exe'	'3668,firefox.exe'
660	'3472,firefox.exe'	'7324,pingsender.exe'
661	'3472,firefox.exe'	'6416,firefox.exe'
662	'3668,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
663	'4012,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
664	'4012,WMIADAP.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
665	'4040,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
666	'3268,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
667	'3280,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
668	'4120,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
669	'4120,simpress.exe'	'4128,soffice.exe'
670	'4128,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
671	'4128,soffice.exe'	'4136,soffice.bin'
672	'4136,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
673	'4348,StikyNot.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
674	'4408,SearchProtocolHost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
675	'4408,SearchProtocolHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
676	'4428,SearchFilterHost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
677	'4428,SearchFilterHost.exe'	'rtffilt.dll,C:Windowssystem32rtffilt.dll'
678	'4468,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
679	'4956,dllhost.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
680	'4956,dllhost.exe'	'gdiplus.dll,C:WindowsWinSxSamd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437agdiplus.dll'
681	'5232,XXX'	'5256,setup_wm.exe'
682	'5256,setup_wm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
683	'5256,setup_wm.exe'	'5412,wmplayer.exe'
684	'5412,wmplayer.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
685	'5928,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
686	'5928,SearchProtocolHost.exe'	'ehtrace.dll,C:Windowsehomeehtrace.dll'
687	'5948,SearchFilterHost.exe'	'mlang.dll,C:Windowssystem32mlang.dll'
688	'5948,SearchFilterHost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
689	'4900,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
690	'5156,SearchFilterHost.exe'	'ksuser.dll,C:WindowsSystem32ksuser.dll'
691	'5316,xpsrchvw.exe'	tiptsf.dll,C:Program FilesCommon Filesmicrosoft sharedinkiptsf.dll'

692	'6684,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
693	'6704,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
694	'6416,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
695	'7224,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
696	'7516,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
697	'7516,cmd.exe'	'7636,java.exe'
698	'7524,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
699	'7636,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
700	'7636,java.exe'	'9936,java.exe'
701	'7764,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
702	'7764,firefox.exe'	'7928,firefox.exe'
703	'7764,firefox.exe'	'8968,simpress.exe'
704	'7928,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
705	'7468,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
706	'7468,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
707	'7468,cmd.exe'	'7508,NETSTAT.EXE'
708	'7476,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
709	'7508,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
710	'7508,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
711	'7596,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
712	'7596,notepad++.exe'	'9304,splwow64.exe'
713	'7460,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
714	'7460,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
715	'7460,Wireshark.exe'	'8240,dumpcap.exe'
716	'7460,Wireshark.exe'	'10192,dumpcap.exe'
717	'8240,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
718	'8248,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
719	'8528,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
720	'8728,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
721	'8748,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
722	'8216,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
723	'8288,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
724	'8312,XXX'	'8328,bash.exe'
725	'8328,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
726	'8968,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
727	'8968,simpress.exe'	'9092,soffice.exe'
728	'9092,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
729	'9092,soffice.exe'	'9052,soffice.bin'
730	'9052,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
731	'8948,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'

732	'9936,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
733	'9944,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
734	'9304,splwow64.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
735	'9460,CPWSave.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
736	'9460,CPWSave.exe'	'9468,CPWSave.exe'
737	'9468,CPWSave.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
738	'9748,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
739	'9780,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
740	'10192,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
741	'10216,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'

7.2.13 Proteus Malware – Instance 1

Table 119: Proteus Malware Instance 1 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'356,XXX'
6	'364,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'416,XXX'
9	'428,csrss.exe'
10	'404,wininit.exe'
11	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
12	'464,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'512,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'528,lsm.exe'
17	'520,lsass.exe'
18	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
19	'wkscli.dll,C:Windowssystem32wkscli.dll'
20	'624,svchost.exe'
21	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
22	'688,VBoxService.exe'
23	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
24	'752,svchost.exe'
25	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
26	'840,svchost.exe'
27	'netutils.dll,C:WindowsSystem32netutils.dll'
28	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
29	'winrnr.dll,C:WindowsSystem32winrnr.dll'
30	'888,svchost.exe'
31	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
32	'928,svchost.exe'
33	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
34	'rasman.dll,C:Windowssystem32rasman.dll'
35	'AVRT.dll,c:windowssystem32AVRT.dll'
36	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'

37	'360,svchost.exe'
38	'dsrole.dll,C:Windowssystem32dsrole.dll'
39	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
40	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
41	'736,svchost.exe'
42	'SensApi.dll,C:Windowssystem32SensApi.dll'
43	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
44	'1144,spoolsv.exe'
45	'1192,svchost.exe'
46	'1344,svchost.exe'
47	'SXS.DLL,C:Windowssystem32SXS.DLL'
48	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
49	'1416,FoxitConnectedPDFService.exe'
50	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
51	'1916,svchost.exe'
52	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
53	'1668,sppsvc.exe'
54	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
55	'1900,svchost.exe'
56	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
57	'1856,SearchIndexer.exe'
58	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
59	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
60	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
61	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
62	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
63	'1044,taskhost.exe'
64	'midimap.dll,C:Windowssystem32midimap.dll'
65	'2184,dwm.exe'
66	'2168,XXX'
67	'2204,explorer.exe'
68	'MLANG.dll,C:Windowssystem32MLANG.dll'
69	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
70	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
71	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
72	tquery.dll,C:Windowssystem32query.dll'
73	'docprop.dll,C:Windowssystem32docprop.dll'
74	'sxproxy.dll,C:Windowssystem32sxproxy.dll'
75	'fdWNet.dll,C:Windowssystem32fdWNet.dll'

76	'shacct.dll,C:WindowsSystem32shacct.dll'
77	'2292,VBoxTray.exe'
78	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
79	'2300,MySQLNotifier.exe'
80	'2564,WmiPrvSE.exe'
81	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
82	'SECUR32.DLL,C:Windowssystem32SECUR32.DLL'
83	'perfos.dll,C:WindowsSystem32perfos.dll'
84	'2320,XXX'
85	'2576,jusched.exe'
86	'2920,wmpnetwk.exe'
87	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
88	'provsvc.dll,C:WindowsSystem32provsvc.dll'
89	'iertutil.dll,C:Windowssystem32iertutil.dll'
90	'2040,XXX'
91	'2464,taskmgr.exe'
92	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
93	'DUser.dll,C:Windowssystem32DUser.dll'
94	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
95	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
96	'3868,mintty.exe'
97	'apphelp.dll,C:Windowssystem32apphelp.dll'
98	'3920,conhost.exe'
99	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
100	'3708,audiodg.exe'
101	'3940,XXX'
102	'3956,bash.exe'
103	'authz.dll,C:Windowssystem32authz.dll'
104	'2664,XXX'
105	'3664,driver_endpoint_netconn.exe'
106	'3356,cmd.exe'
107	'3324,conhost.exe'
108	'996,java.exe'
109	'2504,java.exe'
110	'3900,firefox.exe'
111	'2840,firefox.exe'
112	'3620,cmd.exe'
113	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
114	'3304,conhost.exe'
115	'3628,NETSTAT.EXE'
116	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'

117	'1092,notepad++.exe'
118	'2436,Wireshark.exe'
119	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
120	'DUI70.dll,C:Windowssystem32DUI70.dll'
121	'2844,conhost.exe'
122	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
123	'3888,dumpcap.exe'
124	'3764,FoxitReader.exe'
125	'3232,FoxitReaderUpdater.exe'
126	'4124,SearchProtocolHost.exe'
127	'4144,SearchFilterHost.exe'
128	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
129	'4540,mintty.exe'
130	'4576,conhost.exe'
131	'4592,XXX'
132	'4608,bash.exe'
133	'4732,simpress.exe'
134	'4780,soffice.exe'
135	'4720,soffice.bin'
136	'4312,svchost.exe'
137	'6012,java.exe'
138	'6024,conhost.exe'
139	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
140	'5280,SearchProtocolHost.exe'
141	'profapi.dll,C:Windowssystem32profapi.dll'
142	'5300,SearchFilterHost.exe'
143	'5644,pingsender.exe'
144	'5656,conhost.exe'
145	'5840,dumpcap.exe'
146	'5848,conhost.exe'
147	'6316,audiodg.exe'
148	'6400,dllhost.exe'
149	'6580,dllhost.exe'
150	'6628,consent.exe'
151	'6732,dllhost.exe'
152	'IDStore.dll,C:WindowsSystem32IDStore.dll'
153	'6768,dllhost.exe'
154	'6804,gchrome.exe'
155	'6876,chrome.exe'
156	'6932,SearchProtocolHost.exe'
157	'6956,SearchFilterHost.exe'

158	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
159	'7000,chrome.exe'
160	'7068,chrome.exe'
161	'7964,audiodg.exe'
162	'6436,firefox.exe'
163	'7336,firefox.exe'
164	'6332,plugin-container.exe'
165	'8008,FlashPlayerPlugin_22_0_0_209.exe'
166	'8020,FlashPlayerPlugin_22_0_0_209.exe'
167	'8352,slui.exe'
168	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
169	'8768,dllhost.exe'
170	'8944,svchost.exe'
171	'10620,audiodg.exe'
172	'9032,soffice.exe'
173	'9040,soffice.bin'
174	'9976,soffice.exe'
175	'9008,taskhost.exe'
176	'9880,cmd.exe'
177	'9888,conhost.exe'
178	'9984,soffice.bin'
179	'10228,firefox.exe'
180	'10256,firefox.exe'
181	'10900,WmiPrvSE.exe'
182	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
183	'11588,dllhost.exe'
184	'13024,dllhost.exe'
185	'13224,dllhost.exe'
186	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
187	'12380,XXX'
188	'12372,setup_wm.exe'
189	'12572,wmplayer.exe'
190	'13196,SearchProtocolHost.exe'
191	'slc.dll,C:Windowssystem32slc.dll'
192	'ehtrace.dll,C:Windowsehomeehtrace.dll'
193	'13260,SearchFilterHost.exe'
194	'msxml6.dll,C:WindowsSystem32msxml6.dll'
195	'13720,slui.exe'
196	'12504,firefox.exe'
197	'13360,firefox.exe'
198	'13800,rundll32.exe'

199	'13844,notepad++.exe'
200	'13960,dllhost.exe'
201	'14260,SearchProtocolHost.exe'
202	'14292,SearchFilterHost.exe'
203	'13836,cmd.exe'
204	'13884,conhost.exe'
205	'14228,java.exe'
206	'14432,firefox.exe'
207	'14600,firefox.exe'
208	'15144,cmd.exe'
209	'15152,conhost.exe'
210	'15172,NETSTAT.EXE'
211	'15228,notepad++.exe'
212	'15276,Wireshark.exe'
213	'15308,dumpcap.exe'
214	'msimtf.dll,C:Windowssystem32msimtf.dll'
215	'15056,dumpcap.exe'
216	'15100,conhost.exe'
217	'15808,FoxitReader.exe'
218	'16336,mintty.exe'
219	'16372,conhost.exe'
220	'14520,XXX'
221	'14920,bash.exe'
222	'15676,simpress.exe'
223	'15700,soffice.exe'
224	'15712,soffice.bin'
225	'16736,java.exe'
226	'16716,conhost.exe'
227	'16776,SearchProtocolHost.exe'
228	'17076,SearchFilterHost.exe'
229	'16528,conhost.exe'
230	'17248,dumpcap.exe'
231	'17612,taskhost.exe'
232	'17732,FoxitReader.exe'
233	'17888,SearchProtocolHost.exe'
234	'17908,SearchFilterHost.exe'
235	'13148,conhost.exe'
236	'18040,firefox.exe'
237	'17544,pingsender.exe'
238	'18208,firefox.exe'
239	'17956,firefox.exe'

240	'18564,firefox.exe'
241	'18824,iexplore.exe'
242	'18860,taskmgr.exe'
243	'18940,iexplore.exe'
244	'19248,dllhost.exe'
245	'19288,dllhost.exe'
246	'19320,taskmgr.exe'
247	'19664,audiodg.exe'
248	'19588,SearchProtocolHost.exe'
249	'19612,SearchFilterHost.exe'
250	'20436,iexplore.exe'
251	'19700,slui.exe'
252	'19980,iexplore.exe'
253	'20904,SearchProtocolHost.exe'
254	'20924,SearchFilterHost.exe'

Table 120: Proteus Malware Instance 1 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'356,XXX'	'364,csrss.exe'
5	'356,XXX'	'404,wininit.exe'
6	'364,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'416,XXX'	'428,csrss.exe'
8	'416,XXX'	'464,winlogon.exe'
9	'428,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
10	'428,csrss.exe'	'3920,conhost.exe'
11	'428,csrss.exe'	'3324,conhost.exe'
12	'428,csrss.exe'	'3304,conhost.exe'
13	'428,csrss.exe'	'2844,conhost.exe'
14	'428,csrss.exe'	'4576,conhost.exe'
15	'428,csrss.exe'	'6024,conhost.exe'
16	'428,csrss.exe'	'5656,conhost.exe'
17	'428,csrss.exe'	'5848,conhost.exe'
18	'428,csrss.exe'	'9888,conhost.exe'
19	'428,csrss.exe'	'13884,conhost.exe'
20	'428,csrss.exe'	'15152,conhost.exe'
21	'428,csrss.exe'	'15100,conhost.exe'
22	'428,csrss.exe'	'16372,conhost.exe'
23	'428,csrss.exe'	'16716,conhost.exe'
24	'428,csrss.exe'	'16528,conhost.exe'
25	'428,csrss.exe'	'13148,conhost.exe'
26	'404,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
27	'404,wininit.exe'	'512,services.exe'
28	'404,wininit.exe'	'528,lsm.exe'
29	'404,wininit.exe'	'520,lsass.exe'
30	'464,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
31	'512,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
32	'512,services.exe'	'624,svchost.exe'
33	'512,services.exe'	'688,VBoxService.exe'
34	'512,services.exe'	'752,svchost.exe'
35	'512,services.exe'	'840,svchost.exe'
36	'512,services.exe'	'888,svchost.exe'
37	'512,services.exe'	'928,svchost.exe'
38	'512,services.exe'	'360,svchost.exe'
39	'512,services.exe'	'736,svchost.exe'

40	'512,services.exe'	'1144,spoolsv.exe'
41	'512,services.exe'	'1192,svchost.exe'
42	'512,services.exe'	'1344,svchost.exe'
43	'512,services.exe'	'1416,FoxitConnectedPDFService.exe'
44	'512,services.exe'	'1916,svchost.exe'
45	'512,services.exe'	'1668,sppsvc.exe'
46	'512,services.exe'	'1900,svchost.exe'
47	'512,services.exe'	'1856,SearchIndexer.exe'
48	'512,services.exe'	'1044,taskhost.exe'
49	'512,services.exe'	'2920,wmpnetwk.exe'
50	'512,services.exe'	'4312,svchost.exe'
51	'512,services.exe'	'8944,svchost.exe'
52	'512,services.exe'	'9008,taskhost.exe'
53	'512,services.exe'	'17612,taskhost.exe'
54	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
55	'520,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
56	'520,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
57	'624,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
58	'624,svchost.exe'	'2564,WmiPrvSE.exe'
59	'624,svchost.exe'	'6400,dllhost.exe'
60	'624,svchost.exe'	'6580,dllhost.exe'
61	'624,svchost.exe'	'6732,dllhost.exe'
62	'624,svchost.exe'	'6768,dllhost.exe'
63	'624,svchost.exe'	'8352,slui.exe'
64	'624,svchost.exe'	'8768,dllhost.exe'
65	'624,svchost.exe'	'10900,WmiPrvSE.exe'
66	'624,svchost.exe'	'11588,dllhost.exe'
67	'624,svchost.exe'	'13024,dllhost.exe'
68	'624,svchost.exe'	'13224,dllhost.exe'
69	'624,svchost.exe'	'13720,slui.exe'
70	'624,svchost.exe'	'13960,dllhost.exe'
71	'624,svchost.exe'	'19248,dllhost.exe'
72	'624,svchost.exe'	'19288,dllhost.exe'
73	'624,svchost.exe'	'19700,slui.exe'
74	'688,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
75	'752,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
76	'840,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
77	'840,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
78	'840,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
79	'840,svchost.exe'	'3708,audiodg.exe'
80	'840,svchost.exe'	'6316,audiodg.exe'

81	'840,svchost.exe'	'7964,audiodg.exe'
82	'840,svchost.exe'	'10620,audiodg.exe'
83	'840,svchost.exe'	'19664,audiodg.exe'
84	'888,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
85	'888,svchost.exe'	'2184,dwm.exe'
86	'928,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
87	'928,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
88	'928,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
89	'928,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
90	'928,svchost.exe'	'6628,consent.exe'
91	'360,svchost.exe'	'dsrole.dll,C:Windowssystem32dsrole.dll'
92	'360,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
93	'360,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
94	'736,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
95	'736,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
96	'1144,spoolsv.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
97	'1192,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
98	'1344,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
99	'1344,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
100	'1344,svchost.exe'	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
101	'1416,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
102	'1916,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
103	'1668,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
104	'1900,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
105	'1856,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
106	'1856,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
107	'1856,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
108	'1856,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
109	'1856,SearchIndexer.exe'	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
110	'1856,SearchIndexer.exe'	'4124,SearchProtocolHost.exe'
111	'1856,SearchIndexer.exe'	'4144,SearchFilterHost.exe'
112	'1856,SearchIndexer.exe'	'5280,SearchProtocolHost.exe'
113	'1856,SearchIndexer.exe'	'5300,SearchFilterHost.exe'
114	'1856,SearchIndexer.exe'	'6932,SearchProtocolHost.exe'
115	'1856,SearchIndexer.exe'	'6956,SearchFilterHost.exe'
116	'1856,SearchIndexer.exe'	'13196,SearchProtocolHost.exe'
117	'1856,SearchIndexer.exe'	'13260,SearchFilterHost.exe'
118	'1856,SearchIndexer.exe'	'14260,SearchProtocolHost.exe'
119	'1856,SearchIndexer.exe'	'14292,SearchFilterHost.exe'

120	'1856,SearchIndexer.exe'	'16776,SearchProtocolHost.exe'
121	'1856,SearchIndexer.exe'	'17076,SearchFilterHost.exe'
122	'1856,SearchIndexer.exe'	'17888,SearchProtocolHost.exe'
123	'1856,SearchIndexer.exe'	'17908,SearchFilterHost.exe'
124	'1856,SearchIndexer.exe'	'19588,SearchProtocolHost.exe'
125	'1856,SearchIndexer.exe'	'19612,SearchFilterHost.exe'
126	'1856,SearchIndexer.exe'	'20904,SearchProtocolHost.exe'
127	'1856,SearchIndexer.exe'	'20924,SearchFilterHost.exe'
128	'1044,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
129	'2184,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
130	'2168,XXX'	'2204,explorer.exe'
131	'2204,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
132	'2204,explorer.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
133	'2204,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
134	'2204,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
135	'2204,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
136	'2204,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
137	'2204,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
138	'2204,explorer.exe'	'docprop.dll,C:Windowssystem32docprop.dll'
139	'2204,explorer.exe'	'sxproxy.dll,C:Windowssystem32sxproxy.dll'
140	'2204,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
141	'2204,explorer.exe'	'shacct.dll,C:WindowsSystem32shacct.dll'
142	'2204,explorer.exe'	'2292,VBoxTray.exe'
143	'2204,explorer.exe'	'2300,MySQLNotifier.exe'
144	'2204,explorer.exe'	'3868,mintty.exe'
145	'2204,explorer.exe'	'3356,cmd.exe'
146	'2204,explorer.exe'	'3900,firefox.exe'
147	'2204,explorer.exe'	'3620,cmd.exe'
148	'2204,explorer.exe'	'1092,notepad++.exe'
149	'2204,explorer.exe'	'2436,Wireshark.exe'
150	'2204,explorer.exe'	'3764,FoxitReader.exe'
151	'2204,explorer.exe'	'4540,mintty.exe'
152	'2204,explorer.exe'	'6804,gchrome.exe'
153	'2204,explorer.exe'	'6436,firefox.exe'
154	'2204,explorer.exe'	'9032,soffice.exe'
155	'2204,explorer.exe'	'9976,soffice.exe'
156	'2204,explorer.exe'	'9880,cmd.exe'
157	'2204,explorer.exe'	'10228,firefox.exe'
158	'2204,explorer.exe'	'12504,firefox.exe'
159	'2204,explorer.exe'	'13800,rundll32.exe'
160	'2204,explorer.exe'	'13844,notepad++.exe'

161	'2204,explorer.exe'	'13836,cmd.exe'
162	'2204,explorer.exe'	'14432,firefox.exe'
163	'2204,explorer.exe'	'15144,cmd.exe'
164	'2204,explorer.exe'	'15228,notepad++.exe'
165	'2204,explorer.exe'	'15276,Wireshark.exe'
166	'2204,explorer.exe'	'15808,FoxitReader.exe'
167	'2204,explorer.exe'	'16336,mintty.exe'
168	'2204,explorer.exe'	'17732,FoxitReader.exe'
169	'2204,explorer.exe'	'18040,firefox.exe'
170	'2204,explorer.exe'	'17956,firefox.exe'
171	'2204,explorer.exe'	'18824,iexplore.exe'
172	'2204,explorer.exe'	'18860,taskmgr.exe'
173	'2292,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
174	'2300,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
175	'2564,WmiPrvSE.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
176	'2564,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
177	'2564,WmiPrvSE.exe'	'SECUR32.DLL,C:Windowssystem32SECUR32.DLL'
178	'2564,WmiPrvSE.exe'	'perfos.dll,C:WindowsSystem32perfos.dll'
179	'2320,XXX'	'2576,jusched.exe'
180	'2576,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
181	'2920,wmpnetwk.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
182	'2920,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
183	'2920,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
184	'2920,wmpnetwk.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
185	'2040,XXX'	'2464,taskmgr.exe'
186	'2464,taskmgr.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
187	'2464,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
188	'2464,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
189	'2464,taskmgr.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
190	'2464,taskmgr.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
191	'3868,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
192	'3920,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
193	'3940,XXX'	'3956,bash.exe'
194	'3956,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
195	'2664,XXX'	'3664,driver_endpoint_netconn.exe'
196	'3664,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
197	'3356,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
198	'3356,cmd.exe'	'996,java.exe'
199	'3356,cmd.exe'	'2504,java.exe'
200	'3324,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
201	'2504,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

202	'2504,java.exe'	'6012,java.exe'
203	'3900,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
204	'3900,firefox.exe'	'2840,firefox.exe'
205	'3900,firefox.exe'	'4732,simpress.exe'
206	'3900,firefox.exe'	'5644,pingsender.exe'
207	'2840,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
208	'3620,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
209	'3620,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
210	'3620,cmd.exe'	'3628,NETSTAT.EXE'
211	'3304,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
212	'3628,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
213	'3628,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
214	'1092,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
215	'2436,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
216	'2436,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
217	'2436,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
218	'2436,Wireshark.exe'	'DUI70.dll,C:Windowssystem32DUI70.dll'
219	'2436,Wireshark.exe'	'3888,dumpcap.exe'
220	'2436,Wireshark.exe'	'5840,dumpcap.exe'
221	'2844,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
222	'3888,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
223	'3764,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
224	'3764,FoxitReader.exe'	'3232,FoxitReaderUpdater.exe'
225	'3232,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
226	'4124,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
227	'4144,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
228	'4540,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
229	'4576,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
230	'4592,XXX'	'4608,bash.exe'
231	'4608,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
232	'4732,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
233	'4732,simpress.exe'	'4780,soffice.exe'
234	'4780,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
235	'4780,soffice.exe'	'4720,soffice.bin'
236	'4720,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
237	'4312,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
238	'6012,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
239	'6024,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
240	'5280,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
241	'5300,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
242	'5644,pingsender.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

243	'5656,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
244	'5840,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
245	'5848,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
246	'6400,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
247	'6580,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
248	'6628,consent.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
249	'6732,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
250	'6768,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
251	'6804,gchrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
252	'6804,gchrome.exe'	'6876,chrome.exe'
253	'6876,chrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
254	'6876,chrome.exe'	'7000,chrome.exe'
255	'6876,chrome.exe'	'7068,chrome.exe'
256	'6932,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
257	'6956,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
258	'7000,chrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
259	'7068,chrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
260	'6436,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
261	'6436,firefox.exe'	'7336,firefox.exe'
262	'6436,firefox.exe'	'6332,plugin-container.exe'
263	'7336,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
264	'6332,plugin-container.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
265	'6332,plugin-container.exe'	'8008,FlashPlayerPlugin_22_0_0_209.exe'
266	'8008,FlashPlayerPlugin_22_0_0_209.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
267	'8008,FlashPlayerPlugin_22_0_0_209.exe'	'8020,FlashPlayerPlugin_22_0_0_209.exe'
268	'8020,FlashPlayerPlugin_22_0_0_209.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
269	'8352,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
270	'8768,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
271	'8944,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
272	'9032,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
273	'9032,soffice.exe'	'9040,soffice.bin'
274	'9040,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
275	'9976,soffice.exe'	'9984,soffice.bin'
276	'9008,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
277	'9880,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
278	'9888,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
279	'10228,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
280	'10228,firefox.exe'	'10256,firefox.exe'
281	'10256,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

282	'10900,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
283	'11588,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
284	'13024,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
285	'13224,dllhost.exe'	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
286	'12380,XXX'	'12372,setup_wm.exe'
287	'12372,setup_wm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
288	'12372,setup_wm.exe'	'12572,wmplayer.exe'
289	'12572,wmplayer.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
290	'13196,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
291	'13196,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
292	'13196,SearchProtocolHost.exe'	'ehtrace.dll,C:Windowsehomeehtrace.dll'
293	'13260,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
294	'13260,SearchFilterHost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
295	'12504,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
296	'12504,firefox.exe'	'13360,firefox.exe'
297	'13360,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
298	'13800,rundll32.exe'	'slc.dll,C:Windowssystem32slc.dll'
299	'13844,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
300	'13960,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
301	'14260,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
302	'14292,SearchFilterHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
303	'13836,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
304	'13836,cmd.exe'	'14228,java.exe'
305	'13884,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
306	'14228,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
307	'14228,java.exe'	'16736,java.exe'
308	'14432,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
309	'14432,firefox.exe'	'14600,firefox.exe'
310	'14432,firefox.exe'	'15676,simpress.exe'
311	'14600,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
312	'15144,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
313	'15144,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
314	'15144,cmd.exe'	'15172,NETSTAT.EXE'
315	'15152,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
316	'15172,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
317	'15172,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
318	'15228,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
319	'15276,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
320	'15276,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
321	'15276,Wireshark.exe'	'15308,dumpcap.exe'
322	'15276,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'

323	'15276,Wireshark.exe'	'15056,dumpcap.exe'
324	'15276,Wireshark.exe'	'17248,dumpcap.exe'
325	'15056,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
326	'15100,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
327	'15808,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
328	'16336,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
329	'16372,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
330	'14520,XXX'	'14920,bash.exe'
331	'14920,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
332	'15676,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
333	'15676,simpress.exe'	'15700,soffice.exe'
334	'15700,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
335	'15700,soffice.exe'	'15712,soffice.bin'
336	'15712,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
337	'16736,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
338	'16716,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
339	'16776,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
340	'17076,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
341	'16528,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
342	'17248,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
343	'17612,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
344	'17732,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
345	'17888,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
346	'17888,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
347	'17908,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
348	'17908,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
349	'18040,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
350	'18040,firefox.exe'	'17544,pingsender.exe'
351	'18040,firefox.exe'	'18208,firefox.exe'
352	'18208,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
353	'17956,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
354	'17956,firefox.exe'	'18564,firefox.exe'
355	'18564,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
356	'18824,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
357	'18824,iexplore.exe'	'18940,iexplore.exe'
358	'18824,iexplore.exe'	'20436,iexplore.exe'
359	'18824,iexplore.exe'	'19980,iexplore.exe'
360	'18860,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
361	'18860,taskmgr.exe'	'19320,taskmgr.exe'
362	'18940,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
363	'19248,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'

364	'19288,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
365	'19320,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
366	'19588,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
367	'19612,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
368	'20436,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
369	'19700,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
370	'19980,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
371	'20904,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
372	'20924,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'

7.2.14 Proteus Malware – Instance 2

Table 121: Proteus Malware Instance 2 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,XXX'
6	'360,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'412,XXX'
9	'424,csrss.exe'
10	'400,wininit.exe'
11	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'504,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'528,lsm.exe'
17	'520,lsass.exe'
18	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
19	'628,svchost.exe'
20	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
21	'692,VBoxService.exe'
22	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
23	'756,svchost.exe'
24	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
25	'840,svchost.exe'
26	'netutils.dll,C:WindowsSystem32netutils.dll'
27	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
28	'888,svchost.exe'
29	'credssp.dll,C:WindowsSystem32credssp.dll'
30	'996,audiodg.exe'
31	'928,svchost.exe'
32	'MPR.dll,C:Windowssystem32MPR.dll'
33	'qmgrprxy.dll,C:Windowssystem32qmgrprxy.dll'
34	'AVRT.dll,c:windowssystem32AVRT.dll'
35	'tschannel.dll,C:Windowssystem32schannel.dll'

36	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
37	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
38	'328,svchost.exe'
39	'dsrole.dll,C:Windowssystem32dsrole.dll'
40	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
41	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
42	'740,svchost.exe'
43	'SensApi.dll,C:Windowssystem32SensApi.dll'
44	'1196,spoolsv.exe'
45	'1224,svchost.exe'
46	'1364,svchost.exe'
47	'SXS.DLL,C:Windowssystem32SXS.DLL'
48	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
49	'1388,FoxitConnectedPDFService.exe'
50	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
51	'1860,svchost.exe'
52	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
53	'1304,taskhost.exe'
54	'midimap.dll,C:Windowssystem32midimap.dll'
55	'924,dwm.exe'
56	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
57	'1276,XXX'
58	'212,explorer.exe'
59	'msi.dll,C:Windowssystem32msi.dll'
60	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
61	tquery.dll,C:Windowssystem32query.dll'
62	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
63	'MLANG.dll,C:Windowssystem32MLANG.dll'
64	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
65	'MsftEdit.dll,C:Windowssystem32MsftEdit.dll'
66	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
67	'2096,VBoxTray.exe'
68	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
69	'2112,MySQLNotifier.exe'
70	'2132,XXX'
71	'2212,jusched.exe'
72	'2388,WmiPrvSE.exe'
73	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
74	'perfos.dll,C:WindowsSystem32perfos.dll'
75	'SECUR32.DLL,C:Windowssystem32SECUR32.DLL'
76	'2572,SearchIndexer.exe'

77	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
78	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
79	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
80	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
81	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
82	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
83	'2800,wmpnetwk.exe'
84	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
85	'iertutil.dll,C:Windowssystem32iertutil.dll'
86	'provsvc.dll,C:WindowsSystem32provsvc.dll'
87	'124,sppsvc.exe'
88	'2260,svchost.exe'
89	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
90	'3388,WmiPrvSE.exe'
91	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
92	'3192,XXX'
93	'3064,taskmgr.exe'
94	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
95	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
96	'DUser.dll,C:Windowssystem32DUser.dll'
97	'3780,mintty.exe'
98	'apphelp.dll,C:Windowssystem32apphelp.dll'
99	'3220,conhost.exe'
100	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
101	'3876,XXX'
102	'3608,bash.exe'
103	'authz.dll,C:Windowssystem32authz.dll'
104	'1816,XXX'
105	'1872,driver_endpoint_netconn.exe'
106	'10184,audiodg.exe'
107	'1592,taskeng.exe'
108	'1180,GoogleUpdate.exe'
109	'2232,GoogleUpdate.exe'
110	'3696,GoogleUpdate.exe'
111	'3244,msiexec.exe'
112	'3924,GoogleUpdate.exe'
113	'2164,cmd.exe'
114	'3952,conhost.exe'
115	'784,java.exe'
116	'1328,java.exe'
117	'3092,firefox.exe'

118	'3580,firefox.exe'
119	'4136,cmd.exe'
120	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
121	'4144,conhost.exe'
122	'4168,NETSTAT.EXE'
123	'winrnr.dll,C:WindowsSystem32winrnr.dll'
124	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
125	'4240,notepad++.exe'
126	'4268,Wireshark.exe'
127	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
128	'4408,dumpcap.exe'
129	'4416,conhost.exe'
130	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
131	'4964,taskhost.exe'
132	'4884,FoxitReader.exe'
133	'4924,FoxitReaderUpdater.exe'
134	'4264,SearchProtocolHost.exe'
135	'4304,SearchFilterHost.exe'
136	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
137	'5100,mintty.exe'
138	'4468,conhost.exe'
139	'4504,XXX'
140	'4512,bash.exe'
141	'5440,simpress.exe'
142	'5452,soffice.exe'
143	'5460,soffice.bin'
144	'5416,audiodg.exe'
145	'5724,firefox.exe'
146	'5620,java.exe'
147	'5344,conhost.exe'
148	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
149	'5568,dllhost.exe'
150	'6868,svchost.exe'
151	'7124,SearchProtocolHost.exe'
152	'profapi.dll,C:Windowssystem32profapi.dll'
153	'7144,SearchFilterHost.exe'
154	'6908,consent.exe'
155	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
156	'6548,dllhost.exe'
157	'7076,dllhost.exe'
158	'IDStore.dll,C:WindowsSystem32IDStore.dll'

159	'7080,dllhost.exe'
160	'6332,gchrome.exe'
161	'7024,chrome.exe'
162	'6848,chrome.exe'
163	'6800,chrome.exe'
164	'6576,dumpcap.exe'
165	'6788,conhost.exe'
166	'7400,chrome.exe'
167	'7412,chrome.exe'
168	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
169	'LINKINFO.dll,C:Windowssystem32LINKINFO.dll'
170	'cryptnet.dll,C:Windowssystem32cryptnet.dll'
171	'imagehlp.dll,C:Windowssystem32imagehlp.dll'
172	'7444,chrome.exe'
173	'7560,chrome.exe'
174	'7628,chrome.exe'
175	'7644,chrome.exe'
176	'7772,chrome.exe'
177	'libegl.dll,C:Program Files (x86)GoogleChromeApplication61.0.3163.100swiftshaderlibegl.dll'
178	'7980,dllhost.exe'
179	'8244,chrome.exe'
180	'8392,SearchProtocolHost.exe'
181	'8416,SearchFilterHost.exe'
182	'9656,chrome.exe'
183	'9744,chrome.exe'
184	'9808,chrome.exe'
185	'10128,dllhost.exe'
186	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
187	'9924,XXX'
188	'9596,setup_wm.exe'
189	'10292,slui.exe'
190	'10444,wmplayer.exe'
191	'10656,SearchProtocolHost.exe'
192	'slc.dll,C:Windowssystem32slc.dll'
193	'ehtrace.dll,C:Windowsehomeehtrace.dll'
194	'10676,SearchFilterHost.exe'
195	'msxml6.dll,C:WindowsSystem32msxml6.dll'
196	'10836,chrome.exe'
197	'10932,chrome.exe'
198	'10400,dllhost.exe'
199	'11352,chrome.exe'

200	'11484,chrome.exe'
201	'WDSCORE.dll,C:WindowsSystem32WDSCORE.dll'
202	'11492,chrome.exe'
203	'11524,chrome.exe'
204	'11712,chrome.exe'
205	'11720,chrome.exe'
206	'11872,chrome.exe'
207	'11952,chrome.exe'
208	'12004,chrome.exe'
209	'12100,chrome.exe'
210	'12284,chrome.exe'
211	'12968,pingsender.exe'
212	'12980,conhost.exe'
213	'13308,SearchProtocolHost.exe'
214	'12436,SearchFilterHost.exe'
215	'12948,soffice.exe'
216	'13036,soffice.bin'
217	'13480,dllhost.exe'
218	'13572,dllhost.exe'
219	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
220	'13624,FoxitReader.exe'
221	'13916,WmiPrvSE.exe'
222	'14180,SearchProtocolHost.exe'
223	'14200,SearchFilterHost.exe'
224	'13508,taskhost.exe'
225	'14488,SearchProtocolHost.exe'
226	'14508,SearchFilterHost.exe'
227	'14800,taskeng.exe'
228	'14844,SearchProtocolHost.exe'
229	'14956,SearchFilterHost.exe'
230	'15564,smath.exe'
231	'15572,soffice.exe'
232	'15580,soffice.bin'
233	'15636,splwow64.exe'
234	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
235	'15728,scalc.exe'
236	'15736,soffice.exe'
237	'15744,soffice.bin'
238	'15996,dllhost.exe'
239	'16080,cmd.exe'
240	'16088,conhost.exe'

241	'16192,java.exe'
242	'15864,firefox.exe'
243	'16108,firefox.exe'
244	'16792,cmd.exe'
245	'16800,conhost.exe'
246	'16824,NETSTAT.EXE'
247	'16916,notepad++.exe'
248	'16972,Wireshark.exe'
249	'msimtf.dll,C:Windowssystem32msimtf.dll'
250	'17112,dumpcap.exe'
251	'17120,conhost.exe'
252	'17212,audiodg.exe'
253	'17280,FoxitReader.exe'
254	'17096,SearchProtocolHost.exe'
255	'17176,SearchFilterHost.exe'
256	'17584,mintty.exe'
257	'17620,conhost.exe'
258	'17636,XXX'
259	'17652,bash.exe'
260	'18092,simpress.exe'
261	'18104,soffice.exe'
262	'18116,soffice.bin'

Table 122: Proteus Malware Instance 2 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'352,XXX'	'360,csrss.exe'
5	'352,XXX'	'400,wininit.exe'
6	'360,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'412,XXX'	'424,csrss.exe'
8	'412,XXX'	'460,winlogon.exe'
9	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
10	'424,csrss.exe'	'3220,conhost.exe'
11	'424,csrss.exe'	'3952,conhost.exe'
12	'424,csrss.exe'	'4144,conhost.exe'
13	'424,csrss.exe'	'4416,conhost.exe'
14	'424,csrss.exe'	'4468,conhost.exe'
15	'424,csrss.exe'	'5344,conhost.exe'
16	'424,csrss.exe'	'6788,conhost.exe'
17	'424,csrss.exe'	'12980,conhost.exe'
18	'424,csrss.exe'	'16088,conhost.exe'
19	'424,csrss.exe'	'16800,conhost.exe'
20	'424,csrss.exe'	'17120,conhost.exe'
21	'424,csrss.exe'	'17620,conhost.exe'
22	'400,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
23	'400,wininit.exe'	'504,services.exe'
24	'400,wininit.exe'	'528,lsm.exe'
25	'400,wininit.exe'	'520,lsass.exe'
26	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
27	'504,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
28	'504,services.exe'	'628,svchost.exe'
29	'504,services.exe'	'692,VBoxService.exe'
30	'504,services.exe'	'756,svchost.exe'
31	'504,services.exe'	'840,svchost.exe'
32	'504,services.exe'	'888,svchost.exe'
33	'504,services.exe'	'928,svchost.exe'
34	'504,services.exe'	'328,svchost.exe'
35	'504,services.exe'	'740,svchost.exe'
36	'504,services.exe'	'1196,spoolsv.exe'
37	'504,services.exe'	'1224,svchost.exe'
38	'504,services.exe'	'1364,svchost.exe'
39	'504,services.exe'	'1388,FoxitConnectedPDFService.exe'

40	'504,services.exe'	'1860,svchost.exe'
41	'504,services.exe'	'1304,taskhost.exe'
42	'504,services.exe'	'2572,SearchIndexer.exe'
43	'504,services.exe'	'2800,wmpnetwk.exe'
44	'504,services.exe'	'124,sppsvc.exe'
45	'504,services.exe'	'2260,svchost.exe'
46	'504,services.exe'	'3244,msiexec.exe'
47	'504,services.exe'	'3924,GoogleUpdate.exe'
48	'504,services.exe'	'4964,taskhost.exe'
49	'504,services.exe'	'6868,svchost.exe'
50	'504,services.exe'	'13508,taskhost.exe'
51	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
52	'520,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
53	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
54	'628,svchost.exe'	'2388,WmiPrvSE.exe'
55	'628,svchost.exe'	'3388,WmiPrvSE.exe'
56	'628,svchost.exe'	'5568,dllhost.exe'
57	'628,svchost.exe'	'6548,dllhost.exe'
58	'628,svchost.exe'	'7076,dllhost.exe'
59	'628,svchost.exe'	'7080,dllhost.exe'
60	'628,svchost.exe'	'7980,dllhost.exe'
61	'628,svchost.exe'	'10128,dllhost.exe'
62	'628,svchost.exe'	'10292,slui.exe'
63	'628,svchost.exe'	'10400,dllhost.exe'
64	'628,svchost.exe'	'13480,dllhost.exe'
65	'628,svchost.exe'	'13572,dllhost.exe'
66	'628,svchost.exe'	'13916,WmiPrvSE.exe'
67	'628,svchost.exe'	'15996,dllhost.exe'
68	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
69	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
70	'840,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
71	'840,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
72	'840,svchost.exe'	'996,audiodg.exe'
73	'840,svchost.exe'	'10184,audiodg.exe'
74	'840,svchost.exe'	'5416,audiodg.exe'
75	'840,svchost.exe'	'17212,audiodg.exe'
76	'888,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
77	'888,svchost.exe'	'924,dwm.exe'
78	'928,svchost.exe'	'MPR.dll,C:Windowssystem32MPR.dll'
79	'928,svchost.exe'	'qmgrprxy.dll,C:Windowssystem32qmgrprxy.dll'
80	'928,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'

81	'928,svchost.exe'	tschannel.dll,C:Windowssystem32schannel.dll'
82	'928,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
83	'928,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
84	'928,svchost.exe'	'1592,taskeng.exe'
85	'928,svchost.exe'	'6908,consent.exe'
86	'928,svchost.exe'	'14800,taskeng.exe'
87	'328,svchost.exe'	'dsrole.dll,C:Windowssystem32dsrole.dll'
88	'328,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
89	'328,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
90	'740,svchost.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
91	'740,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
92	'1196,spoolsv.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
93	'1224,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
94	'1224,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
95	'1364,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
96	'1364,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
97	'1364,svchost.exe'	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
98	'1388,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
99	'1860,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
100	'1304,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
101	'924,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
102	'1276,XXX'	'212,explorer.exe'
103	'212,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
104	'212,explorer.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
105	'212,explorer.exe'	'msi.dll,C:Windowssystem32msi.dll'
106	'212,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
107	'212,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
108	'212,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
109	'212,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
110	'212,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
111	'212,explorer.exe'	'MsftEdit.dll,C:Windowssystem32MsftEdit.dll'
112	'212,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
113	'212,explorer.exe'	'2096,VBoxTray.exe'
114	'212,explorer.exe'	'2112,MySQLNotifier.exe'
115	'212,explorer.exe'	'3780,mintty.exe'
116	'212,explorer.exe'	'2164,cmd.exe'
117	'212,explorer.exe'	'3092,firefox.exe'
118	'212,explorer.exe'	'4136,cmd.exe'
119	'212,explorer.exe'	'4240,notepad++.exe'

120	'212,explorer.exe'	'4268,Wireshark.exe'
121	'212,explorer.exe'	'4884,FoxitReader.exe'
122	'212,explorer.exe'	'5100,mintty.exe'
123	'212,explorer.exe'	'5724,firefox.exe'
124	'212,explorer.exe'	'6332,gchrome.exe'
125	'212,explorer.exe'	'7400,chrome.exe'
126	'212,explorer.exe'	'11484,chrome.exe'
127	'212,explorer.exe'	'12948,soffice.exe'
128	'212,explorer.exe'	'13624,FoxitReader.exe'
129	'212,explorer.exe'	'15564,smath.exe'
130	'212,explorer.exe'	'15728,scalc.exe'
131	'212,explorer.exe'	'16080,cmd.exe'
132	'212,explorer.exe'	'15864,firefox.exe'
133	'212,explorer.exe'	'16792,cmd.exe'
134	'212,explorer.exe'	'16916,notepad++.exe'
135	'212,explorer.exe'	'16972,Wireshark.exe'
136	'212,explorer.exe'	'17280,FoxitReader.exe'
137	'212,explorer.exe'	'17584,mintty.exe'
138	'2096,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
139	'2112,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
140	'2132,XXX'	'2212,jusched.exe'
141	'2212,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
142	'2388,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
143	'2388,WmiPrvSE.exe'	'perfos.dll,C:WindowsSystem32perfos.dll'
144	'2388,WmiPrvSE.exe'	'SECUR32.DLL,C:Windowssystem32SECUR32.DLL'
145	'2572,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
146	'2572,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
147	'2572,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
148	'2572,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
149	'2572,SearchIndexer.exe'	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
150	'2572,SearchIndexer.exe'	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
151	'2572,SearchIndexer.exe'	'4264,SearchProtocolHost.exe'
152	'2572,SearchIndexer.exe'	'4304,SearchFilterHost.exe'
153	'2572,SearchIndexer.exe'	'7124,SearchProtocolHost.exe'
154	'2572,SearchIndexer.exe'	'7144,SearchFilterHost.exe'
155	'2572,SearchIndexer.exe'	'8392,SearchProtocolHost.exe'
156	'2572,SearchIndexer.exe'	'8416,SearchFilterHost.exe'
157	'2572,SearchIndexer.exe'	'10656,SearchProtocolHost.exe'
158	'2572,SearchIndexer.exe'	'10676,SearchFilterHost.exe'
159	'2572,SearchIndexer.exe'	'13308,SearchProtocolHost.exe'
160	'2572,SearchIndexer.exe'	'12436,SearchFilterHost.exe'

161	'2572,SearchIndexer.exe'	'14180,SearchProtocolHost.exe'
162	'2572,SearchIndexer.exe'	'14200,SearchFilterHost.exe'
163	'2572,SearchIndexer.exe'	'14488,SearchProtocolHost.exe'
164	'2572,SearchIndexer.exe'	'14508,SearchFilterHost.exe'
165	'2572,SearchIndexer.exe'	'14844,SearchProtocolHost.exe'
166	'2572,SearchIndexer.exe'	'14956,SearchFilterHost.exe'
167	'2572,SearchIndexer.exe'	'17096,SearchProtocolHost.exe'
168	'2572,SearchIndexer.exe'	'17176,SearchFilterHost.exe'
169	'2800,wmpnetwk.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
170	'2800,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
171	'2800,wmpnetwk.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
172	'2800,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
173	'124,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
174	'2260,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
175	'3388,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
176	'3192,XXX'	'3064,taskmgr.exe'
177	'3064,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
178	'3064,taskmgr.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
179	'3064,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
180	'3780,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
181	'3220,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
182	'3876,XXX'	'3608,bash.exe'
183	'3608,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
184	'1816,XXX'	'1872,driver_endpoint_netconn.exe'
185	'1872,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
186	'1592,taskeng.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
187	'1592,taskeng.exe'	'1180,GoogleUpdate.exe'
188	'1592,taskeng.exe'	'2232,GoogleUpdate.exe'
189	'1180,GoogleUpdate.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
190	'2232,GoogleUpdate.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
191	'2232,GoogleUpdate.exe'	'3696,GoogleUpdate.exe'
192	'3696,GoogleUpdate.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
193	'3244,msiexec.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
194	'3924,GoogleUpdate.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
195	'2164,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
196	'2164,cmd.exe'	'784,java.exe'
197	'2164,cmd.exe'	'1328,java.exe'
198	'3952,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
199	'1328,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
200	'1328,java.exe'	'5620,java.exe'
201	'3092,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

202	'3092,firefox.exe'	'3580,firefox.exe'
203	'3092,firefox.exe'	'5440,simpress.exe'
204	'3092,firefox.exe'	'12968,pingsender.exe'
205	'3580,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
206	'4136,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
207	'4136,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
208	'4136,cmd.exe'	'4168,NETSTAT.EXE'
209	'4144,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
210	'4168,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
211	'4168,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
212	'4240,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
213	'4268,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
214	'4268,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
215	'4268,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
216	'4268,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
217	'4268,Wireshark.exe'	'4408,dumpcap.exe'
218	'4268,Wireshark.exe'	'6576,dumpcap.exe'
219	'4408,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
220	'4416,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
221	'4964,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
222	'4884,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
223	'4884,FoxitReader.exe'	'4924,FoxitReaderUpdater.exe'
224	'4924,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
225	'4264,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
226	'4304,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
227	'5100,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
228	'4468,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
229	'4504,XXX'	'4512,bash.exe'
230	'4512,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
231	'5440,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
232	'5440,simpress.exe'	'5452,soffice.exe'
233	'5452,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
234	'5452,soffice.exe'	'5460,soffice.bin'
235	'5460,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
236	'5620,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
237	'5344,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
238	'5568,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
239	'6868,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
240	'7124,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
241	'7124,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
242	'7144,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'

243	'7144,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
244	'6548,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
245	'7076,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
246	'7080,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
247	'6332,gchrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
248	'6332,gchrome.exe'	'7024,chrome.exe'
249	'7024,chrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
250	'7024,chrome.exe'	'6848,chrome.exe'
251	'7024,chrome.exe'	'6800,chrome.exe'
252	'6848,chrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
253	'6848,chrome.exe'	'10836,chrome.exe'
254	'6800,chrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
255	'6576,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
256	'6788,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
257	'7400,chrome.exe'	'qmgrprxy.dll,C:Windowssystem32qmgrprxy.dll'
258	'7400,chrome.exe'	'7412,chrome.exe'
259	'7400,chrome.exe'	'LINKINFO.dll,C:Windowssystem32LINKINFO.dll'
260	'7400,chrome.exe'	'cryptnet.dll,C:Windowssystem32cryptnet.dll'
261	'7400,chrome.exe'	'imagehlp.dll,C:Windowssystem32imagehlp.dll'
262	'7400,chrome.exe'	'7444,chrome.exe'
263	'7400,chrome.exe'	'7560,chrome.exe'
264	'7400,chrome.exe'	'7628,chrome.exe'
265	'7400,chrome.exe'	'7644,chrome.exe'
266	'7400,chrome.exe'	'7772,chrome.exe'
267	'7400,chrome.exe'	'8244,chrome.exe'
268	'7400,chrome.exe'	'9656,chrome.exe'
269	'7400,chrome.exe'	'9744,chrome.exe'
270	'7400,chrome.exe'	'9808,chrome.exe'
271	'7412,chrome.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
272	'7444,chrome.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
273	'7628,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
274	'7644,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
275	'7772,chrome.exe'	'libegl.dll,C:Program Files (x86)GoogleChromeApplication61.0.3163.100swiftshaderlibegl.dll'
276	'7980,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
277	'8244,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
278	'8392,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
279	'8416,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
280	'9656,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
281	'9744,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
282	'9808,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
283	'10128,dllhost.exe'	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'

284	'9924,XXX'	'9596,setup_wm.exe'
285	'9596,setup_wm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
286	'9596,setup_wm.exe'	'10444,wmplayer.exe'
287	'10292,slui.exe'	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
288	'10444,wmplayer.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
289	'10656,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
290	'10656,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
291	'10656,SearchProtocolHost.exe'	'ehtrace.dll,C:Windowsehomeehtrace.dll'
292	'10676,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
293	'10676,SearchFilterHost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
294	'10836,chrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
295	'10836,chrome.exe'	'10932,chrome.exe'
296	'10836,chrome.exe'	'11352,chrome.exe'
297	'10932,chrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
298	'10400,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
299	'11352,chrome.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
300	'11484,chrome.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
301	'11484,chrome.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
302	'11484,chrome.exe'	'cryptnet.dll,C:Windowssystem32cryptnet.dll'
303	'11484,chrome.exe'	'imagehlp.dll,C:Windowssystem32imagehlp.dll'
304	'11484,chrome.exe'	'slc.dll,C:Windowssystem32slc.dll'
305	'11484,chrome.exe'	'WDSCORE.dll,C:WindowsSystem32WDSCORE.dll'
306	'11484,chrome.exe'	'11492,chrome.exe'
307	'11484,chrome.exe'	'11524,chrome.exe'
308	'11484,chrome.exe'	'11712,chrome.exe'
309	'11484,chrome.exe'	'11720,chrome.exe'
310	'11484,chrome.exe'	'11872,chrome.exe'
311	'11484,chrome.exe'	'11952,chrome.exe'
312	'11484,chrome.exe'	'12004,chrome.exe'
313	'11484,chrome.exe'	'12100,chrome.exe'
314	'11484,chrome.exe'	'12284,chrome.exe'
315	'11492,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
316	'11524,chrome.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
317	'11712,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
318	'11720,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
319	'11872,chrome.exe'	'libegl.dll,C:Program Files (x86)GoogleChromeApplication61.0.3163.100swiftshaderlibegl.dll'
320	'12004,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
321	'12100,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
322	'12284,chrome.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
323	'13308,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
324	'12436,SearchFilterHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'

325	'12948,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
326	'12948,soffice.exe'	'13036,soffice.bin'
327	'13036,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
328	'13480,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
329	'13572,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
330	'13624,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
331	'13916,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
332	'14180,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
333	'14200,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
334	'13508,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
335	'14488,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
336	'14508,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
337	'14800,taskeng.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
338	'14844,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
339	'14844,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
340	'14956,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
341	'14956,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
342	'15564,smath.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
343	'15564,smath.exe'	'15572,soffice.exe'
344	'15572,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
345	'15572,soffice.exe'	'15580,soffice.bin'
346	'15580,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
347	'15580,soffice.bin'	'15636,splwow64.exe'
348	'15636,splwow64.exe'	'OLEAUT32.dll,C:Windowssystem32OLEAUT32.dll'
349	'15728,scalc.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
350	'15728,scalc.exe'	'15736,soffice.exe'
351	'15736,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
352	'15736,soffice.exe'	'15744,soffice.bin'
353	'15744,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
354	'15996,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
355	'16080,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
356	'16080,cmd.exe'	'16192,java.exe'
357	'16088,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
358	'16192,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
359	'15864,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
360	'15864,firefox.exe'	'16108,firefox.exe'
361	'15864,firefox.exe'	'18092,simpress.exe'
362	'16108,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
363	'16792,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
364	'16792,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
365	'16792,cmd.exe'	'16824,NETSTAT.EXE'

366	'16800,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
367	'16824,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
368	'16824,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
369	'16916,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
370	'16972,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
371	'16972,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
372	'16972,Wireshark.exe'	'17112,dumpcap.exe'
373	'17112,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
374	'17120,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
375	'17280,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
376	'17096,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
377	'17176,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
378	'17584,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
379	'17620,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
380	'17636,XXX'	'17652,bash.exe'
381	'17652,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
382	'18092,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
383	'18092,simpress.exe'	'18104,soffice.exe'
384	'18104,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
385	'18104,soffice.exe'	'18116,soffice.bin'
386	'18116,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

7.2.15 Stabuniq Malware – Instance 1

Table 123: Stabuniq Malware Instance 1 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,XXX'
6	'360,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'408,XXX'
9	'424,csrss.exe'
10	'400,wininit.exe'
11	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
12	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
13	'460,winlogon.exe'
14	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
15	'504,services.exe'
16	'wship6.dll,C:WindowsSystem32wship6.dll'
17	'528,lsm.exe'
18	'520,lsass.exe'
19	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
20	'632,svchost.exe'
21	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
22	'696,VBoxService.exe'
23	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
24	'760,svchost.exe'
25	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
26	'848,svchost.exe'
27	'netutils.dll,C:WindowsSystem32netutils.dll'
28	'892,svchost.exe'
29	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
30	'928,svchost.exe'
31	'AVRT.dll,c:windowssystem32AVRT.dll'
32	'appinfo.dll,c:windowssystem32appinfo.dll'
33	'356,svchost.exe'
34	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
35	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'

36	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
37	'372,svchost.exe'
38	'SensApi.dll,C:Windowssystem32SensApi.dll'
39	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
40	'1140,spoolsv.exe'
41	'1184,svchost.exe'
42	'diagperf.dll,C:Windowssystem32diagperf.dll'
43	'1352,svchost.exe'
44	'SXS.DLL,C:Windowssystem32SXS.DLL'
45	'1392,FoxitConnectedPDFService.exe'
46	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
47	'1840,svchost.exe'
48	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
49	'428,sppsvc.exe'
50	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
51	'1476,svchost.exe'
52	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
53	'948,SearchIndexer.exe'
54	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
55	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
56	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
57	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
58	'1620,WmiPrvSE.exe'
59	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
60	'2068,taskhost.exe'
61	'midimap.dll,C:Windowssystem32midimap.dll'
62	'2320,dwm.exe'
63	'2312,XXX'
64	'2340,explorer.exe'
65	'sbdrop.dll,C:Program FilesWindows Sidebarsbdrop.dll'
66	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
67	'tquery.dll,C:Windowssystem32query.dll'
68	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
69	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
70	'MLANG.dll,C:Windowssystem32MLANG.dll'
71	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
72	'2428,VBoxTray.exe'
73	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
74	'2436,MySQLNotifier.exe'
75	'2456,XXX'
76	'2720,jusched.exe'

77	'2564,wmpnetwk.exe'
78	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
79	'provsvc.dll,C:WindowsSystem32provsvc.dll'
80	'868,XXX'
81	'2460,taskmgr.exe'
82	'DUser.dll,C:Windowssystem32DUser.dll'
83	'3452,audiodg.exe'
84	'3208,mintty.exe'
85	'apphelp.dll,C:Windowssystem32apphelp.dll'
86	'3468,conhost.exe'
87	'2548,XXX'
88	'2268,bash.exe'
89	'authz.dll,C:Windowssystem32authz.dll'
90	'3612,XXX'
91	'2788,driver_endpoint_netconn.exe'
92	'2144,dllhost.exe'
93	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
94	'704,notepad++.exe'
95	'1792,cmd.exe'
96	'3368,conhost.exe'
97	'3424,java.exe'
98	'1872,firefox.exe'
99	'1668,firefox.exe'
100	'4240,cmd.exe'
101	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
102	'4248,conhost.exe'
103	'4280,NETSTAT.EXE'
104	'winrnr.dll,C:WindowsSystem32winrnr.dll'
105	'4380,notepad++.exe'
106	'4536,Wireshark.exe'
107	'4604,gspawn-win64-helper.exe'
108	'4616,androiddump.exe'
109	'msimtf.dll,C:Windowssystem32msimtf.dll'
110	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
111	'4684,dumpcap.exe'
112	'4692,conhost.exe'
113	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
114	'4508,FoxitReader.exe'
115	'4616,FoxitReaderUpdater.exe'
116	'4968,SearchProtocolHost.exe'
117	'5004,SearchFilterHost.exe'

118	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
119	'3972,mintty.exe'
120	'5040,conhost.exe'
121	'4252,XXX'
122	'4660,bash.exe'
123	'5788,dllhost.exe'
124	'5988,SearchProtocolHost.exe'
125	'6076,SearchFilterHost.exe'
126	'OffFilt.dll,C:Windowssystem32OffFilt.dll'
127	'6772,java.exe'
128	'6780,conhost.exe'
129	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
130	'7036,dumpcap.exe'
131	'7044,conhost.exe'
132	'6612,audiodg.exe'
133	'7084,dllhost.exe'
134	'6280,dllhost.exe'
135	'6712,dllhost.exe'
136	'IDStore.dll,C:WindowsSystem32IDStore.dll'
137	'6752,dllhost.exe'
138	'6832,XXX'
139	'6844,svchost.exe'
140	'6920,XXX'
141	'6916,issch.exe'
142	'6940,iexplore.exe'
143	'6956,iexplore.exe'
144	'6156,svchost.exe'
145	'7448,slui.exe'
146	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
147	'7552,taskhost.exe'
148	'7728,pingsender.exe'
149	'7872,iexplore.exe'
150	'7924,iexplore.exe'
151	'8184,SearchProtocolHost.exe'
152	'profapi.dll,C:Windowssystem32profapi.dll'
153	'6648,SearchFilterHost.exe'
154	'8224,soffice.exe'
155	'8232,soffice.bin'
156	'8452,audiodg.exe'
157	'8352,iexplore.exe'
158	'8552,SearchProtocolHost.exe'

159	'8572,SearchFilterHost.exe'
160	'8808,iexplore.exe'
161	'8448,SearchProtocolHost.exe'
162	'4632,SearchFilterHost.exe'
163	'9248,iexplore.exe'
164	'9608,SearchProtocolHost.exe'
165	'10176,firefox.exe'
166	'9552,firefox.exe'
167	'10784,firefox.exe'
168	'10968,firefox.exe'
169	'11320,dllhost.exe'
170	'11372,SearchProtocolHost.exe'
171	'11392,SearchFilterHost.exe'
172	'11668,dllhost.exe'
173	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
174	'11724,FoxitReader.exe'
175	'11732,SearchProtocolHost.exe'
176	'11752,SearchFilterHost.exe'
177	'12024,calc.exe'
178	'oleacc.dll,C:Windowssystem32oleacc.dll'
179	'12496,WmiPrvSE.exe'
180	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
181	'12948,SearchProtocolHost.exe'
182	'12968,SearchFilterHost.exe'
183	'12712,LogonUI.exe'
184	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
185	'13372,SearchProtocolHost.exe'
186	'13392,SearchFilterHost.exe'
187	'13468,svchost.exe'
188	'292,smss.exe'
189	'364,csrss.exe'
190	'416,svchost.exe'
191	'428,csrss.exe'
192	'404,wininit.exe'
193	'464,winlogon.exe'
194	'508,services.exe'
195	'524,lsass.exe'
196	'532,lsm.exe'
197	'628,svchost.exe'
198	'692,VBoxService.exe'
199	'756,svchost.exe'

200	'836,svchost.exe'
201	'USERENV.dll,C:WindowsSystem32USERENV.dll'
202	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
203	'1000,audiodg.exe'
204	'884,svchost.exe'
205	'pcadm.dll,C:Windowssystem32pcadm.dll'
206	'932,svchost.exe'
207	'credssp.dll,C:WindowsSystem32credssp.dll'
208	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
209	'wer.dll,C:Windowssystem32wer.dll'
210	'rasman.dll,C:Windowssystem32rasman.dll'
211	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
212	'1064,svchost.exe'
213	'psapi.dll,C:Windowssystem32psapi.dll'
214	'1212,spoolsv.exe'
215	'1260,svchost.exe'
216	'1372,svchost.exe'
217	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
218	'1404,FoxitConnectedPDFService.exe'
219	'1892,svchost.exe'
220	'528,taskhost.exe'
221	'1320,sppsvc.exe'
222	'2156,userinit.exe'
223	'2164,dwm.exe'
224	'2188,explorer.exe'
225	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
226	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
227	thumbcache.dll,C:Windowssystem32humbcache.dll'
228	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
229	'NetworkExplorer.dll,C:Windowssystem32NetworkExplorer.dll'
230	'2276,VBoxTray.exe'
231	'2284,MySQLNotifier.exe'
232	'2408,XXX'
233	'2512,jusched.exe'
234	'2656,WmiPrvSE.exe'
235	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
236	'2944,mintty.exe'
237	'2984,conhost.exe'
238	'3000,XXX'
239	'3020,bash.exe'
240	'1100,SearchIndexer.exe'

241	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
242	'2492,SearchProtocolHost.exe'
243	'2524,SearchFilterHost.exe'
244	'2816,wmpnetwk.exe'
245	'2536,XXX'
246	'2124,iexplore.exe'
247	'912,iexplore.exe'
248	'1168,XXX'
249	'1508,driver_endpoint_netconn.exe'
250	'1328,taskmgr.exe'
251	'2360,svchost.exe'
252	tdh.dll,C:WindowsSystem32dh.dll'
253	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
254	'3228,consent.exe'
255	'3252,dllhost.exe'
256	'3288,dllhost.exe'
257	'3320,taskmgr.exe'
258	'3488,mspaint.exe'
259	'3516,svchost.exe'
260	'3568,notepad++.exe'
261	'3672,WMIADAP.exe'
262	'3700,WmiPrvSE.exe'
263	'4320,cmd.exe'
264	'4328,conhost.exe'
265	'4432,java.exe'
266	'4564,firefox.exe'
267	'4744,firefox.exe'
268	'4264,audiodg.exe'
269	'4412,conhost.exe'
270	'4424,cmd.exe'
271	'5024,NETSTAT.EXE'
272	'5184,notepad++.exe'
273	'5344,Wireshark.exe'
274	'5504,dumpcap.exe'
275	'5512,conhost.exe'
276	'5452,FoxitReader.exe'
277	'5688,SearchProtocolHost.exe'
278	'5716,SearchFilterHost.exe'
279	'5216,mintty.exe'
280	'5488,conhost.exe'
281	'5500,XXX'

282	'5780,bash.exe'
283	'6620,audiodg.exe'
284	'6380,dllhost.exe'
285	'7036,SearchProtocolHost.exe'
286	'7172,SearchFilterHost.exe'
287	'7760,iexplore.exe'
288	'7980,iexplore.exe'
289	'7520,SearchProtocolHost.exe'
290	'7452,SearchFilterHost.exe'
291	'8276,iexplore.exe'
292	'8476,audiodg.exe'
293	'10232,audiodg.exe'
294	'8600,SearchProtocolHost.exe'
295	'9172,java.exe'
296	'9180,conhost.exe'
297	'9044,taskhost.exe'
298	'8444,SearchProtocolHost.exe'
299	'8584,SearchFilterHost.exe'
300	'9376,SearchProtocolHost.exe'
301	'9396,SearchFilterHost.exe'
302	'9372,SearchProtocolHost.exe'
303	'9452,SearchFilterHost.exe'
304	'9680,SearchProtocolHost.exe'
305	'9724,SearchFilterHost.exe'

Table 124: Stabuniq Malware Instance 1 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'4,System'	'292,smss.exe'
4	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,XXX'	'360,csrss.exe'
6	'352,XXX'	'400,wininit.exe'
7	'360,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'408,XXX'	'424,csrss.exe'
9	'408,XXX'	'460,winlogon.exe'
10	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
11	'424,csrss.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
12	'424,csrss.exe'	'3468,conhost.exe'
13	'424,csrss.exe'	'3368,conhost.exe'
14	'424,csrss.exe'	'4248,conhost.exe'
15	'424,csrss.exe'	'4692,conhost.exe'
16	'424,csrss.exe'	'5040,conhost.exe'
17	'424,csrss.exe'	'6780,conhost.exe'
18	'424,csrss.exe'	'7044,conhost.exe'
19	'400,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
20	'400,wininit.exe'	'504,services.exe'
21	'400,wininit.exe'	'528,lsm.exe'
22	'400,wininit.exe'	'520,lsass.exe'
23	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
24	'460,winlogon.exe'	'12712,LogonUI.exe'
25	'504,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
26	'504,services.exe'	'632,svchost.exe'
27	'504,services.exe'	'696,VBoxService.exe'
28	'504,services.exe'	'760,svchost.exe'
29	'504,services.exe'	'848,svchost.exe'
30	'504,services.exe'	'892,svchost.exe'
31	'504,services.exe'	'928,svchost.exe'
32	'504,services.exe'	'356,svchost.exe'
33	'504,services.exe'	'372,svchost.exe'
34	'504,services.exe'	'1140,spoolsv.exe'
35	'504,services.exe'	'1184,svchost.exe'
36	'504,services.exe'	'1352,svchost.exe'
37	'504,services.exe'	'1392,FoxitConnectedPDFService.exe'
38	'504,services.exe'	'1840,svchost.exe'
39	'504,services.exe'	'428,sppsvc.exe'

40	'504,services.exe'	'1476,svchost.exe'
41	'504,services.exe'	'948,SearchIndexer.exe'
42	'504,services.exe'	'2068,taskhost.exe'
43	'504,services.exe'	'2564,wmpnetwk.exe'
44	'504,services.exe'	'6156,svchost.exe'
45	'504,services.exe'	'7552,taskhost.exe'
46	'504,services.exe'	'13468,svchost.exe'
47	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
48	'520,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
49	'632,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
50	'632,svchost.exe'	'1620,WmiPrvSE.exe'
51	'632,svchost.exe'	'2144,dllhost.exe'
52	'632,svchost.exe'	'5788,dllhost.exe'
53	'632,svchost.exe'	'7084,dllhost.exe'
54	'632,svchost.exe'	'6280,dllhost.exe'
55	'632,svchost.exe'	'6712,dllhost.exe'
56	'632,svchost.exe'	'6752,dllhost.exe'
57	'632,svchost.exe'	'7448,slui.exe'
58	'632,svchost.exe'	'11320,dllhost.exe'
59	'632,svchost.exe'	'11668,dllhost.exe'
60	'632,svchost.exe'	'12496,WmiPrvSE.exe'
61	'696,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
62	'760,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
63	'848,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
64	'848,svchost.exe'	'3452,audiodg.exe'
65	'848,svchost.exe'	'6612,audiodg.exe'
66	'848,svchost.exe'	'8452,audiodg.exe'
67	'892,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
68	'892,svchost.exe'	'2320,dwm.exe'
69	'928,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
70	'928,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
71	'356,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
72	'356,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
73	'356,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
74	'356,svchost.exe'	'364,csrss.exe'
75	'356,svchost.exe'	'404,wininit.exe'
76	'372,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
77	'372,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
78	'1140,spoolsv.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
79	'1184,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'

80	'1184,svchost.exe'	'diagperf.dll,C:Windowssystem32diagperf.dll'
81	'1352,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
82	'1392,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
83	'1840,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
84	'428,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
85	'428,sppsvc.exe'	'2984,conhost.exe'
86	'428,sppsvc.exe'	'4328,conhost.exe'
87	'428,sppsvc.exe'	'4412,conhost.exe'
88	'428,sppsvc.exe'	'5512,conhost.exe'
89	'428,sppsvc.exe'	'5488,conhost.exe'
90	'428,sppsvc.exe'	'9180,conhost.exe'
91	'1476,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
92	'948,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
93	'948,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
94	'948,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
95	'948,SearchIndexer.exe'	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
96	'948,SearchIndexer.exe'	'4968,SearchProtocolHost.exe'
97	'948,SearchIndexer.exe'	'5004,SearchFilterHost.exe'
98	'948,SearchIndexer.exe'	'5988,SearchProtocolHost.exe'
99	'948,SearchIndexer.exe'	'6076,SearchFilterHost.exe'
100	'948,SearchIndexer.exe'	'8184,SearchProtocolHost.exe'
101	'948,SearchIndexer.exe'	'6648,SearchFilterHost.exe'
102	'948,SearchIndexer.exe'	'8552,SearchProtocolHost.exe'
103	'948,SearchIndexer.exe'	'8572,SearchFilterHost.exe'
104	'948,SearchIndexer.exe'	'8448,SearchProtocolHost.exe'
105	'948,SearchIndexer.exe'	'4632,SearchFilterHost.exe'
106	'948,SearchIndexer.exe'	'9608,SearchProtocolHost.exe'
107	'948,SearchIndexer.exe'	'11372,SearchProtocolHost.exe'
108	'948,SearchIndexer.exe'	'11392,SearchFilterHost.exe'
109	'948,SearchIndexer.exe'	'11732,SearchProtocolHost.exe'
110	'948,SearchIndexer.exe'	'11752,SearchFilterHost.exe'
111	'948,SearchIndexer.exe'	'12948,SearchProtocolHost.exe'
112	'948,SearchIndexer.exe'	'12968,SearchFilterHost.exe'
113	'948,SearchIndexer.exe'	'13372,SearchProtocolHost.exe'
114	'948,SearchIndexer.exe'	'13392,SearchFilterHost.exe'
115	'1620,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
116	'1620,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
117	'2068,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
118	'2320,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
119	'2312,XXX'	'2340,explorer.exe'
120	'2340,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'

121	'2340,explorer.exe'	'sbdrop.dll,C:Program FilesWindows Sidebarsbdrop.dll'
122	'2340,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
123	'2340,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
124	'2340,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
125	'2340,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
126	'2340,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
127	'2340,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
128	'2340,explorer.exe'	'2428,VBoxTray.exe'
129	'2340,explorer.exe'	'2436,MySQLNotifier.exe'
130	'2340,explorer.exe'	'3208,mintty.exe'
131	'2340,explorer.exe'	'704,notepad++.exe'
132	'2340,explorer.exe'	'1792,cmd.exe'
133	'2340,explorer.exe'	'1872,firefox.exe'
134	'2340,explorer.exe'	'4240,cmd.exe'
135	'2340,explorer.exe'	'4380,notepad++.exe'
136	'2340,explorer.exe'	'4536,Wireshark.exe'
137	'2340,explorer.exe'	'4508,FoxitReader.exe'
138	'2340,explorer.exe'	'3972,mintty.exe'
139	'2340,explorer.exe'	'7872,iexplore.exe'
140	'2340,explorer.exe'	'8224,soffice.exe'
141	'2340,explorer.exe'	'10176,firefox.exe'
142	'2340,explorer.exe'	'10784,firefox.exe'
143	'2340,explorer.exe'	'11724,FoxitReader.exe'
144	'2340,explorer.exe'	'12024,calc.exe'
145	'2428,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
146	'2436,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
147	'2456,XXX'	'2720,jusched.exe'
148	'2720,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
149	'2564,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
150	'2564,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
151	'868,XXX'	'2460,taskmgr.exe'
152	'2460,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
153	'3208,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
154	'3468,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
155	'2548,XXX'	'2268,bash.exe'
156	'2268,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
157	'3612,XXX'	'2788,driver_endpoint_netconn.exe'
158	'2788,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
159	'2144,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
160	'704,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
161	'1792,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'

162	'1792,cmd.exe'	'3424,java.exe'
163	'3368,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
164	'3424,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
165	'3424,java.exe'	'6772,java.exe'
166	'1872,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
167	'1872,firefox.exe'	'1668,firefox.exe'
168	'1872,firefox.exe'	'7728,pingsender.exe'
169	'1668,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
170	'4240,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
171	'4240,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
172	'4240,cmd.exe'	'4280,NETSTAT.EXE'
173	'4248,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
174	'4280,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
175	'4280,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
176	'4380,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
177	'4536,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
178	'4536,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
179	'4536,Wireshark.exe'	'4604,gspawn-win64-helper.exe'
180	'4536,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
181	'4536,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
182	'4536,Wireshark.exe'	'4684,dumpcap.exe'
183	'4536,Wireshark.exe'	'7036,dumpcap.exe'
184	'4604,gspawn-win64-helper.exe'	'4616,androiddump.exe'
185	'4684,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
186	'4692,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
187	'4508,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
188	'4508,FoxitReader.exe'	'4616,FoxitReaderUpdater.exe'
189	'4616,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
190	'4968,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
191	'5004,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
192	'3972,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
193	'5040,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
194	'4252,XXX'	'4660,bash.exe'
195	'4660,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
196	'5788,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
197	'5988,SearchProtocolHost.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
198	'6076,SearchFilterHost.exe'	'OffFilt.dll,C:Windowssystem32OffFilt.dll'
199	'6772,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
200	'6780,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
201	'7036,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
202	'7044,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'

203	'7084,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
204	'6280,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
205	'6712,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
206	'6752,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
207	'6832,XXX'	'6844,svchost.exe'
208	'6844,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
209	'6920,XXX'	'6916,issch.exe'
210	'6916,issch.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
211	'6916,issch.exe'	'6940,iexplore.exe'
212	'6940,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
213	'6940,iexplore.exe'	'6956,iexplore.exe'
214	'6956,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
215	'6156,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
216	'7448,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
217	'7552,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
218	'7872,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
219	'7872,iexplore.exe'	'7924,iexplore.exe'
220	'7872,iexplore.exe'	'8352,iexplore.exe'
221	'7872,iexplore.exe'	'8808,iexplore.exe'
222	'7872,iexplore.exe'	'9248,iexplore.exe'
223	'7924,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
224	'8184,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
225	'6648,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
226	'8224,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
227	'8224,soffice.exe'	'8232,soffice.bin'
228	'8232,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
229	'8352,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
230	'8552,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
231	'8572,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
232	'8808,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
233	'8448,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
234	'4632,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
235	'9248,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
236	'9608,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
237	'10176,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
238	'10176,firefox.exe'	'9552,firefox.exe'
239	'9552,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
240	'10784,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
241	'10784,firefox.exe'	'10968,firefox.exe'
242	'10968,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
243	'11320,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

244	'11372,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
245	'11392,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
246	'11668,dllhost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
247	'11724,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
248	'11732,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
249	'11752,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
250	'12024,calc.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
251	'12496,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
252	'12948,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
253	'12968,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
254	'12712,LogonUI.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
255	'13372,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
256	'13392,SearchFilterHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
257	'13468,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
258	'292,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
259	'364,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
260	'416,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
261	'416,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
262	'416,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
263	'416,svchost.exe'	'428,csrss.exe'
264	'416,svchost.exe'	'464,winlogon.exe'
265	'428,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
266	'404,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
267	'404,wininit.exe'	'508,services.exe'
268	'404,wininit.exe'	'524,lsass.exe'
269	'404,wininit.exe'	'532,lsm.exe'
270	'464,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
271	'464,winlogon.exe'	'2156,userinit.exe'
272	'508,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
273	'508,services.exe'	'416,svchost.exe'
274	'508,services.exe'	'628,svchost.exe'
275	'508,services.exe'	'692,VBoxService.exe'
276	'508,services.exe'	'756,svchost.exe'
277	'508,services.exe'	'836,svchost.exe'
278	'508,services.exe'	'884,svchost.exe'
279	'508,services.exe'	'932,svchost.exe'
280	'508,services.exe'	'1064,svchost.exe'
281	'508,services.exe'	'1212,spoolsv.exe'
282	'508,services.exe'	'1260,svchost.exe'
283	'508,services.exe'	'1372,svchost.exe'

284	'508,services.exe'	'1404,FoxitConnectedPDFService.exe'
285	'508,services.exe'	'1892,svchost.exe'
286	'508,services.exe'	'528,taskhost.exe'
287	'508,services.exe'	'1320,sppsvc.exe'
288	'508,services.exe'	'1100,SearchIndexer.exe'
289	'508,services.exe'	'2816,wmpnetwk.exe'
290	'508,services.exe'	'2360,svchost.exe'
291	'508,services.exe'	'3516,svchost.exe'
292	'508,services.exe'	'9044,taskhost.exe'
293	'524,lsass.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
294	'532,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
295	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
296	'628,svchost.exe'	'2656,WmiPrvSE.exe'
297	'628,svchost.exe'	'3252,dllhost.exe'
298	'628,svchost.exe'	'3288,dllhost.exe'
299	'628,svchost.exe'	'3700,WmiPrvSE.exe'
300	'628,svchost.exe'	'6380,dllhost.exe'
301	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
302	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
303	'836,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
304	'836,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
305	'836,svchost.exe'	'USERENV.dll,C:WindowsSystem32USERENV.dll'
306	'836,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
307	'836,svchost.exe'	'1000,audiodg.exe'
308	'836,svchost.exe'	'4264,audiodg.exe'
309	'836,svchost.exe'	'6620,audiodg.exe'
310	'836,svchost.exe'	'8476,audiodg.exe'
311	'836,svchost.exe'	'10232,audiodg.exe'
312	'884,svchost.exe'	'pcadm.dll,C:Windowssystem32pcadm.dll'
313	'884,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
314	'884,svchost.exe'	'2164,dwm.exe'
315	'932,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
316	'932,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
317	'932,svchost.exe'	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
318	'932,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
319	'932,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
320	'932,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
321	'932,svchost.exe'	'3228,consent.exe'
322	'932,svchost.exe'	'3672,WMIADAP.exe'
323	'1064,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
324	'1064,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'

325	'1064,svchost.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
326	'1212,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
327	'1260,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
328	'1260,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
329	'1372,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
330	'1372,svchost.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
331	'1372,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
332	'1404,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
333	'1892,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
334	'528,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
335	'1320,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
336	'2156,userinit.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
337	'2156,userinit.exe'	'2188,explorer.exe'
338	'2164,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
339	'2188,explorer.exe'	'sbdrop.dll,C:Program FilesWindows Sidebarsbdrop.dll'
340	'2188,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
341	'2188,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
342	'2188,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
343	'2188,explorer.exe'	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
344	'2188,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
345	'2188,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
346	'2188,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
347	'2188,explorer.exe'	'NetworkExplorer.dll,C:Windowssystem32NetworkExplorer.dll'
348	'2188,explorer.exe'	'2276,VBoxTray.exe'
349	'2188,explorer.exe'	'2284,MySQLNotifier.exe'
350	'2188,explorer.exe'	'2944,mintty.exe'
351	'2188,explorer.exe'	'1328,taskmgr.exe'
352	'2188,explorer.exe'	'3488,mspaint.exe'
353	'2188,explorer.exe'	'3568,notepad++.exe'
354	'2188,explorer.exe'	'4320,cmd.exe'
355	'2188,explorer.exe'	'4564,firefox.exe'
356	'2188,explorer.exe'	'4424,cmd.exe'
357	'2188,explorer.exe'	'5184,notepad++.exe'
358	'2188,explorer.exe'	'5344,Wireshark.exe'
359	'2188,explorer.exe'	'5452,FoxitReader.exe'
360	'2188,explorer.exe'	'5216,mintty.exe'
361	'2188,explorer.exe'	'7760,iexplore.exe'
362	'2276,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
363	'2284,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
364	'2408,XXX'	'2512,jusched.exe'
365	'2512,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

366	'2656,WmiPrvSE.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
367	'2656,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
368	'2656,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
369	'2656,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
370	'2944,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
371	'2984,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
372	'3000,XXX'	'3020,bash.exe'
373	'3020,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
374	'1100,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
375	'1100,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
376	'1100,SearchIndexer.exe'	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
377	'1100,SearchIndexer.exe'	'2492,SearchProtocolHost.exe'
378	'1100,SearchIndexer.exe'	'2524,SearchFilterHost.exe'
379	'1100,SearchIndexer.exe'	'5688,SearchProtocolHost.exe'
380	'1100,SearchIndexer.exe'	'5716,SearchFilterHost.exe'
381	'1100,SearchIndexer.exe'	'7036,SearchProtocolHost.exe'
382	'1100,SearchIndexer.exe'	'7172,SearchFilterHost.exe'
383	'1100,SearchIndexer.exe'	'7520,SearchProtocolHost.exe'
384	'1100,SearchIndexer.exe'	'7452,SearchFilterHost.exe'
385	'1100,SearchIndexer.exe'	'8600,SearchProtocolHost.exe'
386	'1100,SearchIndexer.exe'	'8444,SearchProtocolHost.exe'
387	'1100,SearchIndexer.exe'	'8584,SearchFilterHost.exe'
388	'1100,SearchIndexer.exe'	'9376,SearchProtocolHost.exe'
389	'1100,SearchIndexer.exe'	'9396,SearchFilterHost.exe'
390	'1100,SearchIndexer.exe'	'9372,SearchProtocolHost.exe'
391	'1100,SearchIndexer.exe'	'9452,SearchFilterHost.exe'
392	'1100,SearchIndexer.exe'	'9680,SearchProtocolHost.exe'
393	'1100,SearchIndexer.exe'	'9724,SearchFilterHost.exe'
394	'2492,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
395	'2524,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
396	'2816,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
397	'2536,XXX'	'2124,iexplore.exe'
398	'2124,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
399	'2124,iexplore.exe'	'912,iexplore.exe'
400	'912,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
401	'1168,XXX'	'1508,driver_endpoint_netconn.exe'
402	'1508,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
403	'1328,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
404	'1328,taskmgr.exe'	'3320,taskmgr.exe'
405	'2360,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
406	'2360,svchost.exe'	tdh.dll,C:WindowsSystem32dh.dll'

407	'2360,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
408	'3252,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
409	'3288,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
410	'3320,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
411	'3488,mspaint.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
412	'3516,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
413	'3568,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
414	'3672,WMIADAP.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
415	'3672,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
416	'3700,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
417	'4320,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
418	'4320,cmd.exe'	'4432,java.exe'
419	'4328,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
420	'4432,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
421	'4432,java.exe'	'9172,java.exe'
422	'4564,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
423	'4564,firefox.exe'	'4744,firefox.exe'
424	'4744,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
425	'4412,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
426	'4424,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
427	'4424,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
428	'4424,cmd.exe'	'5024,NETSTAT.EXE'
429	'5024,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
430	'5024,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
431	'5184,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
432	'5344,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
433	'5344,Wireshark.exe'	'5504,dumpcap.exe'
434	'5504,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
435	'5512,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
436	'5452,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
437	'5688,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
438	'5716,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
439	'5216,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
440	'5488,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
441	'5500,XXX'	'5780,bash.exe'
442	'5780,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
443	'6380,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
444	'7036,SearchProtocolHost.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
445	'7172,SearchFilterHost.exe'	'OffFilt.dll,C:Windowssystem32OffFilt.dll'
446	'7760,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
447	'7760,iexplore.exe'	'7980,iexplore.exe'

448	'7760,iexplore.exe'	'8276,iexplore.exe'
449	'7980,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
450	'7520,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
451	'7452,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
452	'8276,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
453	'8600,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
454	'9172,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
455	'9180,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
456	'9044,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
457	'8444,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
458	'8584,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
459	'9376,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
460	'9396,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
461	'9372,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
462	'9452,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
463	'9680,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
464	'9724,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'

7.2.16 Stabuniq Malware – Instance 2

Table 125: Stabuniq Malware Instance 2 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'264,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'328,XXX'
6	'336,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'376,XXX'
9	'396,csrss.exe'
10	'384,wininit.exe'
11	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
12	'436,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'480,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'496,lsm.exe'
17	'488,lsass.exe'
18	'GPAPI.dll,C:Windowssystem32GPAPI.dll'
19	'wkscli.dll,C:Windowssystem32wkscli.dll'
20	'612,svchost.exe'
21	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
22	'672,VBoxService.exe'
23	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
24	'724,svchost.exe'
25	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
26	'824,svchost.exe'
27	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
28	'profapi.dll,C:WindowsSystem32profapi.dll'
29	'netutils.dll,C:WindowsSystem32netutils.dll'
30	'winrnr.dll,C:WindowsSystem32winrnr.dll'
31	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
32	'856,svchost.exe'
33	'credssp.dll,C:WindowsSystem32credssp.dll'
34	'972,audiodg.exe'
35	'896,svchost.exe'

36	'appinfo.dll,c:windowssystem32appinfo.dll'
37	'mspatcha.dll,c:windowssystem32mspatcha.dll'
38	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
39	'wer.dll,C:Windowssystem32wer.dll'
40	'rasman.dll,C:Windowssystem32rasman.dll'
41	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
42	'AVRT.dll,c:windowssystem32AVRT.dll'
43	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
44	'wups2.dll,C:Windowssystem32wups2.dll'
45	'iertutil.dll,C:Windowssystem32iertutil.dll'
46	'schannel.DLL,C:Windowssystem32schannel.DLL'
47	'CbsApi.dll,C:WindowsservicingCbsApi.dll'
48	'352,svchost.exe'
49	'webio.dll,C:Windowssystem32webio.dll'
50	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
51	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
52	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
53	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
54	'892,svchost.exe'
55	'psapi.dll,C:Windowssystem32psapi.dll'
56	'SensApi.dll,C:Windowssystem32SensApi.dll'
57	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
58	'1156,spoolsv.exe'
59	'1188,svchost.exe'
60	'1296,svchost.exe'
61	'RpcRtRemote.dll,C:Windowssystem32RpcRtRemote.dll'
62	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
63	'SXS.DLL,C:Windowssystem32SXS.DLL'
64	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
65	'1328,FoxitConnectedPDFService.exe'
66	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
67	'1700,svchost.exe'
68	'2024,taskhost.exe'
69	'midimap.dll,C:Windowssystem32midimap.dll'
70	'1104,sppsvc.exe'
71	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
72	'1108,XXX'
73	'1272,explorer.exe'
74	'msxml3.dll,C:WindowsSystem32msxml3.dll'
75	'1984,dwm.exe'
76	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'

77	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
78	tquery.dll,C:Windowssystem32query.dll'
79	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
80	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
81	'NetworkExplorer.dll,C:Windowssystem32NetworkExplorer.dll'
82	'MLANG.dll,C:Windowssystem32MLANG.dll'
83	'browcli.dll,C:Windowssystem32rowcli.dll'
84	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
85	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
86	'dsrole.dll,C:Windowssystem32dsrole.dll'
87	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
88	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
89	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
90	'icm32.dll,C:Windowssystem32icm32.dll'
91	'shacct.dll,C:WindowsSystem32shacct.dll'
92	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
93	'mtxoci.dll,C:Windowssystem32mtxoci.dll'
94	'1884,VBoxTray.exe'
95	'1880,MySQLNotifier.exe'
96	'1872,XXX'
97	'1532,jusched.exe'
98	'2124,WmiPrvSE.exe'
99	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
100	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
101	'2288,XXX'
102	'2444,taskmgr.exe'
103	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
104	'2520,SearchIndexer.exe'
105	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
106	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
107	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
108	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
109	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
110	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
111	'ktmw32.dll,C:Windowssystem32ktmw32.dll'
112	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
113	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
114	'2728,wmpnetwk.exe'
115	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
116	'provsvc.dll,C:WindowsSystem32provsvc.dll'
117	'2360,mintty.exe'

118	'apphelp.dll,C:Windowssystem32apphelp.dll'
119	'2316,conhost.exe'
120	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
121	'2668,bash.exe'
122	'authz.dll,C:Windowssystem32authz.dll'
123	'620,XXX'
124	'1580,driver_endpoint_netconn.exe'
125	'2044,svchost.exe'
126	tdh.dll,C:WindowsSystem32dh.dll'
127	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
128	'2620,WMIADAP.exe'
129	'2276,WmiPrvSE.exe'
130	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
131	'3044,taskhost.exe'
132	'3468,cmd.exe'
133	'3480,conhost.exe'
134	'3596,java.exe'
135	'4064,firefox.exe'
136	'3980,firefox.exe'
137	'4356,pingsender.exe'
138	'4376,conhost.exe'
139	'4436,firefox.exe'
140	'4604,firefox.exe'
141	'4984,cmd.exe'
142	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
143	'5028,conhost.exe'
144	'4920,NETSTAT.EXE'
145	'5224,notepad++.exe'
146	'5404,Wireshark.exe'
147	'5500,gspawn-win64-helper.exe'
148	'5512,androiddump.exe'
149	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
150	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
151	'5592,dumpcap.exe'
152	'5600,conhost.exe'
153	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
154	'5696,FoxitReader.exe'
155	'5860,FoxitReaderUpdater.exe'
156	'5848,mintty.exe'
157	'6104,conhost.exe'
158	'6080,XXX'

159	'6160,bash.exe'
160	'7552,audiodg.exe'
161	'8016,SearchProtocolHost.exe'
162	'8152,SearchFilterHost.exe'
163	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
164	'7420,dllhost.exe'
165	'7364,dllhost.exe'
166	'IDStore.dll,C:WindowsSystem32IDStore.dll'
167	'7604,dllhost.exe'
168	'7636,XXX'
169	'7548,svchost.exe'
170	'7264,XXX'
171	'7268,issch.exe'
172	'7680,iexplore.exe'
173	'7628,iexplore.exe'
174	'9852,audiodg.exe'
175	'7528,SearchProtocolHost.exe'
176	'7324,SearchFilterHost.exe'
177	'8420,svchost.exe'
178	'9000,iexplore.exe'
179	'8336,iexplore.exe'
180	'8616,java.exe'
181	'8624,conhost.exe'
182	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
183	'8984,SearchProtocolHost.exe'
184	'10232,iexplore.exe'
185	'10960,iexplore.exe'
186	'11224,SearchProtocolHost.exe'
187	'10256,SearchFilterHost.exe'
188	'11832,SearchFilterHost.exe'
189	'12068,slui.exe'
190	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
191	'12948,dumpcap.exe'
192	'12960,conhost.exe'
193	'13016,taskmgr.exe'
194	'13212,dllhost.exe'
195	'13252,dllhost.exe'
196	'13288,taskmgr.exe'
197	'DUser.dll,C:Windowssystem32DUser.dll'
198	'WINMM.dll,C:Windowssystem32WINMM.dll'
199	'12480,SearchProtocolHost.exe'

200	'12688,SearchFilterHost.exe'
201	'13032,soffice.exe'
202	'13016,soffice.bin'
203	'12512,FoxitReader.exe'
204	'12940,SearchProtocolHost.exe'
205	'13392,SearchFilterHost.exe'
206	'14316,WmiPrvSE.exe'
207	'15232,iexplore.exe'
208	'15316,iexplore.exe'
209	'15784,audiodg.exe'
210	'15568,dllhost.exe'
211	'15948,dllhost.exe'
212	'16016,dllhost.exe'
213	'16180,StikyNot.exe'
214	'16240,SearchProtocolHost.exe'
215	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
216	'16260,SearchFilterHost.exe'
217	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
218	'rtffilt.dll,C:Windowssystem32rtffilt.dll'
219	'16296,SearchProtocolHost.exe'
220	'15884,dllhost.exe'
221	'13448,dllhost.exe'
222	'16544,svchost.exe'
223	'28436,audiodg.exe'
224	'32500,audiodg.exe'
225	'16648,dllhost.exe'
226	'16752,taskhost.exe'
227	'16420,iexplore.exe'
228	'15804,iexplore.exe'
229	'18064,audiodg.exe'
230	'18180,SearchProtocolHost.exe'
231	'18240,SearchFilterHost.exe'
232	'18392,iexplore.exe'
233	'18556,iexplore.exe'
234	'24452,audiodg.exe'
235	'20360,cmd.exe'
236	'20368,conhost.exe'
237	'20472,java.exe'
238	'20424,firefox.exe'
239	'20584,firefox.exe'
240	'21356,cmd.exe'

241	'21364,conhost.exe'
242	'21412,NETSTAT.EXE'
243	'21468,SearchProtocolHost.exe'
244	'20852,SearchFilterHost.exe'
245	'20840,Wireshark.exe'
246	'21532,dumpcap.exe'
247	'21540,conhost.exe'
248	'msimtf.dll,C:Windowssystem32msimtf.dll'
249	'21660,dumpcap.exe'
250	'21668,conhost.exe'
251	'22288,audiodg.exe'
252	'21536,SearchProtocolHost.exe'
253	'21912,SearchFilterHost.exe'
254	'22136,FoxitReader.exe'
255	'22464,mintty.exe'
256	'21692,conhost.exe'
257	'21712,XXX'
258	'21980,bash.exe'
259	'22092,bash.exe'
260	'22324,bash.exe'
261	'22424,hostname.exe'
262	'23540,SearchProtocolHost.exe'
263	'22744,SearchFilterHost.exe'
264	'23292,SearchProtocolHost.exe'
265	'23368,slui.exe'
266	'23468,SearchProtocolHost.exe'
267	'22732,SearchFilterHost.exe'
268	'23940,SearchProtocolHost.exe'
269	'23960,SearchFilterHost.exe'
270	'24200,java.exe'
271	'24228,conhost.exe'
272	'24536,SearchProtocolHost.exe'
273	'23748,SearchFilterHost.exe'
274	'24932,SearchProtocolHost.exe'
275	'25224,SearchFilterHost.exe'
276	'25340,dumpcap.exe'
277	'25348,conhost.exe'
278	'24584,svchost.exe'
279	'24820,SearchProtocolHost.exe'
280	'25216,Wireshark.exe'
281	'24800,dumpcap.exe'

282	'24808,conhost.exe'
283	'25320,SearchProtocolHost.exe'
284	'24692,SearchFilterHost.exe'
285	'25584,conhost.exe'
286	'5236,dumpcap.exe'
287	'25980,soffice.exe'
288	'25988,soffice.bin'
289	'28388,iexplore.exe'
290	'26260,iexplore.exe'
291	'26440,SearchProtocolHost.exe'
292	'26472,SearchFilterHost.exe'
293	'25848,firefox.exe'
294	'26660,firefox.exe'
295	'26984,dllhost.exe'
296	'27316,taskhost.exe'
297	'27484,firefox.exe'
298	'26632,firefox.exe'
299	'28544,SearchProtocolHost.exe'
300	'28612,SearchFilterHost.exe'
301	'27872,dllhost.exe'
302	'28676,dllhost.exe'
303	'28928,dllhost.exe'
304	'29108,dllhost.exe'
305	'29208,wab.exe'
306	'29216,SearchProtocolHost.exe'
307	'slc.dll,C:Windowssystem32slc.dll'
308	'ehtrace.dll,C:Windowsehomeehtrace.dll'
309	'29236,SearchFilterHost.exe'
310	'msxml6.dll,C:WindowsSystem32msxml6.dll'
311	'29380,dllhost.exe'
312	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
313	'29484,XXX'
314	'29508,setup_wm.exe'
315	'29620,wmplayer.exe'
316	'29304,rundll32.exe'
317	'30688,Wireshark.exe'
318	'29728,gspawn-win64-helper.exe'
319	'29732,androiddump.exe'
320	'28776,dllhost.exe'
321	'29100,dllhost.exe'
322	'29372,dllhost.exe'

323	'29576,dllhost.exe'
324	'27832,dllhost.exe'
325	'29104,dllhost.exe'
326	'29520,dllhost.exe'
327	'29420,dllhost.exe'
328	'29744,dllhost.exe'
329	'29900,firefox.exe'
330	'30056,firefox.exe'
331	'30488,SearchProtocolHost.exe'
332	'30576,SearchFilterHost.exe'
333	'30588,cmd.exe'
334	'30596,conhost.exe'
335	'31384,firefox.exe'
336	'31544,firefox.exe'
337	'31676,dllhost.exe'
338	'31380,calc.exe'
339	'oleacc.dll,C:Windowssystem32oleacc.dll'
340	'31756,notepad++.exe'
341	'31816,iexplore.exe'
342	'31888,iexplore.exe'
343	'32592,SearchProtocolHost.exe'
344	'32724,SearchFilterHost.exe'
345	'32400,WinRAR.exe'
346	'32844,dllhost.exe'
347	'32944,dllhost.exe'
348	'32980,dllhost.exe'
349	'33016,slui.exe'
350	'33156,TrustedInstaller.exe'
351	'33220,taskmgr.exe'
352	'33324,SearchProtocolHost.exe'
353	'33360,SearchFilterHost.exe'

Table 126: Stabuniq Malware Instance 2 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'264,smss.exe'
3	'264,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'328,XXX'	'336,csrss.exe'
5	'328,XXX'	'384,wininit.exe'
6	'336,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'376,XXX'	'396,csrss.exe'
8	'376,XXX'	'436,winlogon.exe'
9	'396,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
10	'396,csrss.exe'	'2316,conhost.exe'
11	'396,csrss.exe'	'3480,conhost.exe'
12	'396,csrss.exe'	'4376,conhost.exe'
13	'396,csrss.exe'	'5028,conhost.exe'
14	'396,csrss.exe'	'5600,conhost.exe'
15	'396,csrss.exe'	'6104,conhost.exe'
16	'396,csrss.exe'	'8624,conhost.exe'
17	'396,csrss.exe'	'12960,conhost.exe'
18	'396,csrss.exe'	'20368,conhost.exe'
19	'396,csrss.exe'	'21364,conhost.exe'
20	'396,csrss.exe'	'21540,conhost.exe'
21	'396,csrss.exe'	'21668,conhost.exe'
22	'396,csrss.exe'	'21692,conhost.exe'
23	'396,csrss.exe'	'24228,conhost.exe'
24	'396,csrss.exe'	'25348,conhost.exe'
25	'396,csrss.exe'	'24808,conhost.exe'
26	'396,csrss.exe'	'25584,conhost.exe'
27	'396,csrss.exe'	'30596,conhost.exe'
28	'384,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
29	'384,wininit.exe'	'480,services.exe'
30	'384,wininit.exe'	'496,lsm.exe'
31	'384,wininit.exe'	'488,lsass.exe'
32	'436,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
33	'480,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
34	'480,services.exe'	'612,svchost.exe'
35	'480,services.exe'	'672,VBoxService.exe'
36	'480,services.exe'	'724,svchost.exe'
37	'480,services.exe'	'824,svchost.exe'
38	'480,services.exe'	'856,svchost.exe'
39	'480,services.exe'	'896,svchost.exe'

40	'480,services.exe'	'352,svchost.exe'
41	'480,services.exe'	'892,svchost.exe'
42	'480,services.exe'	'1156,spoolsv.exe'
43	'480,services.exe'	'1188,svchost.exe'
44	'480,services.exe'	'1296,svchost.exe'
45	'480,services.exe'	'1328,FoxitConnectedPDFService.exe'
46	'480,services.exe'	'1700,svchost.exe'
47	'480,services.exe'	'2024,taskhost.exe'
48	'480,services.exe'	'1104,sppsvc.exe'
49	'480,services.exe'	'2520,SearchIndexer.exe'
50	'480,services.exe'	'2728,wmpnetwk.exe'
51	'480,services.exe'	'2044,svchost.exe'
52	'480,services.exe'	'3044,taskhost.exe'
53	'480,services.exe'	'8420,svchost.exe'
54	'480,services.exe'	'16544,svchost.exe'
55	'480,services.exe'	'16752,taskhost.exe'
56	'480,services.exe'	'24584,svchost.exe'
57	'480,services.exe'	'27316,taskhost.exe'
58	'480,services.exe'	'33156,TrustedInstaller.exe'
59	'496,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
60	'488,lsass.exe'	'GPAPI.dll,C:Windowssystem32GPAPI.dll'
61	'488,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
62	'612,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
63	'612,svchost.exe'	'2124,WmiPrvSE.exe'
64	'612,svchost.exe'	'2276,WmiPrvSE.exe'
65	'612,svchost.exe'	'7420,dllhost.exe'
66	'612,svchost.exe'	'7364,dllhost.exe'
67	'612,svchost.exe'	'7604,dllhost.exe'
68	'612,svchost.exe'	'12068,slui.exe'
69	'612,svchost.exe'	'13212,dllhost.exe'
70	'612,svchost.exe'	'13252,dllhost.exe'
71	'612,svchost.exe'	'14316,WmiPrvSE.exe'
72	'612,svchost.exe'	'15568,dllhost.exe'
73	'612,svchost.exe'	'15948,dllhost.exe'
74	'612,svchost.exe'	'16016,dllhost.exe'
75	'612,svchost.exe'	'15884,dllhost.exe'
76	'612,svchost.exe'	'13448,dllhost.exe'
77	'612,svchost.exe'	'16648,dllhost.exe'
78	'612,svchost.exe'	'23368,slui.exe'
79	'612,svchost.exe'	'26984,dllhost.exe'
80	'612,svchost.exe'	'27872,dllhost.exe'

81	'612,svchost.exe'	'28676,dllhost.exe'
82	'612,svchost.exe'	'28928,dllhost.exe'
83	'612,svchost.exe'	'29108,dllhost.exe'
84	'612,svchost.exe'	'29380,dllhost.exe'
85	'612,svchost.exe'	'28776,dllhost.exe'
86	'612,svchost.exe'	'29100,dllhost.exe'
87	'612,svchost.exe'	'29372,dllhost.exe'
88	'612,svchost.exe'	'29576,dllhost.exe'
89	'612,svchost.exe'	'27832,dllhost.exe'
90	'612,svchost.exe'	'29104,dllhost.exe'
91	'612,svchost.exe'	'29520,dllhost.exe'
92	'612,svchost.exe'	'29420,dllhost.exe'
93	'612,svchost.exe'	'29744,dllhost.exe'
94	'612,svchost.exe'	'31676,dllhost.exe'
95	'612,svchost.exe'	'32844,dllhost.exe'
96	'612,svchost.exe'	'32944,dllhost.exe'
97	'612,svchost.exe'	'32980,dllhost.exe'
98	'612,svchost.exe'	'33016,slui.exe'
99	'672,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
100	'724,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
101	'824,svchost.exe'	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
102	'824,svchost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
103	'824,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
104	'824,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
105	'824,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
106	'824,svchost.exe'	'972,audiodg.exe'
107	'824,svchost.exe'	'7552,audiodg.exe'
108	'824,svchost.exe'	'9852,audiodg.exe'
109	'824,svchost.exe'	'15784,audiodg.exe'
110	'824,svchost.exe'	'28436,audiodg.exe'
111	'824,svchost.exe'	'32500,audiodg.exe'
112	'824,svchost.exe'	'18064,audiodg.exe'
113	'824,svchost.exe'	'24452,audiodg.exe'
114	'824,svchost.exe'	'22288,audiodg.exe'
115	'856,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
116	'856,svchost.exe'	'1984,dwm.exe'
117	'896,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
118	'896,svchost.exe'	'mspatcha.dll,c:windowssystem32mspatcha.dll'
119	'896,svchost.exe'	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
120	'896,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
121	'896,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'

122	'896,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
123	'896,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
124	'896,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
125	'896,svchost.exe'	'wups2.dll,C:Windowssystem32wups2.dll'
126	'896,svchost.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
127	'896,svchost.exe'	'schannel.DLL,C:Windowssystem32schannel.DLL'
128	'896,svchost.exe'	'CbsApi.dll,C:WindowsservicingCbsApi.dll'
129	'896,svchost.exe'	'2620,WMIADAP.exe'
130	'352,svchost.exe'	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
131	'352,svchost.exe'	'webio.dll,C:Windowssystem32webio.dll'
132	'352,svchost.exe'	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
133	'352,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
134	'352,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
135	'352,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
136	'892,svchost.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
137	'892,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
138	'892,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
139	'1156,spoolsv.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
140	'1188,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
141	'1188,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
142	'1296,svchost.exe'	'RpcRtRemote.dll,C:Windowssystem32RpcRtRemote.dll'
143	'1296,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
144	'1296,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
145	'1296,svchost.exe'	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
146	'1328,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
147	'1700,svchost.exe'	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
148	'2024,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
149	'1104,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
150	'1108,XXX'	'1272,explorer.exe'
151	'1272,explorer.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
152	'1272,explorer.exe'	'wups2.dll,C:Windowssystem32wups2.dll'
153	'1272,explorer.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
154	'1272,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
155	'1272,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
156	'1272,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
157	'1272,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
158	'1272,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
159	'1272,explorer.exe'	'NetworkExplorer.dll,C:Windowssystem32NetworkExplorer.dll'
160	'1272,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
161	'1272,explorer.exe'	'browcli.dll,C:Windowssystem32rowcli.dll'

162	'1272,explorer.exe'	'Normaliz.dll,C:Windowssystem32Normaliz.dll'
163	'1272,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
164	'1272,explorer.exe'	'dsrole.dll,C:Windowssystem32dsrole.dll'
165	'1272,explorer.exe'	'hhsetup.dll,C:Windowssystem32hhsetup.dll'
166	'1272,explorer.exe'	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
167	'1272,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
168	'1272,explorer.exe'	'icm32.dll,C:Windowssystem32icm32.dll'
169	'1272,explorer.exe'	'shacct.dll,C:WindowsSystem32shacct.dll'
170	'1272,explorer.exe'	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
171	'1272,explorer.exe'	'mtxoci.dll,C:Windowssystem32mtxoci.dll'
172	'1272,explorer.exe'	'1884,VBoxTray.exe'
173	'1272,explorer.exe'	'1880,MySQLNotifier.exe'
174	'1272,explorer.exe'	'2360,mintty.exe'
175	'1272,explorer.exe'	'3468,cmd.exe'
176	'1272,explorer.exe'	'4064,firefox.exe'
177	'1272,explorer.exe'	'4436,firefox.exe'
178	'1272,explorer.exe'	'4984,cmd.exe'
179	'1272,explorer.exe'	'5224,notepad++.exe'
180	'1272,explorer.exe'	'5404,Wireshark.exe'
181	'1272,explorer.exe'	'5696,FoxitReader.exe'
182	'1272,explorer.exe'	'5848,mintty.exe'
183	'1272,explorer.exe'	'9000,iexplore.exe'
184	'1272,explorer.exe'	'13016,taskmgr.exe'
185	'1272,explorer.exe'	'13032,soffice.exe'
186	'1272,explorer.exe'	'12512,FoxitReader.exe'
187	'1272,explorer.exe'	'16180,StikyNot.exe'
188	'1272,explorer.exe'	'16420,iexplore.exe'
189	'1272,explorer.exe'	'20360,cmd.exe'
190	'1272,explorer.exe'	'20424,firefox.exe'
191	'1272,explorer.exe'	'21356,cmd.exe'
192	'1272,explorer.exe'	'20840,Wireshark.exe'
193	'1272,explorer.exe'	'22136,FoxitReader.exe'
194	'1272,explorer.exe'	'22464,mintty.exe'
195	'1272,explorer.exe'	'25216,Wireshark.exe'
196	'1272,explorer.exe'	'25980,soffice.exe'
197	'1272,explorer.exe'	'25848,firefox.exe'
198	'1272,explorer.exe'	'27484,firefox.exe'
199	'1272,explorer.exe'	'29208,wab.exe'
200	'1272,explorer.exe'	'29304,rundll32.exe'
201	'1272,explorer.exe'	'30688,Wireshark.exe'
202	'1272,explorer.exe'	'29900,firefox.exe'

203	'1272,explorer.exe'	'30588,cmd.exe'
204	'1272,explorer.exe'	'31384,firefox.exe'
205	'1272,explorer.exe'	'31380,calc.exe'
206	'1272,explorer.exe'	'31756,notepad++.exe'
207	'1272,explorer.exe'	'31816,iexplore.exe'
208	'1272,explorer.exe'	'32400,WinRAR.exe'
209	'1272,explorer.exe'	'33220,taskmgr.exe'
210	'1984,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
211	'1884,VBoxTray.exe'	'RpcRtRemote.dll,C:Windowssystem32RpcRtRemote.dll'
212	'1880,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
213	'1872,XXX'	'1532,jusched.exe'
214	'1532,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
215	'2124,WmiPrvSE.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
216	'2124,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
217	'2124,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
218	'2124,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
219	'2288,XXX'	'2444,taskmgr.exe'
220	'2288,XXX'	'2668,bash.exe'
221	'2444,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
222	'2520,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
223	'2520,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
224	'2520,SearchIndexer.exe'	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
225	'2520,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
226	'2520,SearchIndexer.exe'	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
227	'2520,SearchIndexer.exe'	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
228	'2520,SearchIndexer.exe'	'ktmw32.dll,C:Windowssystem32ktmw32.dll'
229	'2520,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
230	'2520,SearchIndexer.exe'	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
231	'2520,SearchIndexer.exe'	'8016,SearchProtocolHost.exe'
232	'2520,SearchIndexer.exe'	'8152,SearchFilterHost.exe'
233	'2520,SearchIndexer.exe'	'7528,SearchProtocolHost.exe'
234	'2520,SearchIndexer.exe'	'7324,SearchFilterHost.exe'
235	'2520,SearchIndexer.exe'	'8984,SearchProtocolHost.exe'
236	'2520,SearchIndexer.exe'	'11224,SearchProtocolHost.exe'
237	'2520,SearchIndexer.exe'	'10256,SearchFilterHost.exe'
238	'2520,SearchIndexer.exe'	'11832,SearchFilterHost.exe'
239	'2520,SearchIndexer.exe'	'12480,SearchProtocolHost.exe'
240	'2520,SearchIndexer.exe'	'12688,SearchFilterHost.exe'
241	'2520,SearchIndexer.exe'	'12940,SearchProtocolHost.exe'
242	'2520,SearchIndexer.exe'	'13392,SearchFilterHost.exe'
243	'2520,SearchIndexer.exe'	'16240,SearchProtocolHost.exe'

244	'2520,SearchIndexer.exe'	'16260,SearchFilterHost.exe'
245	'2520,SearchIndexer.exe'	'16296,SearchProtocolHost.exe'
246	'2520,SearchIndexer.exe'	'18180,SearchProtocolHost.exe'
247	'2520,SearchIndexer.exe'	'18240,SearchFilterHost.exe'
248	'2520,SearchIndexer.exe'	'21468,SearchProtocolHost.exe'
249	'2520,SearchIndexer.exe'	'20852,SearchFilterHost.exe'
250	'2520,SearchIndexer.exe'	'21536,SearchProtocolHost.exe'
251	'2520,SearchIndexer.exe'	'21912,SearchFilterHost.exe'
252	'2520,SearchIndexer.exe'	'23540,SearchProtocolHost.exe'
253	'2520,SearchIndexer.exe'	'22744,SearchFilterHost.exe'
254	'2520,SearchIndexer.exe'	'23292,SearchProtocolHost.exe'
255	'2520,SearchIndexer.exe'	'23468,SearchProtocolHost.exe'
256	'2520,SearchIndexer.exe'	'22732,SearchFilterHost.exe'
257	'2520,SearchIndexer.exe'	'23940,SearchProtocolHost.exe'
258	'2520,SearchIndexer.exe'	'23960,SearchFilterHost.exe'
259	'2520,SearchIndexer.exe'	'24536,SearchProtocolHost.exe'
260	'2520,SearchIndexer.exe'	'23748,SearchFilterHost.exe'
261	'2520,SearchIndexer.exe'	'24932,SearchProtocolHost.exe'
262	'2520,SearchIndexer.exe'	'25224,SearchFilterHost.exe'
263	'2520,SearchIndexer.exe'	'24820,SearchProtocolHost.exe'
264	'2520,SearchIndexer.exe'	'25320,SearchProtocolHost.exe'
265	'2520,SearchIndexer.exe'	'24692,SearchFilterHost.exe'
266	'2520,SearchIndexer.exe'	'26440,SearchProtocolHost.exe'
267	'2520,SearchIndexer.exe'	'26472,SearchFilterHost.exe'
268	'2520,SearchIndexer.exe'	'28544,SearchProtocolHost.exe'
269	'2520,SearchIndexer.exe'	'28612,SearchFilterHost.exe'
270	'2520,SearchIndexer.exe'	'29216,SearchProtocolHost.exe'
271	'2520,SearchIndexer.exe'	'29236,SearchFilterHost.exe'
272	'2520,SearchIndexer.exe'	'30488,SearchProtocolHost.exe'
273	'2520,SearchIndexer.exe'	'30576,SearchFilterHost.exe'
274	'2520,SearchIndexer.exe'	'32592,SearchProtocolHost.exe'
275	'2520,SearchIndexer.exe'	'32724,SearchFilterHost.exe'
276	'2520,SearchIndexer.exe'	'33324,SearchProtocolHost.exe'
277	'2520,SearchIndexer.exe'	'33360,SearchFilterHost.exe'
278	'2728,wmpnetwk.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
279	'2728,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
280	'2728,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
281	'2360,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
282	'2316,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
283	'2668,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
284	'620,XXX'	'1580,driver_endpoint_netconn.exe'

285	'1580,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
286	'2044,svchost.exe'	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
287	'2044,svchost.exe'	tdh.dll,C:WindowsSystem32dh.dll'
288	'2044,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
289	'2620,WMIADAP.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
290	'2620,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
291	'2276,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
292	'3044,taskhost.exe'	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
293	'3468,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
294	'3468,cmd.exe'	'3596,java.exe'
295	'3480,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
296	'3596,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
297	'3596,java.exe'	'8616,java.exe'
298	'4064,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
299	'4064,firefox.exe'	'3980,firefox.exe'
300	'4064,firefox.exe'	'4356,pingsender.exe'
301	'3980,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
302	'4356,pingsender.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
303	'4376,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
304	'4436,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
305	'4436,firefox.exe'	'4604,firefox.exe'
306	'4604,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
307	'4984,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
308	'4984,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
309	'4984,cmd.exe'	'4920,NETSTAT.EXE'
310	'5028,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
311	'4920,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
312	'4920,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
313	'5224,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
314	'5404,Wireshark.exe'	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
315	'5404,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
316	'5404,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
317	'5404,Wireshark.exe'	'5500,gspawn-win64-helper.exe'
318	'5404,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
319	'5404,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
320	'5404,Wireshark.exe'	'5592,dumpcap.exe'
321	'5404,Wireshark.exe'	'12948,dumpcap.exe'
322	'5500,gspawn-win64-helper.exe'	'5512,androiddump.exe'
323	'5592,dumpcap.exe'	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
324	'5600,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'

325	'5696,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
326	'5696,FoxitReader.exe'	'5860,FoxitReaderUpdater.exe'
327	'5860,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
328	'5848,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
329	'6104,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
330	'6080,XXX'	'6160,bash.exe'
331	'6160,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
332	'8016,SearchProtocolHost.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
333	'8152,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
334	'7364,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
335	'7604,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
336	'7636,XXX'	'7548,svchost.exe'
337	'7548,svchost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
338	'7264,XXX'	'7268,issch.exe'
339	'7268,issch.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
340	'7268,issch.exe'	'7680,iexplore.exe'
341	'7680,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
342	'7680,iexplore.exe'	'7628,iexplore.exe'
343	'7680,iexplore.exe'	'15232,iexplore.exe'
344	'7628,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
345	'7528,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
346	'7528,SearchProtocolHost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
347	'7528,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
348	'7528,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
349	'7324,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
350	'7324,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
351	'8420,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
352	'9000,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
353	'9000,iexplore.exe'	'8336,iexplore.exe'
354	'9000,iexplore.exe'	'10232,iexplore.exe'
355	'9000,iexplore.exe'	'10960,iexplore.exe'
356	'8336,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
357	'8616,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
358	'8624,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
359	'8984,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
360	'8984,SearchProtocolHost.exe'	'RpcRtRemote.dll,C:Windowssystem32RpcRtRemote.dll'
361	'8984,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
362	'8984,SearchProtocolHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
363	'10232,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
364	'10960,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
365	'11224,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'

366	'10256,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
367	'11832,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
368	'12068,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
369	'12948,dumpcap.exe'	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
370	'12960,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
371	'13016,taskmgr.exe'	'13288,taskmgr.exe'
372	'13212,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
373	'13252,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
374	'13288,taskmgr.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
375	'13288,taskmgr.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
376	'13288,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
377	'13288,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
378	'13288,taskmgr.exe'	'WINMM.dll,C:Windowssystem32WINMM.dll'
379	'12480,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
380	'12688,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
381	'13032,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
382	'13032,soffice.exe'	'13016,soffice.bin'
383	'13016,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
384	'12512,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
385	'12940,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
386	'13392,SearchFilterHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
387	'14316,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
388	'15232,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
389	'15232,iexplore.exe'	'15316,iexplore.exe'
390	'15316,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
391	'15568,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
392	'15948,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
393	'16016,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
394	'16180,StikyNot.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
395	'16240,SearchProtocolHost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
396	'16240,SearchProtocolHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
397	'16260,SearchFilterHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
398	'16260,SearchFilterHost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
399	'16260,SearchFilterHost.exe'	'rtffilt.dll,C:Windowssystem32rtffilt.dll'
400	'16296,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
401	'15884,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
402	'13448,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
403	'16544,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
404	'16648,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
405	'16752,taskhost.exe'	'XmlLite.dll,C:Windowssystem32XmlLite.dll'

406	'16420,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
407	'16420,iexplore.exe'	'15804,iexplore.exe'
408	'16420,iexplore.exe'	'18392,iexplore.exe'
409	'16420,iexplore.exe'	'18556,iexplore.exe'
410	'16420,iexplore.exe'	'28388,iexplore.exe'
411	'16420,iexplore.exe'	'26260,iexplore.exe'
412	'15804,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
413	'18180,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
414	'18180,SearchProtocolHost.exe'	'RpcRtRemote.dll,C:Windowssystem32RpcRtRemote.dll'
415	'18180,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
416	'18240,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
417	'18392,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
418	'18556,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
419	'20360,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
420	'20360,cmd.exe'	'20472,java.exe'
421	'20368,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
422	'20472,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
423	'20472,java.exe'	'24200,java.exe'
424	'20424,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
425	'20424,firefox.exe'	'20584,firefox.exe'
426	'20584,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
427	'21356,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
428	'21356,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
429	'21356,cmd.exe'	'21412,NETSTAT.EXE'
430	'21364,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
431	'21412,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
432	'21412,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
433	'21468,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
434	'21468,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
435	'20852,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
436	'20840,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
437	'20840,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
438	'20840,Wireshark.exe'	'21532,dumpcap.exe'
439	'20840,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
440	'20840,Wireshark.exe'	'21660,dumpcap.exe'
441	'20840,Wireshark.exe'	'25340,dumpcap.exe'
442	'21660,dumpcap.exe'	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
443	'21668,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
444	'21536,SearchProtocolHost.exe'	'RpcRtRemote.dll,C:Windowssystem32RpcRtRemote.dll'
445	'21536,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
446	'21536,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'

447	'21912,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
448	'22136,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
449	'22464,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
450	'21692,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
451	'21712,XXX'	'21980,bash.exe'
452	'21980,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
453	'21980,bash.exe'	'22092,bash.exe'
454	'22092,bash.exe'	'22324,bash.exe'
455	'22324,bash.exe'	'22424,hostname.exe'
456	'23540,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
457	'23540,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
458	'22744,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
459	'23292,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
460	'23292,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
461	'23368,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
462	'23468,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
463	'23468,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
464	'22732,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
465	'23940,SearchProtocolHost.exe'	'RpcRtRemote.dll,C:Windowssystem32RpcRtRemote.dll'
466	'23940,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
467	'23940,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
468	'23960,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
469	'24200,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
470	'24228,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
471	'24536,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
472	'23748,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
473	'24932,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
474	'24932,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
475	'24932,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
476	'25224,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
477	'25224,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
478	'25340,dumpcap.exe'	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
479	'25348,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
480	'24584,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
481	'24820,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
482	'25216,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
483	'25216,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
484	'25216,Wireshark.exe'	'24800,dumpcap.exe'
485	'25216,Wireshark.exe'	'5236,dumpcap.exe'
486	'24800,dumpcap.exe'	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
487	'24808,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'

488	'25320,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
489	'24692,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
490	'25584,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
491	'5236,dumpcap.exe'	'dhcpcsvc.DLL,C:WindowsSystem32dhcpcsvc.DLL'
492	'25980,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
493	'25980,soffice.exe'	'25988,soffice.bin'
494	'25988,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
495	'26260,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
496	'26440,SearchProtocolHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
497	'26472,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
498	'25848,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
499	'25848,firefox.exe'	'26660,firefox.exe'
500	'26660,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
501	'26984,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
502	'27316,taskhost.exe'	'XmlLite.dll,C:Windowssystem32XmlLite.dll'
503	'27484,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
504	'27484,firefox.exe'	'26632,firefox.exe'
505	'26632,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
506	'28544,SearchProtocolHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
507	'28612,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
508	'27872,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
509	'28676,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
510	'28928,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
511	'29108,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
512	'29216,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
513	'29216,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
514	'29216,SearchProtocolHost.exe'	'ehtrace.dll,C:Windowsehomeehtrace.dll'
515	'29236,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
516	'29236,SearchFilterHost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
517	'29380,dllhost.exe'	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
518	'29484,XXX'	'29508,setup_wm.exe'
519	'29508,setup_wm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
520	'29508,setup_wm.exe'	'29620,wmplayer.exe'
521	'29620,wmplayer.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
522	'30688,Wireshark.exe'	'29728,gspawn-win64-helper.exe'
523	'29728,gspawn-win64-helper.exe'	'29732,androiddump.exe'
524	'28776,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
525	'29100,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
526	'29372,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
527	'29576,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
528	'27832,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'

529	'29104,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
530	'29520,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
531	'29420,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
532	'29744,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
533	'29900,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
534	'29900,firefox.exe'	'30056,firefox.exe'
535	'30056,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
536	'30488,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
537	'30576,SearchFilterHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
538	'30588,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
539	'30588,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
540	'30596,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
541	'31384,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
542	'31384,firefox.exe'	'31544,firefox.exe'
543	'31544,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
544	'31676,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
545	'31380,calc.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
546	'31756,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
547	'31816,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
548	'31816,iexplore.exe'	'31888,iexplore.exe'
549	'31888,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
550	'32592,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
551	'32592,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
552	'32724,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
553	'32400,WinRAR.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
554	'32844,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
555	'32944,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
556	'32980,dllhost.exe'	'wups2.dll,C:Windowssystem32wups2.dll'
557	'33016,slui.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
558	'33156,TrustedInstaller.exe'	'CbsApi.dll,C:WindowsservicingCbsApi.dll'
559	'33220,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
560	'33324,SearchProtocolHost.exe'	'profapi.dll,C:WindowsSystem32profapi.dll'
561	'33360,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'

7.2.17 Nivdort Malware – Instance 1

Table 127: Nivdort Malware Instance 1 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,XXX'
6	'360,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'400,wininit.exe'
9	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
10	'412,XXX'
11	'424,csrss.exe'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'508,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'524,lsm.exe'
17	'516,lsass.exe'
18	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
19	'628,svchost.exe'
20	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
21	'692,VBoxService.exe'
22	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
23	'756,svchost.exe'
24	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
25	'844,svchost.exe'
26	'netutils.dll,C:WindowsSystem32netutils.dll'
27	'888,svchost.exe'
28	'credssp.dll,C:WindowsSystem32credssp.dll'
29	'932,svchost.exe'
30	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
31	'AVRT.dll,c:windowssystem32AVRT.dll'
32	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
33	'376,svchost.exe'
34	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
35	'304,svchost.exe'

36	'msxml3.dll,C:WindowsSystem32msxml3.dll'
37	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
38	'1140,spoolsv.exe'
39	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
40	'1188,svchost.exe'
41	'1352,svchost.exe'
42	'SXS.DLL,C:Windowssystem32SXS.DLL'
43	'1400,FoxitConnectedPDFService.exe'
44	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
45	'1904,svchost.exe'
46	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
47	'1032,dwm.exe'
48	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
49	'916,XXX'
50	'1408,explorer.exe'
51	thumbcache.dll,C:Windowssystem32humbcache.dll'
52	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
53	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
54	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
55	tquery.dll,C:Windowssystem32query.dll'
56	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
57	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
58	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
59	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
60	'2068,taskhost.exe'
61	'midimap.dll,C:Windowssystem32midimap.dll'
62	'2168,VBoxTray.exe'
63	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
64	'2192,MySQLNotifier.exe'
65	'2236,XXX'
66	'2284,jusched.exe'
67	'2468,WmiPrvSE.exe'
68	'VERSION.dll,C:Windowssystem32VERSION.dll'
69	'2628,SearchIndexer.exe'
70	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
71	'2816,wmpnetwk.exe'
72	'provsvc.dll,C:WindowsSystem32provsvc.dll'
73	'2572,sppsvc.exe'
74	'2344,svchost.exe'
75	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
76	'636,mintty.exe'

77	'apphelp.dll,C:Windowssystem32apphelp.dll'
78	'2760,conhost.exe'
79	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
80	'2328,XXX'
81	'2996,bash.exe'
82	'authz.dll,C:Windowssystem32authz.dll'
83	'3308,audiodg.exe'
84	'3128,XXX'
85	'3876,taskmgr.exe'
86	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
87	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
88	'3264,XXX'
89	'2376,driver_endpoint_netconn.exe'
90	'2528,cmd.exe'
91	'1568,conhost.exe'
92	'3828,java.exe'
93	'3440,firefox.exe'
94	'2984,firefox.exe'
95	'3508,cmd.exe'
96	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
97	'3272,conhost.exe'
98	'3588,NETSTAT.EXE'
99	'winrnr.dll,C:WindowsSystem32winrnr.dll'
100	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
101	'3688,notepad++.exe'
102	'752,Wireshark.exe'
103	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
104	'1968,conhost.exe'
105	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
106	'1988,dumpcap.exe'
107	'3116,slui.exe'
108	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
109	'4252,FoxitReader.exe'
110	'4316,FoxitReaderUpdater.exe'
111	'4468,SearchProtocolHost.exe'
112	'4488,SearchFilterHost.exe'
113	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
114	'4908,mintty.exe'
115	'4944,conhost.exe'
116	'4960,XXX'
117	'4976,bash.exe'

118	'5060,bash.exe'
119	'5100,simpress.exe'
120	'5092,soffice.exe'
121	'5096,soffice.bin'
122	'16704,audiodg.exe'
123	'5368,java.exe'
124	'5372,conhost.exe'
125	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
126	'5644,SearchProtocolHost.exe'
127	'5684,SearchFilterHost.exe'
128	'6028,dumpcap.exe'
129	'6032,conhost.exe'
130	'5744,audiodg.exe'
131	'5332,dllhost.exe'
132	'5852,dllhost.exe'
133	'5972,consent.exe'
134	'5880,dllhost.exe'
135	'IDStore.dll,C:WindowsSystem32IDStore.dll'
136	'6000,dllhost.exe'
137	'1300,sample.exe'
138	'8460,tdtxjtat.exe'
139	'9628,ylxgpkkuiif.exe'
140	'8204,dllhost.exe'
141	'7316,tdtxjtat.exe'
142	'11492,ylxgpkkuiif.exe'
143	'13424,tdtxjtat.exe'
144	'14580,ylxgpkkuiif.exe'
145	'16312,iexplore.exe'
146	'16356,iexplore.exe'
147	'16624,SearchProtocolHost.exe'
148	'profapi.dll,C:Windowssystem32profapi.dll'
149	'16644,SearchFilterHost.exe'
150	'17048,firefox.exe'
151	'3452,firefox.exe'
152	'17632,firefox.exe'
153	'17800,firefox.exe'
154	'18128,tdtxjtat.exe'
155	'19028,ylxgpkkuiif.exe'
156	'20464,taskhost.exe'
157	'20852,firefox.exe'
158	'21028,firefox.exe'

159	'356,XXX'
160	'368,csrss.exe'
161	'408,wininit.exe'
162	'416,XXX'
163	'428,csrss.exe'
164	'464,winlogon.exe'
165	'512,services.exe'
166	'528,lsm.exe'
167	'520,lsass.exe'
168	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
169	'836,svchost.exe'
170	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
171	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
172	'992,audiodg.exe'
173	'920,svchost.exe'
174	'appinfo.dll,c:windowssystem32appinfo.dll'
175	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
176	'wer.dll,C:Windowssystem32wer.dll'
177	'rasman.dll,C:Windowssystem32rasman.dll'
178	'bcryptprimitives.dll,C:Windowssystem32cryptprimitives.dll'
179	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
180	'740,svchost.exe'
181	'psapi.dll,C:Windowssystem32psapi.dll'
182	'SensApi.dll,C:Windowssystem32SensApi.dll'
183	'1228,spoolsv.exe'
184	'1256,svchost.exe'
185	'1376,svchost.exe'
186	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
187	'1444,FoxitConnectedPDFService.exe'
188	'1556,tdtxjtat.exe'
189	'2636,ylxgpkkuiif.exe'
190	'4084,svchost.exe'
191	'4448,taskhost.exe'
192	'4496,sppsvc.exe'
193	'4656,userinit.exe'
194	'4664,dwm.exe'
195	'4688,explorer.exe'
196	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
197	'browcli.dll,C:Windowssystem32rowcli.dll'
198	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
199	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'

200	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
201	'4788,VBoxTray.exe'
202	'4808,MySQLNotifier.exe'
203	'4828,XXX'
204	'4976,jusched.exe'
205	'5100,WmiPrvSE.exe'
206	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
207	'4564,SearchIndexer.exe'
208	'ktmw32.dll,C:Windowssystem32ktmw32.dll'
209	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
210	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
211	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
212	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
213	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
214	'4284,wmpnetwk.exe'
215	'iertutil.dll,C:Windowssystem32iertutil.dll'
216	'4948,SearchProtocolHost.exe'
217	'336,SearchFilterHost.exe'
218	'1120,mintty.exe'
219	'4316,conhost.exe'
220	'1128,XXX'
221	'4832,bash.exe'
222	'4956,driver_endpoint_netconn.exe'
223	'4292,taskmgr.exe'
224	'5152,dllhost.exe'
225	'5188,dllhost.exe'
226	'5220,taskmgr.exe'
227	'5668,dllhost.exe'
228	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
229	'5784,XXX'
230	'5812,setup_wm.exe'
231	'5892,XXX'
232	'5924,unregmp2.exe'
233	'5936,unregmp2.exe'
234	'5960,wmplayer.exe'
235	'5612,StikyNot.exe'
236	'5980,svchost.exe'
237	tdh.dll,C:WindowsSystem32dh.dll'
238	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
239	'6176,SearchFilterHost.exe'
240	'actxprxy.dll,C:Windowssystem32actxprxy.dll'

241	'msxml6.dll,C:WindowsSystem32msxml6.dll'
242	'rtffilt.dll,C:Windowssystem32rtffilt.dll'
243	'6204,SearchProtocolHost.exe'
244	'slc.dll,C:Windowssystem32slc.dll'
245	'ehtrace.dll,C:Windowsehomeehtrace.dll'
246	'6328,WMIADAP.exe'
247	'6356,WmiPrvSE.exe'
248	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
249	'6528,taskmgr.exe'
250	'6608,dllhost.exe'
251	'6648,dllhost.exe'
252	'6680,taskmgr.exe'
253	'7036,tdtxjtat.exe'
254	'2388,ylxgpkkuiif.exe'
255	'7348,cmd.exe'
256	'7364,conhost.exe'
257	'7468,java.exe'
258	'7908,SearchProtocolHost.exe'
259	'7928,SearchFilterHost.exe'
260	'8008,firefox.exe'
261	'8180,firefox.exe'
262	'7396,tdtxjtat.exe'
263	'9244,ylxgpkkuiif.exe'
264	'10840,cmd.exe'
265	'10848,conhost.exe'
266	'10884,NETSTAT.EXE'
267	'11008,notepad++.exe'
268	'11112,Wireshark.exe'
269	'11180,gspawn-win64-helper.exe'
270	'11192,androiddump.exe'
271	'msimtf.dll,C:Windowssystem32msimtf.dll'
272	'10492,conhost.exe'
273	'8172,dumpcap.exe'
274	'11196,SearchProtocolHost.exe'
275	'11216,SearchFilterHost.exe'
276	'12028,FoxitReader.exe'
277	'12180,SearchProtocolHost.exe'
278	'12200,SearchFilterHost.exe'
279	'11920,mintty.exe'
280	'11984,conhost.exe'
281	'12000,XXX'

282	'12020,bash.exe'
283	'11780,simpress.exe'
284	'11784,soffice.exe'
285	'11860,soffice.bin'
286	'11992,tdtxjtat.exe'
287	'13340,ylxgpkkuiif.exe'
288	'15116,SearchProtocolHost.exe'
289	'15136,SearchFilterHost.exe'
290	'15328,java.exe'
291	'15316,conhost.exe'
292	'14708,SearchProtocolHost.exe'
293	'14760,SearchFilterHost.exe'
294	'14912,conhost.exe'
295	'14932,dumpcap.exe'
296	'15660,tdtxjtat.exe'
297	'16816,ylxgpkkuiif.exe'
298	'18788,tdtxjtat.exe'
299	'19892,ylxgpkkuiif.exe'
300	'21496,SearchProtocolHost.exe'
301	'21300,SearchFilterHost.exe'
302	'mlang.dll,C:Windowssystem32mlang.dll'
303	'22148,WinRAR.exe'
304	'22236,soffice.exe'
305	'22244,soffice.bin'
306	'21348,slui.exe'
307	'22008,tdtxjtat.exe'
308	'23544,ylxgpkkuiif.exe'
309	'24876,taskhost.exe'

Table 128: Nivdort Malware Instance 1 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'352,XXX'	'360,csrss.exe'
5	'352,XXX'	'400,wininit.exe'
6	'360,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'400,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
8	'400,wininit.exe'	'508,services.exe'
9	'400,wininit.exe'	'524,lsm.exe'
10	'400,wininit.exe'	'516,lsass.exe'
11	'412,XXX'	'424,csrss.exe'
12	'412,XXX'	'460,winlogon.exe'
13	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
14	'424,csrss.exe'	'2760,conhost.exe'
15	'424,csrss.exe'	'1568,conhost.exe'
16	'424,csrss.exe'	'3272,conhost.exe'
17	'424,csrss.exe'	'1968,conhost.exe'
18	'424,csrss.exe'	'4944,conhost.exe'
19	'424,csrss.exe'	'5372,conhost.exe'
20	'424,csrss.exe'	'6032,conhost.exe'
21	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
22	'508,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
23	'508,services.exe'	'628,svchost.exe'
24	'508,services.exe'	'692,VBoxService.exe'
25	'508,services.exe'	'756,svchost.exe'
26	'508,services.exe'	'844,svchost.exe'
27	'508,services.exe'	'888,svchost.exe'
28	'508,services.exe'	'932,svchost.exe'
29	'508,services.exe'	'376,svchost.exe'
30	'508,services.exe'	'304,svchost.exe'
31	'508,services.exe'	'1140,spoolsv.exe'
32	'508,services.exe'	'1188,svchost.exe'
33	'508,services.exe'	'1352,svchost.exe'
34	'508,services.exe'	'1400,FoxitConnectedPDFService.exe'
35	'508,services.exe'	'1904,svchost.exe'
36	'508,services.exe'	'2068,taskhost.exe'
37	'508,services.exe'	'2628,SearchIndexer.exe'
38	'508,services.exe'	'2816,wmpnetwk.exe'
39	'508,services.exe'	'2572,sppsvc.exe'

40	'508,services.exe'	'2344,svchost.exe'
41	'508,services.exe'	'8460,tdtxjtat.exe'
42	'508,services.exe'	'20464,taskhost.exe'
43	'524,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
44	'516,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
45	'628,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
46	'628,svchost.exe'	'2468,WmiPrvSE.exe'
47	'628,svchost.exe'	'3116,slui.exe'
48	'628,svchost.exe'	'5332,dllhost.exe'
49	'628,svchost.exe'	'5852,dllhost.exe'
50	'628,svchost.exe'	'5880,dllhost.exe'
51	'628,svchost.exe'	'6000,dllhost.exe'
52	'628,svchost.exe'	'8204,dllhost.exe'
53	'628,svchost.exe'	'5100,WmiPrvSE.exe'
54	'628,svchost.exe'	'5152,dllhost.exe'
55	'628,svchost.exe'	'5188,dllhost.exe'
56	'628,svchost.exe'	'5668,dllhost.exe'
57	'628,svchost.exe'	'6356,WmiPrvSE.exe'
58	'628,svchost.exe'	'6608,dllhost.exe'
59	'628,svchost.exe'	'6648,dllhost.exe'
60	'628,svchost.exe'	'21348,slui.exe'
61	'692,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
62	'756,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
63	'844,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
64	'844,svchost.exe'	'3308,audiodg.exe'
65	'844,svchost.exe'	'16704,audiodg.exe'
66	'844,svchost.exe'	'5744,audiodg.exe'
67	'888,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
68	'888,svchost.exe'	'1032,dwm.exe'
69	'888,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
70	'888,svchost.exe'	'4664,dwm.exe'
71	'932,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
72	'932,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
73	'932,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
74	'932,svchost.exe'	'5972,consent.exe'
75	'376,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
76	'304,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
77	'304,svchost.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
78	'304,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
79	'304,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
80	'304,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'

81	'304,svchost.exe'	'bcryptprimitives.dll,C:Windowssystem32cryptprimitives.dll'
82	'304,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
83	'1140,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
84	'1188,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
85	'1352,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
86	'1400,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
87	'1904,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
88	'1032,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
89	'916,XXX'	'1408,explorer.exe'
90	'1408,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
91	'1408,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
92	'1408,explorer.exe'	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
93	'1408,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
94	'1408,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
95	'1408,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
96	'1408,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
97	'1408,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
98	'1408,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
99	'1408,explorer.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
100	'1408,explorer.exe'	'2168,VBoxTray.exe'
101	'1408,explorer.exe'	'2192,MySQLNotifier.exe'
102	'1408,explorer.exe'	'636,mintty.exe'
103	'1408,explorer.exe'	'2528,cmd.exe'
104	'1408,explorer.exe'	'3440,firefox.exe'
105	'1408,explorer.exe'	'3508,cmd.exe'
106	'1408,explorer.exe'	'3688,notepad++.exe'
107	'1408,explorer.exe'	'752,Wireshark.exe'
108	'1408,explorer.exe'	'4252,FoxitReader.exe'
109	'1408,explorer.exe'	'4908,mintty.exe'
110	'1408,explorer.exe'	'1300,sample.exe'
111	'1408,explorer.exe'	'16312,iexplore.exe'
112	'1408,explorer.exe'	'17048,firefox.exe'
113	'1408,explorer.exe'	'17632,firefox.exe'
114	'1408,explorer.exe'	'20852,firefox.exe'
115	'2068,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
116	'2168,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
117	'2192,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
118	'2236,XXX'	'2284,jusched.exe'
119	'2284,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
120	'2468,WmiPrvSE.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'

121	'2468,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
122	'2468,WmiPrvSE.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
123	'2628,SearchIndexer.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
124	'2628,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
125	'2628,SearchIndexer.exe'	'4468,SearchProtocolHost.exe'
126	'2628,SearchIndexer.exe'	'4488,SearchFilterHost.exe'
127	'2628,SearchIndexer.exe'	'5644,SearchProtocolHost.exe'
128	'2628,SearchIndexer.exe'	'5684,SearchFilterHost.exe'
129	'2628,SearchIndexer.exe'	'16624,SearchProtocolHost.exe'
130	'2628,SearchIndexer.exe'	'16644,SearchFilterHost.exe'
131	'2816,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
132	'2572,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
133	'2344,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
134	'636,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
135	'2760,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
136	'2328,XXX'	'2996,bash.exe'
137	'2996,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
138	'3128,XXX'	'3876,taskmgr.exe'
139	'3876,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
140	'3876,taskmgr.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
141	'3264,XXX'	'2376,driver_endpoint_netconn.exe'
142	'2376,driver_endpoint_netconn .exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
143	'2528,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
144	'2528,cmd.exe'	'3828,java.exe'
145	'1568,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
146	'3828,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
147	'3828,java.exe'	'5368,java.exe'
148	'3440,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
149	'3440,firefox.exe'	'2984,firefox.exe'
150	'3440,firefox.exe'	'5100,simpress.exe'
151	'2984,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
152	'3508,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
153	'3508,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
154	'3508,cmd.exe'	'3588,NETSTAT.EXE'
155	'3272,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
156	'3588,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
157	'3588,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
158	'3688,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
159	'752,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
160	'752,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
161	'752,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'

162	'752,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
163	'752,Wireshark.exe'	'1988,dumpcap.exe'
164	'752,Wireshark.exe'	'6028,dumpcap.exe'
165	'1968,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
166	'1988,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
167	'3116,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
168	'4252,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
169	'4252,FoxitReader.exe'	'4316,FoxitReaderUpdater.exe'
170	'4316,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
171	'4468,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
172	'4488,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
173	'4908,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
174	'4944,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
175	'4944,conhost.exe'	'4956,driver_endpoint_netconn.exe'
176	'4960,XXX'	'4976,bash.exe'
177	'4976,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
178	'4976,bash.exe'	'5060,bash.exe'
179	'5100,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
180	'5100,simpress.exe'	'5092,soffice.exe'
181	'5092,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
182	'5092,soffice.exe'	'5096,soffice.bin'
183	'5096,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
184	'5368,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
185	'5372,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
186	'5644,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
187	'5684,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
188	'6028,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
189	'6032,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
190	'5332,dllhost.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
191	'5852,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
192	'5972,consent.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
193	'5880,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
194	'6000,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
195	'1300,sample.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
196	'8460,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
197	'8460,tdtxjtat.exe'	'9628,ylxgpkkuiif.exe'
198	'9628,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
199	'9628,ylxgpkkuiif.exe'	'7316,tdtxjtat.exe'
200	'8204,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
201	'7316,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
202	'7316,tdtxjtat.exe'	'11492,ylxgpkkuiif.exe'

203	'11492,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
204	'11492,ylxgpkkuiif.exe'	'13424,tdtxjtat.exe'
205	'13424,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
206	'13424,tdtxjtat.exe'	'14580,ylxgpkkuiif.exe'
207	'14580,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
208	'14580,ylxgpkkuiif.exe'	'18128,tdtxjtat.exe'
209	'16312,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
210	'16312,iexplore.exe'	'16356,iexplore.exe'
211	'16356,iexplore.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
212	'16624,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
213	'16644,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
214	'17048,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
215	'17048,firefox.exe'	'3452,firefox.exe'
216	'3452,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
217	'17632,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
218	'17632,firefox.exe'	'17800,firefox.exe'
219	'17800,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
220	'18128,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
221	'18128,tdtxjtat.exe'	'19028,ylxgpkkuiif.exe'
222	'19028,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
223	'20464,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
224	'20852,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
225	'20852,firefox.exe'	'21028,firefox.exe'
226	'21028,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
227	'356,XXX'	'368,csrss.exe'
228	'356,XXX'	'408,wininit.exe'
229	'368,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
230	'408,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
231	'408,wininit.exe'	'512,services.exe'
232	'408,wininit.exe'	'528,lsm.exe'
233	'408,wininit.exe'	'520,lsass.exe'
234	'416,XXX'	'428,csrss.exe'
235	'416,XXX'	'464,winlogon.exe'
236	'428,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
237	'428,csrss.exe'	'4316,conhost.exe'
238	'428,csrss.exe'	'7364,conhost.exe'
239	'428,csrss.exe'	'10848,conhost.exe'
240	'428,csrss.exe'	'10492,conhost.exe'
241	'428,csrss.exe'	'11984,conhost.exe'
242	'428,csrss.exe'	'15316,conhost.exe'
243	'428,csrss.exe'	'14912,conhost.exe'

244	'464,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
245	'464,winlogon.exe'	'4656,userinit.exe'
246	'512,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
247	'512,services.exe'	'628,svchost.exe'
248	'512,services.exe'	'692,VBoxService.exe'
249	'512,services.exe'	'756,svchost.exe'
250	'512,services.exe'	'888,svchost.exe'
251	'512,services.exe'	'304,svchost.exe'
252	'512,services.exe'	'836,svchost.exe'
253	'512,services.exe'	'920,svchost.exe'
254	'512,services.exe'	'740,svchost.exe'
255	'512,services.exe'	'1228,spoolsv.exe'
256	'512,services.exe'	'1256,svchost.exe'
257	'512,services.exe'	'1376,svchost.exe'
258	'512,services.exe'	'1444,FoxitConnectedPDFService.exe'
259	'512,services.exe'	'1556,tdtxjtat.exe'
260	'512,services.exe'	'4084,svchost.exe'
261	'512,services.exe'	'4448,taskhost.exe'
262	'512,services.exe'	'4496,sppsvc.exe'
263	'512,services.exe'	'4564,SearchIndexer.exe'
264	'512,services.exe'	'4284,wmpnetwk.exe'
265	'512,services.exe'	'5980,svchost.exe'
266	'512,services.exe'	'24876,taskhost.exe'
267	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
268	'520,lsass.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
269	'520,lsass.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
270	'836,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
271	'836,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
272	'836,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
273	'836,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
274	'836,svchost.exe'	'992,audiodg.exe'
275	'920,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
276	'920,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
277	'920,svchost.exe'	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
278	'920,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
279	'920,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
280	'920,svchost.exe'	'6328,WMIADAP.exe'
281	'740,svchost.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
282	'740,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
283	'1228,spoolsv.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
284	'1256,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'

285	'1256,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
286	'1376,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
287	'1376,svchost.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
288	'1376,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
289	'1376,svchost.exe'	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
290	'1444,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
291	'1556,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
292	'1556,tdtxjtat.exe'	'2636,ylxgpkkuiif.exe'
293	'2636,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
294	'2636,ylxgpkkuiif.exe'	'7036,tdtxjtat.exe'
295	'4084,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
296	'4448,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
297	'4496,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
298	'4656,userinit.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
299	'4656,userinit.exe'	'4688,explorer.exe'
300	'4664,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
301	'4688,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
302	'4688,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
303	'4688,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
304	'4688,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
305	'4688,explorer.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
306	'4688,explorer.exe'	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
307	'4688,explorer.exe'	'browcli.dll,C:Windowssystem32rowcli.dll'
308	'4688,explorer.exe'	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
309	'4688,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
310	'4688,explorer.exe'	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
311	'4688,explorer.exe'	'4788,VBoxTray.exe'
312	'4688,explorer.exe'	'4808,MySQLNotifier.exe'
313	'4688,explorer.exe'	'1120,mintty.exe'
314	'4688,explorer.exe'	'4292,taskmgr.exe'
315	'4688,explorer.exe'	'5612,StikyNot.exe'
316	'4688,explorer.exe'	'6528,taskmgr.exe'
317	'4688,explorer.exe'	'7348,cmd.exe'
318	'4688,explorer.exe'	'8008,firefox.exe'
319	'4688,explorer.exe'	'10840,cmd.exe'
320	'4688,explorer.exe'	'11008,notepad++.exe'
321	'4688,explorer.exe'	'11112,Wireshark.exe'
322	'4688,explorer.exe'	'12028,FoxitReader.exe'
323	'4688,explorer.exe'	'11920,mintty.exe'
324	'4688,explorer.exe'	'22148,WinRAR.exe'
325	'4688,explorer.exe'	'22236,soffice.exe'

326	'4788,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
327	'4808,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
328	'4828,XXX'	'4976,jusched.exe'
329	'4976,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
330	'5100,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
331	'5100,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
332	'5100,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
333	'4564,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
334	'4564,SearchIndexer.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
335	'4564,SearchIndexer.exe'	'ktmw32.dll,C:Windowssystem32ktmw32.dll'
336	'4564,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
337	'4564,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
338	'4564,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
339	'4564,SearchIndexer.exe'	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
340	'4564,SearchIndexer.exe'	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
341	'4564,SearchIndexer.exe'	'4948,SearchProtocolHost.exe'
342	'4564,SearchIndexer.exe'	'336,SearchFilterHost.exe'
343	'4564,SearchIndexer.exe'	'6176,SearchFilterHost.exe'
344	'4564,SearchIndexer.exe'	'6204,SearchProtocolHost.exe'
345	'4564,SearchIndexer.exe'	'7908,SearchProtocolHost.exe'
346	'4564,SearchIndexer.exe'	'7928,SearchFilterHost.exe'
347	'4564,SearchIndexer.exe'	'11196,SearchProtocolHost.exe'
348	'4564,SearchIndexer.exe'	'11216,SearchFilterHost.exe'
349	'4564,SearchIndexer.exe'	'12180,SearchProtocolHost.exe'
350	'4564,SearchIndexer.exe'	'12200,SearchFilterHost.exe'
351	'4564,SearchIndexer.exe'	'15116,SearchProtocolHost.exe'
352	'4564,SearchIndexer.exe'	'15136,SearchFilterHost.exe'
353	'4564,SearchIndexer.exe'	'14708,SearchProtocolHost.exe'
354	'4564,SearchIndexer.exe'	'14760,SearchFilterHost.exe'
355	'4564,SearchIndexer.exe'	'21496,SearchProtocolHost.exe'
356	'4564,SearchIndexer.exe'	'21300,SearchFilterHost.exe'
357	'4284,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
358	'4284,wmpnetwk.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
359	'4948,SearchProtocolHost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
360	'4948,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
361	'4948,SearchProtocolHost.exe'	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
362	'336,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
363	'1120,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
364	'4316,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
365	'1128,XXX'	'4832,bash.exe'
366	'4832,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'

367	'4956,driver_endpoint_netconn .exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
368	'4292,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
369	'4292,taskmgr.exe'	'5220,taskmgr.exe'
370	'5152,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
371	'5188,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
372	'5220,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
373	'5668,dllhost.exe'	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
374	'5784,XXX'	'5812,setup_wm.exe'
375	'5812,setup_wm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
376	'5812,setup_wm.exe'	'5936,unregmp2.exe'
377	'5812,setup_wm.exe'	'5960,wmplayer.exe'
378	'5892,XXX'	'5924,unregmp2.exe'
379	'5960,wmplayer.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
380	'5612,StikyNot.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
381	'5980,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
382	'5980,svchost.exe'	tdh.dll,C:WindowsSystem32dh.dll'
383	'5980,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
384	'6176,SearchFilterHost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
385	'6176,SearchFilterHost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
386	'6176,SearchFilterHost.exe'	'rtffilt.dll,C:Windowssystem32rtffilt.dll'
387	'6204,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
388	'6204,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'
389	'6204,SearchProtocolHost.exe'	'ehtrace.dll,C:Windowsehomeehtrace.dll'
390	'6328,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
391	'6328,WMIADAP.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
392	'6356,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
393	'6528,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
394	'6528,taskmgr.exe'	'6680,taskmgr.exe'
395	'6608,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
396	'6648,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
397	'6680,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
398	'7036,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
399	'7036,tdtxjtat.exe'	'2388,ylxgpkkuiif.exe'
400	'2388,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
401	'2388,ylxgpkkuiif.exe'	'7396,tdtxjtat.exe'
402	'7348,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
403	'7348,cmd.exe'	'7468,java.exe'
404	'7364,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
405	'7468,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
406	'7468,java.exe'	'15328,java.exe'
407	'7908,SearchProtocolHost.exe'	'slc.dll,C:Windowssystem32slc.dll'

408	'7928,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
409	'8008,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
410	'8008,firefox.exe'	'8180,firefox.exe'
411	'8008,firefox.exe'	'11780,simpress.exe'
412	'8180,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
413	'7396,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
414	'7396,tdtxjtat.exe'	'9244,ylxgpkkuiif.exe'
415	'9244,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
416	'9244,ylxgpkkuiif.exe'	'11992,tdtxjtat.exe'
417	'10840,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
418	'10840,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
419	'10840,cmd.exe'	'10884,NETSTAT.EXE'
420	'10848,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
421	'10884,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
422	'10884,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
423	'11008,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
424	'11112,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
425	'11112,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
426	'11112,Wireshark.exe'	'11180,gspawn-win64-helper.exe'
427	'11112,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
428	'11112,Wireshark.exe'	'8172,dumpcap.exe'
429	'11112,Wireshark.exe'	'14932,dumpcap.exe'
430	'11180,gspawn-win64-helper.exe'	'11192,androiddump.exe'
431	'10492,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
432	'8172,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
433	'11196,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
434	'11216,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
435	'12028,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
436	'12180,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
437	'12200,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
438	'11920,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
439	'11984,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
440	'12000,XXX'	'12020,bash.exe'
441	'12020,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
442	'11780,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
443	'11780,simpress.exe'	'11784,soffice.exe'
444	'11784,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
445	'11784,soffice.exe'	'11860,soffice.bin'
446	'11860,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
447	'11992,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
448	'11992,tdtxjtat.exe'	'13340,ylxgpkkuiif.exe'

449	'13340,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
450	'13340,ylxgpkkuiif.exe'	'15660,tdtxjtat.exe'
451	'15116,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
452	'15136,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
453	'15328,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
454	'15316,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
455	'14708,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
456	'14760,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
457	'14912,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
458	'14932,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
459	'15660,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
460	'15660,tdtxjtat.exe'	'16816,ylxgpkkuiif.exe'
461	'16816,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
462	'16816,ylxgpkkuiif.exe'	'18788,tdtxjtat.exe'
463	'18788,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
464	'18788,tdtxjtat.exe'	'19892,ylxgpkkuiif.exe'
465	'19892,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
466	'19892,ylxgpkkuiif.exe'	'22008,tdtxjtat.exe'
467	'21496,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
468	'21300,SearchFilterHost.exe'	'mlang.dll,C:Windowssystem32mlang.dll'
469	'22148,WinRAR.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
470	'22236,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
471	'22236,soffice.exe'	'22244,soffice.bin'
472	'22244,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
473	'21348,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
474	'22008,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
475	'22008,tdtxjtat.exe'	'23544,ylxgpkkuiif.exe'
476	'23544,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
477	'24876,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'

7.2.18 Nivdort Malware – Instance 2

Table 129: Nivdort Malware Instance 2 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'264,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'328,XXX'
6	'336,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'376,XXX'
9	'396,csrss.exe'
10	'384,wininit.exe'
11	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
12	'436,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'480,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'504,lsm.exe'
17	'496,lsass.exe'
18	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
19	'616,svchost.exe'
20	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
21	'676,VBoxService.exe'
22	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
23	'740,svchost.exe'
24	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
25	'824,svchost.exe'
26	'netutils.dll,C:WindowsSystem32netutils.dll'
27	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
28	'888,svchost.exe'
29	'credssp.dll,C:WindowsSystem32credssp.dll'
30	'912,svchost.exe'
31	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
32	'rasman.dll,C:Windowssystem32rasman.dll'
33	'AVRT.dll,c:windowssystem32AVRT.dll'
34	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
35	'332,svchost.exe'

36	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
37	'964,svchost.exe'
38	'msxml3.dll,C:WindowsSystem32msxml3.dll'
39	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
40	'1156,spoolsv.exe'
41	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
42	'1188,svchost.exe'
43	'1312,svchost.exe'
44	'SXS.DLL,C:Windowssystem32SXS.DLL'
45	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
46	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
47	'1352,FoxitConnectedPDFService.exe'
48	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
49	'1736,svchost.exe'
50	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
51	'1292,dwm.exe'
52	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
53	'1244,XXX'
54	'876,explorer.exe'
55	'thumbcache.dll,C:Windowssystem32humbcache.dll'
56	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
57	tquery.dll,C:Windowssystem32query.dll'
58	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
59	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
60	'MLANG.dll,C:Windowssystem32MLANG.dll'
61	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
62	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'
63	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
64	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
65	'shacct.dll,C:WindowsSystem32shacct.dll'
66	'1116,taskhost.exe'
67	'midimap.dll,C:Windowssystem32midimap.dll'
68	'1536,MySQLNotifier.exe'
69	'2012,VBoxTray.exe'
70	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
71	'1548,driver_endpoint_netconn.exe'
72	'808,jusched.exe'
73	'2220,WmiPrvSE.exe'
74	'VERSION.dll,C:Windowssystem32VERSION.dll'
75	'2456,SearchIndexer.exe'
76	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'

77	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
78	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
79	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
80	'2688,wmpnetwk.exe'
81	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
82	'msdmo.dll,C:Windowssystem32msdmo.dll'
83	'provsvc.dll,C:WindowsSystem32provsvc.dll'
84	'iertutil.dll,C:Windowssystem32iertutil.dll'
85	'812,sppsvc.exe'
86	'1820,svchost.exe'
87	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
88	'2944,XXX'
89	'2872,taskmgr.exe'
90	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
91	'DUser.dll,C:Windowssystem32DUser.dll'
92	'1992,mintty.exe'
93	'apphelp.dll,C:Windowssystem32apphelp.dll'
94	'2052,conhost.exe'
95	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
96	'1676,audiodg.exe'
97	'2820,XXX'
98	'2492,bash.exe'
99	'authz.dll,C:Windowssystem32authz.dll'
100	'2564,XXX'
101	'1308,WmiPrvSE.exe'
102	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
103	'3324,cmd.exe'
104	'3332,conhost.exe'
105	'3436,java.exe'
106	'3888,firefox.exe'
107	'3256,firefox.exe'
108	'4264,audiodg.exe'
109	'4548,cmd.exe'
110	'4556,conhost.exe'
111	'4588,NETSTAT.EXE'
112	'winrnr.dll,C:WindowsSystem32winrnr.dll'
113	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
114	'4720,notepad++.exe'
115	'4892,Wireshark.exe'
116	'4956,gspawn-win64-helper.exe'
117	'4968,androiddump.exe'

118	'5056,dumpcap.exe'
119	'5064,conhost.exe'
120	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
121	'4672,FoxitReader.exe'
122	'6892,audiodg.exe'
123	'7312,pingsender.exe'
124	'7328,conhost.exe'
125	'5136,FoxitReaderUpdater.exe'
126	'6004,mintty.exe'
127	'6040,conhost.exe'
128	'6076,bash.exe'
129	'5428,bash.exe'
130	'5444,bash.exe'
131	'5460,tzset.exe'
132	'6056,XXX'
133	'5844,simpress.exe'
134	'5948,soffice.exe'
135	'5996,soffice.bin'
136	'6692,java.exe'
137	'6700,conhost.exe'
138	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
139	'6412,svchost.exe'
140	'7116,dllhost.exe'
141	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
142	'7556,svchost.exe'
143	'7844,consent.exe'
144	'7932,dllhost.exe'
145	'7980,dllhost.exe'
146	'7680,consent.exe'
147	'8012,sample.exe'
148	'10024,tdtxjtat.exe'
149	'11184,ylxgpkkuiif.exe'
150	'9908,tdtxjtat.exe'
151	'8964,ylxgpkkuiif.exe'
152	'14372,taskhost.exe'
153	'14660,soffice.exe'
154	'14668,soffice.bin'
155	'21684,audiodg.exe'
156	'14876,Wireshark.exe'
157	'14960,gspawn-win64-helper.exe'
158	'14972,androiddump.exe'

159	'15060,dumpcap.exe'
160	'15068,conhost.exe'
161	'15176,dumpcap.exe'
162	'15184,conhost.exe'
163	'14968,tdtxjtat.exe'
164	'16348,ylxgpkkuiif.exe'
165	'18008,SearchProtocolHost.exe'
166	'profapi.dll,C:Windowssystem32profapi.dll'
167	'18028,SearchFilterHost.exe'
168	'18092,firefox.exe'
169	'18260,firefox.exe'
170	'18836,cmd.exe'
171	'18844,conhost.exe'
172	'18480,slui.exe'
173	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
174	'18952,tdtxjtat.exe'
175	'19984,ylxgpkkuiif.exe'
176	'21632,dllhost.exe'
177	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
178	'21800,XXX'
179	'21836,setup_wm.exe'
180	'21908,XXX'
181	'21940,unregmp2.exe'
182	'21972,unregmp2.exe'
183	'21980,wmplayer.exe'
184	'22216,SearchProtocolHost.exe'
185	'ehtrace.dll,C:Windowsehomeehtrace.dll'
186	'22236,SearchFilterHost.exe'
187	'msxml6.dll,C:WindowsSystem32msxml6.dll'
188	'22592,taskmgr.exe'
189	'22680,dllhost.exe'
190	'IDStore.dll,C:WindowsSystem32IDStore.dll'
191	'22720,dllhost.exe'
192	'22752,taskmgr.exe'
193	'24752,dllhost.exe'
194	'24788,dllhost.exe'
195	'25072,consent.exe'
196	'23160,dllhost.exe'
197	'23364,dllhost.exe'
198	'23428,dllhost.exe'
199	'23500,dllhost.exe'

200	'23536,ylxgpkkuiif.exe'
201	'24676,XXX'
202	'24828,migwiz.exe'
203	'WINTRUST.dll,C:Windowssystem32WINTRUST.dll'
204	'25132,dllhost.exe'
205	'25168,dllhost.exe'
206	'25200,ylxgpkkuiif.exe'
207	'27532,ylxgpkkuiif.exe'
208	'27168,notepad++.exe'
209	'27212,dllhost.exe'
210	'27428,SearchProtocolHost.exe'
211	'27256,SearchFilterHost.exe'
212	'27656,mspaint.exe'
213	'oleacc.dll,C:Windowssystem32oleacc.dll'
214	'27688,svchost.exe'
215	'27812,cmd.exe'
216	'27820,conhost.exe'
217	'27928,java.exe'
218	'28252,firefox.exe'
219	'28476,firefox.exe'
220	'28212,firefox.exe'
221	'28268,firefox.exe'
222	'29096,cmd.exe'
223	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
224	'29104,conhost.exe'
225	'29136,NETSTAT.EXE'
226	'29268,notepad++.exe'
227	'29384,Wireshark.exe'
228	'29528,dumpcap.exe'
229	'29536,conhost.exe'
230	'29036,tdtxjtat.exe'
231	'30380,ylxgpkkuiif.exe'
232	'32348,FoxitReader.exe'
233	'38752,audiodg.exe'
234	'32192,mintty.exe'
235	'32232,conhost.exe'
236	'32248,XXX'
237	'32268,bash.exe'
238	'32376,simpress.exe'
239	'32568,soffice.exe'
240	'32564,soffice.bin'

241	'31964,svchost.exe'
242	'33464,tdtxjtat.exe'
243	'34160,ylxgpkkuiif.exe'
244	'35352,java.exe'
245	'35368,conhost.exe'
246	'36648,tdtxjtat.exe'
247	'37468,ylxgpkkuiif.exe'
248	'39712,tdtxjtat.exe'
249	'40868,ylxgpkkuiif.exe'
250	'42692,slui.exe'
251	'42064,tdtxjtat.exe'
252	'44044,ylxgpkkuiif.exe'
253	'45712,dumpcap.exe'
254	'45720,conhost.exe'
255	'45488,taskhost.exe'
256	'46284,tdtxjtat.exe'
257	'47420,ylxgpkkuiif.exe'
258	'49300,tdtxjtat.exe'
259	'50456,ylxgpkkuiif.exe'
260	'52328,tdtxjtat.exe'
261	'53484,ylxgpkkuiif.exe'
262	'54884,slui.exe'
263	'55504,tdtxjtat.exe'
264	'56656,ylxgpkkuiif.exe'

Table 130: Nivdort Malware Instance 2 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'264,smss.exe'
3	'264,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'328,XXX'	'336,csrss.exe'
5	'328,XXX'	'384,wininit.exe'
6	'336,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'376,XXX'	'396,csrss.exe'
8	'376,XXX'	'436,winlogon.exe'
9	'396,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
10	'396,csrss.exe'	'2052,conhost.exe'
11	'396,csrss.exe'	'3332,conhost.exe'
12	'396,csrss.exe'	'4556,conhost.exe'
13	'396,csrss.exe'	'5064,conhost.exe'
14	'396,csrss.exe'	'7328,conhost.exe'
15	'396,csrss.exe'	'6040,conhost.exe'
16	'396,csrss.exe'	'6700,conhost.exe'
17	'396,csrss.exe'	'15068,conhost.exe'
18	'396,csrss.exe'	'15184,conhost.exe'
19	'396,csrss.exe'	'18844,conhost.exe'
20	'396,csrss.exe'	'27820,conhost.exe'
21	'396,csrss.exe'	'29104,conhost.exe'
22	'396,csrss.exe'	'29536,conhost.exe'
23	'396,csrss.exe'	'32232,conhost.exe'
24	'396,csrss.exe'	'35368,conhost.exe'
25	'396,csrss.exe'	'45720,conhost.exe'
26	'384,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
27	'384,wininit.exe'	'480,services.exe'
28	'384,wininit.exe'	'504,lsm.exe'
29	'384,wininit.exe'	'496,lsass.exe'
30	'436,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
31	'480,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
32	'480,services.exe'	'616,svchost.exe'
33	'480,services.exe'	'676,VBoxService.exe'
34	'480,services.exe'	'740,svchost.exe'
35	'480,services.exe'	'824,svchost.exe'
36	'480,services.exe'	'888,svchost.exe'
37	'480,services.exe'	'912,svchost.exe'
38	'480,services.exe'	'332,svchost.exe'
39	'480,services.exe'	'964,svchost.exe'

40	'480,services.exe'	'1156,spoolsv.exe'
41	'480,services.exe'	'1188,svchost.exe'
42	'480,services.exe'	'1312,svchost.exe'
43	'480,services.exe'	'1352,FoxitConnectedPDFService.exe'
44	'480,services.exe'	'1736,svchost.exe'
45	'480,services.exe'	'1116,taskhost.exe'
46	'480,services.exe'	'2456,SearchIndexer.exe'
47	'480,services.exe'	'2688,wmpnetwk.exe'
48	'480,services.exe'	'812,sppsvc.exe'
49	'480,services.exe'	'1820,svchost.exe'
50	'480,services.exe'	'6412,svchost.exe'
51	'480,services.exe'	'7556,svchost.exe'
52	'480,services.exe'	'10024,tdtxjtat.exe'
53	'480,services.exe'	'14372,taskhost.exe'
54	'480,services.exe'	'27688,svchost.exe'
55	'480,services.exe'	'31964,svchost.exe'
56	'480,services.exe'	'45488,taskhost.exe'
57	'504,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
58	'496,lsass.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
59	'616,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
60	'616,svchost.exe'	'2220,WmiPrvSE.exe'
61	'616,svchost.exe'	'1308,WmiPrvSE.exe'
62	'616,svchost.exe'	'7116,dllhost.exe'
63	'616,svchost.exe'	'7932,dllhost.exe'
64	'616,svchost.exe'	'7980,dllhost.exe'
65	'616,svchost.exe'	'18480,slui.exe'
66	'616,svchost.exe'	'21632,dllhost.exe'
67	'616,svchost.exe'	'22680,dllhost.exe'
68	'616,svchost.exe'	'22720,dllhost.exe'
69	'616,svchost.exe'	'24752,dllhost.exe'
70	'616,svchost.exe'	'24788,dllhost.exe'
71	'616,svchost.exe'	'23160,dllhost.exe'
72	'616,svchost.exe'	'23364,dllhost.exe'
73	'616,svchost.exe'	'23428,dllhost.exe'
74	'616,svchost.exe'	'23500,dllhost.exe'
75	'616,svchost.exe'	'25132,dllhost.exe'
76	'616,svchost.exe'	'25168,dllhost.exe'
77	'616,svchost.exe'	'27212,dllhost.exe'
78	'616,svchost.exe'	'42692,slui.exe'
79	'616,svchost.exe'	'54884,slui.exe'
80	'676,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'

81	'740,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
82	'824,svchost.exe'	'netutils.dll,C:WindowsSystem32netutils.dll'
83	'824,svchost.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
84	'824,svchost.exe'	'1676,audiodg.exe'
85	'824,svchost.exe'	'4264,audiodg.exe'
86	'824,svchost.exe'	'6892,audiodg.exe'
87	'824,svchost.exe'	'21684,audiodg.exe'
88	'824,svchost.exe'	'38752,audiodg.exe'
89	'888,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
90	'888,svchost.exe'	'1292,dwm.exe'
91	'912,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
92	'912,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
93	'912,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
94	'912,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
95	'912,svchost.exe'	'7844,consent.exe'
96	'912,svchost.exe'	'7680,consent.exe'
97	'912,svchost.exe'	'25072,consent.exe'
98	'332,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
99	'964,svchost.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
100	'964,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
101	'1156,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
102	'1188,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
103	'1312,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
104	'1312,svchost.exe'	'udhisapi.dll,C:Windowssystem32udhisapi.dll'
105	'1312,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
106	'1352,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
107	'1736,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
108	'1292,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
109	'1244,XXX'	'876,explorer.exe'
110	'876,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
111	'876,explorer.exe'	'mfplat.DLL,C:WindowsSystem32mfplat.DLL'
112	'876,explorer.exe'	thumbcache.dll,C:Windowssystem32humbcache.dll'
113	'876,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
114	'876,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
115	'876,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
116	'876,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
117	'876,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
118	'876,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
119	'876,explorer.exe'	'PhotoMetadataHandler.dll,C:Windowssystem32PhotoMetadataHandler.dll'

120	'876,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
121	'876,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
122	'876,explorer.exe'	'shacct.dll,C:WindowsSystem32shacct.dll'
123	'876,explorer.exe'	'1536,MySQLNotifier.exe'
124	'876,explorer.exe'	'2012,VBoxTray.exe'
125	'876,explorer.exe'	'1992,mintty.exe'
126	'876,explorer.exe'	'3324,cmd.exe'
127	'876,explorer.exe'	'3888,firefox.exe'
128	'876,explorer.exe'	'4548,cmd.exe'
129	'876,explorer.exe'	'4720,notepad++.exe'
130	'876,explorer.exe'	'4892,Wireshark.exe'
131	'876,explorer.exe'	'4672,FoxitReader.exe'
132	'876,explorer.exe'	'6004,mintty.exe'
133	'876,explorer.exe'	'8012,sample.exe'
134	'876,explorer.exe'	'14660,soffice.exe'
135	'876,explorer.exe'	'14876,Wireshark.exe'
136	'876,explorer.exe'	'18092,firefox.exe'
137	'876,explorer.exe'	'18836,cmd.exe'
138	'876,explorer.exe'	'22592,taskmgr.exe'
139	'876,explorer.exe'	'23536,ylxgpkkuiif.exe'
140	'876,explorer.exe'	'25200,ylxgpkkuiif.exe'
141	'876,explorer.exe'	'27168,notepad++.exe'
142	'876,explorer.exe'	'27656,mspaint.exe'
143	'876,explorer.exe'	'27812,cmd.exe'
144	'876,explorer.exe'	'28252,firefox.exe'
145	'876,explorer.exe'	'28212,firefox.exe'
146	'876,explorer.exe'	'29096,cmd.exe'
147	'876,explorer.exe'	'29268,notepad++.exe'
148	'876,explorer.exe'	'29384,Wireshark.exe'
149	'876,explorer.exe'	'32348,FoxitReader.exe'
150	'876,explorer.exe'	'32192,mintty.exe'
151	'1116,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
152	'1536,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
153	'2012,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
154	'1548,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
155	'1548,driver_endpoint_netconn.exe'	'808,jusched.exe'
156	'808,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
157	'2220,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
158	'2220,WmiPrvSE.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
159	'2456,SearchIndexer.exe'	'msxml3.dll,C:WindowsSystem32msxml3.dll'
160	'2456,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'

161	'2456,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
162	'2456,SearchIndexer.exe'	'NLSData0000.dll,C:WindowsSystem32NLSData0000.dll'
163	'2456,SearchIndexer.exe'	'NLSLexicons0021.dll,C:WindowsSystem32NLSLexicons0021.dll'
164	'2456,SearchIndexer.exe'	'18008,SearchProtocolHost.exe'
165	'2456,SearchIndexer.exe'	'18028,SearchFilterHost.exe'
166	'2456,SearchIndexer.exe'	'22216,SearchProtocolHost.exe'
167	'2456,SearchIndexer.exe'	'22236,SearchFilterHost.exe'
168	'2456,SearchIndexer.exe'	'27428,SearchProtocolHost.exe'
169	'2456,SearchIndexer.exe'	'27256,SearchFilterHost.exe'
170	'2688,wmpnetwk.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
171	'2688,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
172	'2688,wmpnetwk.exe'	'msdmo.dll,C:Windowssystem32msdmo.dll'
173	'2688,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
174	'2688,wmpnetwk.exe'	'iertutil.dll,C:Windowssystem32iertutil.dll'
175	'812,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
176	'1820,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
177	'2944,XXX'	'2872,taskmgr.exe'
178	'2872,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
179	'2872,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
180	'1992,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
181	'2052,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
182	'2820,XXX'	'2492,bash.exe'
183	'2492,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
184	'2564,XXX'	'1548,driver_endpoint_netconn.exe'
185	'1308,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
186	'3324,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
187	'3324,cmd.exe'	'3436,java.exe'
188	'3332,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
189	'3436,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
190	'3436,java.exe'	'6692,java.exe'
191	'3888,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
192	'3888,firefox.exe'	'3256,firefox.exe'
193	'3888,firefox.exe'	'7312,pingsender.exe'
194	'3888,firefox.exe'	'5844,simpress.exe'
195	'3256,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
196	'4548,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
197	'4548,cmd.exe'	'4588,NETSTAT.EXE'
198	'4556,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
199	'4588,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
200	'4588,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
201	'4720,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

202	'4892,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
203	'4892,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
204	'4892,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
205	'4892,Wireshark.exe'	'4956,gspawn-win64-helper.exe'
206	'4892,Wireshark.exe'	'5056,dumpcap.exe'
207	'4956,gspawn-win64-helper.exe'	'4968,androiddump.exe'
208	'5056,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
209	'5064,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
210	'4672,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
211	'4672,FoxitReader.exe'	'5136,FoxitReaderUpdater.exe'
212	'5136,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
213	'6004,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
214	'6040,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
215	'6076,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
216	'6076,bash.exe'	'5428,bash.exe'
217	'5428,bash.exe'	'5444,bash.exe'
218	'5444,bash.exe'	'5460,tzset.exe'
219	'6056,XXX'	'6076,bash.exe'
220	'5844,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
221	'5844,simpress.exe'	'5948,soffice.exe'
222	'5948,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
223	'5948,soffice.exe'	'5996,soffice.bin'
224	'5996,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
225	'6692,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
226	'6700,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
227	'6412,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
228	'7116,dllhost.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
229	'7556,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
230	'7680,consent.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
231	'8012,sample.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
232	'10024,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
233	'10024,tdtxjtat.exe'	'11184,ylxgpkkuiif.exe'
234	'11184,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
235	'11184,ylxgpkkuiif.exe'	'9908,tdtxjtat.exe'
236	'9908,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
237	'9908,tdtxjtat.exe'	'8964,ylxgpkkuiif.exe'
238	'8964,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
239	'8964,ylxgpkkuiif.exe'	'14968,tdtxjtat.exe'
240	'14372,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
241	'14660,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
242	'14660,soffice.exe'	'14668,soffice.bin'

243	'14668,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
244	'14876,Wireshark.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
245	'14876,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
246	'14876,Wireshark.exe'	'14960,gspawn-win64-helper.exe'
247	'14876,Wireshark.exe'	'15060,dumpcap.exe'
248	'14876,Wireshark.exe'	'15176,dumpcap.exe'
249	'14960,gspawn-win64-helper.exe'	'14972,androiddump.exe'
250	'15176,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
251	'15184,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
252	'14968,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
253	'14968,tdtxjtat.exe'	'16348,ylxgpkkuiif.exe'
254	'16348,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
255	'16348,ylxgpkkuiif.exe'	'18952,tdtxjtat.exe'
256	'18008,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
257	'18028,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
258	'18092,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
259	'18092,firefox.exe'	'18260,firefox.exe'
260	'18260,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
261	'18480,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
262	'18952,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
263	'18952,tdtxjtat.exe'	'19984,ylxgpkkuiif.exe'
264	'18952,tdtxjtat.exe'	'27532,ylxgpkkuiif.exe'
265	'19984,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
266	'21632,dllhost.exe'	'WindowsCodecs.dll,C:Windowssystem32WindowsCodecs.dll'
267	'21800,XXX'	'21836,setup_wm.exe'
268	'21836,setup_wm.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
269	'21836,setup_wm.exe'	'21972,unregmp2.exe'
270	'21836,setup_wm.exe'	'21980,wmplayer.exe'
271	'21908,XXX'	'21940,unregmp2.exe'
272	'21980,wmplayer.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
273	'22216,SearchProtocolHost.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
274	'22216,SearchProtocolHost.exe'	'ehtrace.dll,C:Windowsehomeehtrace.dll'
275	'22236,SearchFilterHost.exe'	'msxml6.dll,C:WindowsSystem32msxml6.dll'
276	'22592,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
277	'22592,taskmgr.exe'	'22752,taskmgr.exe'
278	'22680,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
279	'22720,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
280	'22752,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
281	'23160,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
282	'23364,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
283	'23428,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'

284	'23500,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
285	'23536,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
286	'24676,XXX'	'24828,migwiz.exe'
287	'24828,migwiz.exe'	'WINTRUST.dll,C:Windowssystem32WINTRUST.dll'
288	'25132,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
289	'25168,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
290	'25200,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
291	'27532,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
292	'27532,ylxgpkkuiif.exe'	'29036,tdtxjtat.exe'
293	'27168,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
294	'27212,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
295	'27428,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
296	'27256,SearchFilterHost.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
297	'27656,mspaint.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
298	'27688,svchost.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
299	'27812,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
300	'27812,cmd.exe'	'27928,java.exe'
301	'27820,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
302	'27928,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
303	'27928,java.exe'	'35352,java.exe'
304	'28252,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
305	'28252,firefox.exe'	'28476,firefox.exe'
306	'28476,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
307	'28212,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
308	'28212,firefox.exe'	'28268,firefox.exe'
309	'28212,firefox.exe'	'32376,simpress.exe'
310	'28268,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
311	'29096,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
312	'29096,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
313	'29096,cmd.exe'	'29136,NETSTAT.EXE'
314	'29104,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
315	'29136,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
316	'29136,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
317	'29268,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
318	'29384,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
319	'29384,Wireshark.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
320	'29384,Wireshark.exe'	'29528,dumpcap.exe'
321	'29384,Wireshark.exe'	'45712,dumpcap.exe'
322	'29528,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
323	'29536,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
324	'29036,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

325	'29036,tdtxjtat.exe'	'30380,ylxgpkkuiif.exe'
326	'30380,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
327	'30380,ylxgpkkuiif.exe'	'33464,tdtxjtat.exe'
328	'32348,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
329	'32192,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
330	'32232,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
331	'32248,XXX'	'32268,bash.exe'
332	'32268,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
333	'32376,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
334	'32376,simpress.exe'	'32568,soffice.exe'
335	'32568,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
336	'32568,soffice.exe'	'32564,soffice.bin'
337	'32564,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
338	'31964,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
339	'33464,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
340	'33464,tdtxjtat.exe'	'34160,ylxgpkkuiif.exe'
341	'34160,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
342	'34160,ylxgpkkuiif.exe'	'36648,tdtxjtat.exe'
343	'35352,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
344	'35368,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
345	'36648,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
346	'36648,tdtxjtat.exe'	'37468,ylxgpkkuiif.exe'
347	'37468,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
348	'37468,ylxgpkkuiif.exe'	'39712,tdtxjtat.exe'
349	'39712,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
350	'39712,tdtxjtat.exe'	'40868,ylxgpkkuiif.exe'
351	'40868,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
352	'40868,ylxgpkkuiif.exe'	'42064,tdtxjtat.exe'
353	'42064,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
354	'42064,tdtxjtat.exe'	'44044,ylxgpkkuiif.exe'
355	'44044,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
356	'44044,ylxgpkkuiif.exe'	'46284,tdtxjtat.exe'
357	'45712,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
358	'45720,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
359	'45488,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
360	'46284,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
361	'46284,tdtxjtat.exe'	'47420,ylxgpkkuiif.exe'
362	'47420,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
363	'47420,ylxgpkkuiif.exe'	'49300,tdtxjtat.exe'
364	'49300,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
365	'49300,tdtxjtat.exe'	'50456,ylxgpkkuiif.exe'

366	'50456,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
367	'50456,ylxgpkkuiif.exe'	'52328,tdtxjtat.exe'
368	'52328,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
369	'52328,tdtxjtat.exe'	'53484,ylxgpkkuiif.exe'
370	'53484,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
371	'53484,ylxgpkkuiif.exe'	'55504,tdtxjtat.exe'
372	'54884,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
373	'55504,tdtxjtat.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
374	'55504,tdtxjtat.exe'	'56656,ylxgpkkuiif.exe'
375	'56656,ylxgpkkuiif.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

7.2.19 Poweliks Malware – Instance 1

Table 131: Poweliks Malware Instance 1 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'264,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'328,XXX'
6	'336,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'388,wininit.exe'
9	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
10	'376,XXX'
11	'396,csrss.exe'
12	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
13	'436,winlogon.exe'
14	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
15	'484,services.exe'
16	'wship6.dll,C:WindowsSystem32wship6.dll'
17	'500,lsm.exe'
18	'492,lsass.exe'
19	'netutils.dll,C:Windowssystem32netutils.dll'
20	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
21	'608,svchost.exe'
22	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
23	'668,VBoxService.exe'
24	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
25	'720,svchost.exe'
26	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
27	'772,svchost.exe'
28	'872,svchost.exe'
29	'credssp.dll,C:WindowsSystem32credssp.dll'
30	'radardt.dll,C:Windowssystem32radardt.dll'
31	'972,audiodg.exe'
32	'912,svchost.exe'
33	'wer.dll,C:Windowssystem32wer.dll'
34	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
35	'rasman.dll,C:Windowssystem32rasman.dll'

36	'AVRT.dll,c:windowssystem32AVRT.dll'
37	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
38	'344,svchost.exe'
39	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
40	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
41	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
42	'564,svchost.exe'
43	'psapi.dll,C:Windowssystem32psapi.dll'
44	'SensApi.dll,C:Windowssystem32SensApi.dll'
45	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
46	'1148,spoolsv.exe'
47	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
48	'1184,svchost.exe'
49	'diagperf.dll,C:Windowssystem32diagperf.dll'
50	'1320,svchost.exe'
51	'SXS.DLL,C:Windowssystem32SXS.DLL'
52	'1364,FoxitConnectedPDFService.exe'
53	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
54	'1820,svchost.exe'
55	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
56	'1464,taskhost.exe'
57	'midimap.dll,C:Windowssystem32midimap.dll'
58	'1580,sppsvc.exe'
59	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
60	'1912,dwm.exe'
61	'1920,XXX'
62	'540,explorer.exe'
63	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
64	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
65	'tquery.dll,C:Windowssystem32query.dll'
66	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
67	'MLANG.dll,C:Windowssystem32MLANG.dll'
68	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
69	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
70	'1208,VBoxTray.exe'
71	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
72	'1728,MySQLNotifier.exe'
73	'896,XXX'
74	'892,jusched.exe'
75	'2232,WmiPrvSE.exe'
76	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'

77	'2384,SearchIndexer.exe'
78	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
79	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
80	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
81	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
82	'2584,wmpnetwk.exe'
83	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
84	'provsvc.dll,C:WindowsSystem32provsvc.dll'
85	'2748,XXX'
86	'2888,taskmgr.exe'
87	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
88	'DUser.dll,C:Windowssystem32DUser.dll'
89	'2640,svchost.exe'
90	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
91	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
92	'1640,mintty.exe'
93	'apphelp.dll,C:Windowssystem32apphelp.dll'
94	'1660,conhost.exe'
95	'1688,XXX'
96	'1832,bash.exe'
97	'authz.dll,C:Windowssystem32authz.dll'
98	'2868,SearchProtocolHost.exe'
99	'VERSION.dll,C:Windowssystem32VERSION.dll'
100	'1600,SearchFilterHost.exe'
101	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
102	'2480,WMIADAP.exe'
103	'3008,WmiPrvSE.exe'
104	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
105	'904,XXX'
106	'2164,driver_endpoint_netconn.exe'
107	'10924,audiodg.exe'
108	'868,taskhost.exe'
109	'4032,dllhost.exe'
110	'4080,SearchProtocolHost.exe'
111	'profapi.dll,C:Windowssystem32profapi.dll'
112	'3136,SearchFilterHost.exe'
113	'4060,dllhost.exe'
114	'4248,cmd.exe'
115	'4264,conhost.exe'
116	'4372,java.exe'
117	'4732,firefox.exe'

118	'5024,firefox.exe'
119	'4284,pingsender.exe'
120	'4368,conhost.exe'
121	'5192,java.exe'
122	'5200,conhost.exe'
123	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
124	'5256,cmd.exe'
125	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
126	'5264,conhost.exe'
127	'5372,cmd.exe'
128	'5380,conhost.exe'
129	'5484,java.exe'
130	'5608,firefox.exe'
131	'5784,firefox.exe'
132	'5480,conhost.exe'
133	'5532,cmd.exe'
134	'5180,NETSTAT.EXE'
135	'winrnr.dll,C:WindowsSystem32winrnr.dll'
136	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
137	'6280,notepad++.exe'
138	'6408,Wireshark.exe'
139	'6476,gspawn-win64-helper.exe'
140	'6488,androiddump.exe'
141	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
142	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
143	'6556,dumpcap.exe'
144	'6564,conhost.exe'
145	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
146	'6244,FoxitReader.exe'
147	'9088,audiodg.exe'
148	'6460,FoxitReaderUpdater.exe'
149	'6888,mintty.exe'
150	'6968,conhost.exe'
151	'6992,XXX'
152	'7028,bash.exe'
153	'7976,simpress.exe'
154	'8016,soffice.exe'
155	'8024,soffice.bin'
156	'9096,dllhost.exe'
157	'7804,java.exe'
158	'7840,conhost.exe'

159	'8632,consent.exe'
160	'8760,dllhost.exe'
161	'IDStore.dll,C:WindowsSystem32IDStore.dll'
162	'8828,dllhost.exe'
163	'8856,cmd.exe'
164	'8552,rundll32.exe'
165	'8588,powershell.exe'
166	'8600,conhost.exe'
167	'8864,dllhost.exe'
168	'1536,cmd.exe:0'
169	'8872,SearchProtocolHost.exe'
170	'8588,SearchFilterHost.exe'
171	'9436,dumpcap.exe'
172	'9444,conhost.exe'
173	'10024,audiodg.exe'
174	'9616,SearchProtocolHost.exe'
175	'9656,SearchFilterHost.exe'
176	'9744,dllhost.exe'
177	'10060,dllhost.exe'
178	'10188,taskhost.exe'
179	'10780,slui.exe'
180	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
181	'12800,taskhost.exe'
182	'12980,WmiPrvSE.exe'
183	'12936,SearchProtocolHost.exe'
184	'12904,SearchFilterHost.exe'
185	'14216,dllhost.exe'
186	'14252,dllhost.exe'
187	'14332,cmd.exe'
188	'13520,XXX'
189	'13372,dllhost.exe'
190	'13464,cmd.exe:0'
191	'13468,SearchProtocolHost.exe'
192	'14340,SearchFilterHost.exe'
193	'14764,dllhost.exe'
194	'14868,pingsender.exe'
195	'14884,conhost.exe'
196	'15056,cmd.exe'
197	'15064,conhost.exe'
198	'15168,java.exe'
199	'15340,firefox.exe'

200	'14900,firefox.exe'
201	'15948,cmd.exe'
202	'15956,conhost.exe'
203	'15972,NETSTAT.EXE'
204	'16152,notepad++.exe'
205	'16240,Wireshark.exe'
206	'msimtf.dll,C:Windowssystem32msimtf.dll'
207	'15420,dumpcap.exe'
208	'15432,conhost.exe'
209	'16100,FoxitReader.exe'
210	'16760,mintty.exe'
211	'16800,conhost.exe'
212	'16816,XXX'
213	'16836,bash.exe'
214	'16864,simpress.exe'
215	'16856,soffice.exe'
216	'16908,soffice.bin'
217	'20316,taskhost.exe'
218	'19948,slui.exe'
219	'23364,audiodg.exe'
220	'23960,java.exe'
221	'23968,conhost.exe'
222	'24184,LogonUI.exe'
223	'24288,SearchProtocolHost.exe'
224	'24420,SearchFilterHost.exe'
225	'nlhtml.dll,C:Windowssystem32nlhtml.dll'

Table 132: Poweliks Malware Instance 1 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'264,smss.exe'
3	'264,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'328,XXX'	'336,csrss.exe'
5	'328,XXX'	'388,wininit.exe'
6	'336,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'388,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
8	'388,wininit.exe'	'484,services.exe'
9	'388,wininit.exe'	'500,lsm.exe'
10	'388,wininit.exe'	'492,lsass.exe'
11	'376,XXX'	'396,csrss.exe'
12	'376,XXX'	'436,winlogon.exe'
13	'396,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
14	'396,csrss.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
15	'396,csrss.exe'	'1660,conhost.exe'
16	'396,csrss.exe'	'4264,conhost.exe'
17	'396,csrss.exe'	'4368,conhost.exe'
18	'396,csrss.exe'	'5200,conhost.exe'
19	'396,csrss.exe'	'5264,conhost.exe'
20	'396,csrss.exe'	'5380,conhost.exe'
21	'396,csrss.exe'	'5480,conhost.exe'
22	'396,csrss.exe'	'6564,conhost.exe'
23	'396,csrss.exe'	'6968,conhost.exe'
24	'396,csrss.exe'	'7840,conhost.exe'
25	'396,csrss.exe'	'8600,conhost.exe'
26	'396,csrss.exe'	'9444,conhost.exe'
27	'396,csrss.exe'	'14884,conhost.exe'
28	'396,csrss.exe'	'15064,conhost.exe'
29	'396,csrss.exe'	'15956,conhost.exe'
30	'396,csrss.exe'	'15432,conhost.exe'
31	'396,csrss.exe'	'16800,conhost.exe'
32	'396,csrss.exe'	'23968,conhost.exe'
33	'436,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
34	'436,winlogon.exe'	'24184,LogonUI.exe'
35	'484,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
36	'484,services.exe'	'608,svchost.exe'
37	'484,services.exe'	'668,VBoxService.exe'

38	'484,services.exe'	'720,svchost.exe'
39	'484,services.exe'	'772,svchost.exe'
40	'484,services.exe'	'872,svchost.exe'
41	'484,services.exe'	'912,svchost.exe'
42	'484,services.exe'	'344,svchost.exe'
43	'484,services.exe'	'564,svchost.exe'
44	'484,services.exe'	'1148,spoolsv.exe'
45	'484,services.exe'	'1184,svchost.exe'
46	'484,services.exe'	'1320,svchost.exe'
47	'484,services.exe'	'1364,FoxitConnectedPDFService.exe'
48	'484,services.exe'	'1820,svchost.exe'
49	'484,services.exe'	'1464,taskhost.exe'
50	'484,services.exe'	'1580,sppsvc.exe'
51	'484,services.exe'	'2384,SearchIndexer.exe'
52	'484,services.exe'	'2584,wmpnetwk.exe'
53	'484,services.exe'	'2640,svchost.exe'
54	'484,services.exe'	'868,taskhost.exe'
55	'484,services.exe'	'10188,taskhost.exe'
56	'484,services.exe'	'12800,taskhost.exe'
57	'484,services.exe'	'20316,taskhost.exe'
58	'500,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
59	'492,lsass.exe'	'netutils.dll,C:Windowssystem32netutils.dll'
60	'492,lsass.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
61	'608,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
62	'608,svchost.exe'	'2232,WmiPrvSE.exe'
63	'608,svchost.exe'	'3008,WmiPrvSE.exe'
64	'608,svchost.exe'	'4032,dllhost.exe'
65	'608,svchost.exe'	'4060,dllhost.exe'
66	'608,svchost.exe'	'9096,dllhost.exe'
67	'608,svchost.exe'	'8760,dllhost.exe'
68	'608,svchost.exe'	'8828,dllhost.exe'
69	'608,svchost.exe'	'9744,dllhost.exe'
70	'608,svchost.exe'	'10060,dllhost.exe'
71	'608,svchost.exe'	'10780,slui.exe'
72	'608,svchost.exe'	'12980,WmiPrvSE.exe'
73	'608,svchost.exe'	'14216,dllhost.exe'
74	'608,svchost.exe'	'14252,dllhost.exe'
75	'608,svchost.exe'	'14764,dllhost.exe'
76	'608,svchost.exe'	'19948,slui.exe'
77	'668,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
78	'720,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'

79	'772,svchost.exe'	'netutils.dll,C:Windowssystem32netutils.dll'
80	'772,svchost.exe'	'972,audiodg.exe'
81	'772,svchost.exe'	'10924,audiodg.exe'
82	'772,svchost.exe'	'9088,audiodg.exe'
83	'772,svchost.exe'	'10024,audiodg.exe'
84	'772,svchost.exe'	'23364,audiodg.exe'
85	'872,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
86	'872,svchost.exe'	'radardt.dll,C:Windowssystem32radardt.dll'
87	'872,svchost.exe'	'1912,dwm.exe'
88	'912,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
89	'912,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
90	'912,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
91	'912,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
92	'912,svchost.exe'	'wbemprox.dll,C:Windowssystem32wbemwbemprox.dll'
93	'912,svchost.exe'	'2480,WMIADAP.exe'
94	'912,svchost.exe'	'8632,consent.exe'
95	'344,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
96	'344,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
97	'344,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
98	'564,svchost.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
99	'564,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
100	'564,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
101	'1148,spoolsv.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
102	'1184,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
103	'1184,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
104	'1184,svchost.exe'	'diagperf.dll,C:Windowssystem32diagperf.dll'
105	'1320,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
106	'1364,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
107	'1820,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
108	'1464,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
109	'1580,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
110	'1912,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
111	'1920,XXX'	'540,explorer.exe'
112	'540,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
113	'540,explorer.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
114	'540,explorer.exe'	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
115	'540,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
116	'540,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
117	'540,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'

118	'540,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
119	'540,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
120	'540,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
121	'540,explorer.exe'	'1208,VBoxTray.exe'
122	'540,explorer.exe'	'1728,MySQLNotifier.exe'
123	'540,explorer.exe'	'1640,mintty.exe'
124	'540,explorer.exe'	'4248,cmd.exe'
125	'540,explorer.exe'	'4732,firefox.exe'
126	'540,explorer.exe'	'5256,cmd.exe'
127	'540,explorer.exe'	'5372,cmd.exe'
128	'540,explorer.exe'	'5608,firefox.exe'
129	'540,explorer.exe'	'5532,cmd.exe'
130	'540,explorer.exe'	'6280,notepad++.exe'
131	'540,explorer.exe'	'6408,Wireshark.exe'
132	'540,explorer.exe'	'6244,FoxitReader.exe'
133	'540,explorer.exe'	'6888,mintty.exe'
134	'540,explorer.exe'	'8856,cmd.exe'
135	'540,explorer.exe'	'14332,cmd.exe'
136	'540,explorer.exe'	'15056,cmd.exe'
137	'540,explorer.exe'	'15340,firefox.exe'
138	'540,explorer.exe'	'15948,cmd.exe'
139	'540,explorer.exe'	'16152,notepad++.exe'
140	'540,explorer.exe'	'16240,Wireshark.exe'
141	'540,explorer.exe'	'16100,FoxitReader.exe'
142	'540,explorer.exe'	'16760,mintty.exe'
143	'1208,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
144	'1728,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
145	'896,XXX'	'892,jusched.exe'
146	'892,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
147	'2232,WmiPrvSE.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
148	'2232,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
149	'2232,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
150	'2384,SearchIndexer.exe'	'NLSLexicons0003.dll,C:WindowsSystem32NLSLexicons0003.dll'
151	'2384,SearchIndexer.exe'	'ElsLad.dll,C:Windowssystem32ElsLad.dll'
152	'2384,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
153	'2384,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
154	'2384,SearchIndexer.exe'	'2868,SearchProtocolHost.exe'
155	'2384,SearchIndexer.exe'	'1600,SearchFilterHost.exe'
156	'2384,SearchIndexer.exe'	'4080,SearchProtocolHost.exe'
157	'2384,SearchIndexer.exe'	'3136,SearchFilterHost.exe'
158	'2384,SearchIndexer.exe'	'8872,SearchProtocolHost.exe'

159	'2384,SearchIndexer.exe'	'8588,SearchFilterHost.exe'
160	'2384,SearchIndexer.exe'	'9616,SearchProtocolHost.exe'
161	'2384,SearchIndexer.exe'	'9656,SearchFilterHost.exe'
162	'2384,SearchIndexer.exe'	'12936,SearchProtocolHost.exe'
163	'2384,SearchIndexer.exe'	'12904,SearchFilterHost.exe'
164	'2384,SearchIndexer.exe'	'13468,SearchProtocolHost.exe'
165	'2384,SearchIndexer.exe'	'14340,SearchFilterHost.exe'
166	'2384,SearchIndexer.exe'	'24288,SearchProtocolHost.exe'
167	'2384,SearchIndexer.exe'	'24420,SearchFilterHost.exe'
168	'2584,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
169	'2584,wmpnetwk.exe'	'provsvc.dll,C:WindowsSystem32provsvc.dll'
170	'2748,XXX'	'2888,taskmgr.exe'
171	'2888,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
172	'2888,taskmgr.exe'	'DUser.dll,C:Windowssystem32DUser.dll'
173	'2640,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
174	'2640,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
175	'1640,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
176	'1660,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
177	'1688,XXX'	'1832,bash.exe'
178	'1832,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
179	'2868,SearchProtocolHost.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
180	'1600,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
181	'2480,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
182	'2480,WMIADAP.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
183	'3008,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
184	'904,XXX'	'2164,driver_endpoint_netconn.exe'
185	'2164,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
186	'868,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
187	'4032,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
188	'4080,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
189	'3136,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
190	'4060,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
191	'4248,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
192	'4248,cmd.exe'	'4372,java.exe'
193	'4264,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
194	'4372,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
195	'4372,java.exe'	'5192,java.exe'
196	'4732,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
197	'4732,firefox.exe'	'5024,firefox.exe'
198	'4732,firefox.exe'	'4284,pingsender.exe'
199	'5024,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

200	'4284,pingsender.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
201	'4368,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
202	'5192,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
203	'5200,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
204	'5256,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
205	'5264,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
206	'5372,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
207	'5372,cmd.exe'	'5484,java.exe'
208	'5380,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
209	'5484,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
210	'5484,java.exe'	'7804,java.exe'
211	'5608,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
212	'5608,firefox.exe'	'5784,firefox.exe'
213	'5608,firefox.exe'	'7976,simpress.exe'
214	'5608,firefox.exe'	'14868,pingsender.exe'
215	'5784,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
216	'5480,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
217	'5532,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
218	'5532,cmd.exe'	'5180,NETSTAT.EXE'
219	'5180,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
220	'5180,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
221	'6280,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
222	'6408,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
223	'6408,Wireshark.exe'	'6476,gspawn-win64-helper.exe'
224	'6408,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
225	'6408,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
226	'6408,Wireshark.exe'	'6556,dumpcap.exe'
227	'6408,Wireshark.exe'	'9436,dumpcap.exe'
228	'6476,gspawn-win64-helper.exe'	'6488,androiddump.exe'
229	'6556,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
230	'6564,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
231	'6244,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
232	'6244,FoxitReader.exe'	'6460,FoxitReaderUpdater.exe'
233	'6460,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
234	'6888,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
235	'6968,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
236	'6992,XXX'	'7028,bash.exe'
237	'7028,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
238	'7976,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
239	'7976,simpress.exe'	'8016,soffice.exe'
240	'8016,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'

241	'8016,soffice.exe'	'8024,soffice.bin'
242	'8024,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
243	'7804,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
244	'7840,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
245	'8632,consent.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
246	'8760,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
247	'8828,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
248	'8856,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
249	'8856,cmd.exe'	'8552,rundll32.exe'
250	'8856,cmd.exe'	'1536,cmd.exe:0'
251	'8552,rundll32.exe'	'8588,powershell.exe'
252	'8588,powershell.exe'	'8864,dllhost.exe'
253	'8864,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
254	'1536,cmd.exe:0'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
255	'8872,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
256	'8588,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
257	'9436,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
258	'9444,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
259	'9616,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
260	'9656,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
261	'9744,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
262	'10060,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
263	'10188,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
264	'10780,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
265	'12800,taskhost.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
266	'12980,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
267	'12936,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
268	'12904,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
269	'14216,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
270	'14252,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
271	'14332,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
272	'14332,cmd.exe'	'13464,cmd.exe:0'
273	'13520,XXX'	'13372,dllhost.exe'
274	'13372,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
275	'13464,cmd.exe:0'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
276	'13468,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
277	'14340,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
278	'14764,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
279	'15056,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
280	'15056,cmd.exe'	'15168,java.exe'
281	'15064,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'

282	'15168,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
283	'15168,java.exe'	'23960,java.exe'
284	'15340,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
285	'15340,firefox.exe'	'14900,firefox.exe'
286	'15340,firefox.exe'	'16864,simpress.exe'
287	'14900,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
288	'15948,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
289	'15948,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
290	'15948,cmd.exe'	'15972,NETSTAT.EXE'
291	'15956,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
292	'15972,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
293	'15972,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
294	'16152,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
295	'16240,Wireshark.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
296	'16240,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
297	'16240,Wireshark.exe'	'15420,dumpcap.exe'
298	'15420,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
299	'15432,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
300	'16100,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
301	'16760,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
302	'16800,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
303	'16816,XXX'	'16836,bash.exe'
304	'16836,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
305	'16864,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
306	'16864,simpress.exe'	'16856,soffice.exe'
307	'16856,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
308	'16856,soffice.exe'	'16908,soffice.bin'
309	'16908,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
310	'20316,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
311	'19948,slui.exe'	'dwmapi.dll,C:WindowsSystem32dwmapi.dll'
312	'24184,LogonUI.exe'	'rsaenh.dll,C:Windowssystem32rsaenh.dll'
313	'24288,SearchProtocolHost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
314	'24288,SearchProtocolHost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
315	'24420,SearchFilterHost.exe'	'nlhtml.dll,C:Windowssystem32nlhtml.dll'

7.2.20 Poweliks Malware – Instance 2

Table 133: Poweliks Malware Instance 2 - Node IDs and Names.

Node ID	Node Name
1	'0,XXX'
2	'4,System'
3	'288,smss.exe'
4	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
5	'352,XXX'
6	'364,csrss.exe'
7	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
8	'412,XXX'
9	'424,csrss.exe'
10	'404,wininit.exe'
11	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
12	'460,winlogon.exe'
13	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
14	'504,services.exe'
15	'wship6.dll,C:WindowsSystem32wship6.dll'
16	'528,lsm.exe'
17	'520,lsass.exe'
18	'wkscli.dll,C:Windowssystem32wkscli.dll'
19	'636,svchost.exe'
20	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
21	'700,VBoxService.exe'
22	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
23	'764,svchost.exe'
24	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
25	'860,svchost.exe'
26	'winrnr.dll,C:WindowsSystem32winrnr.dll'
27	'904,svchost.exe'
28	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
29	'944,svchost.exe'
30	'rasman.dll,C:Windowssystem32rasman.dll'
31	'AVRT.dll,c:windowssystem32AVRT.dll'
32	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
33	'368,svchost.exe'
34	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
35	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'

36	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
37	'1004,svchost.exe'
38	'SensApi.dll,C:Windowssystem32SensApi.dll'
39	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
40	'1160,spoolsv.exe'
41	'1204,svchost.exe'
42	'1372,svchost.exe'
43	'SXS.DLL,C:Windowssystem32SXS.DLL'
44	'1404,FoxitConnectedPDFService.exe'
45	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
46	'1872,svchost.exe'
47	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
48	'1492,sppsvc.exe'
49	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
50	'1840,svchost.exe'
51	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
52	'1772,SearchIndexer.exe'
53	'NLSLexicons000a.dll,C:WindowsSystem32NLSLexicons000a.dll'
54	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
55	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
56	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
57	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
58	'1636,taskhost.exe'
59	'midimap.dll,C:Windowssystem32midimap.dll'
60	'2356,dwm.exe'
61	'2340,XXX'
62	'2376,explorer.exe'
63	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
64	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
65	'tquery.dll,C:Windowssystem32query.dll'
66	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
67	'MLANG.dll,C:Windowssystem32MLANG.dll'
68	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
69	'2500,VBoxTray.exe'
70	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
71	'2516,MySQLNotifier.exe'
72	'2624,audiodg.exe'
73	'2544,XXX'
74	'2664,jusched.exe'
75	'2868,WmiPrvSE.exe'
76	'WMI.DLL,C:Windowssystem32WMI.DLL'

77	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
78	'1812,wmpnetwk.exe'
79	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
80	'1896,mintty.exe'
81	'apphelp.dll,C:Windowssystem32apphelp.dll'
82	'2396,conhost.exe'
83	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
84	'2848,XXX'
85	'1156,bash.exe'
86	'authz.dll,C:Windowssystem32authz.dll'
87	'2492,XXX'
88	'2756,taskmgr.exe'
89	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
90	'3224,SearchProtocolHost.exe'
91	'VERSION.dll,C:Windowssystem32VERSION.dll'
92	'1684,SearchFilterHost.exe'
93	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
94	'3392,XXX'
95	'3408,driver_endpoint_netconn.exe'
96	'3932,cmd.exe'
97	'3920,conhost.exe'
98	'3172,java.exe'
99	'3260,firefox.exe'
100	'980,firefox.exe'
101	'4112,cmd.exe'
102	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
103	'4120,conhost.exe'
104	'4156,NETSTAT.EXE'
105	'4260,notepad++.exe'
106	'4364,Wireshark.exe'
107	'wimaxmacphy.dll,C:Program FilesWiresharkplugins2.0.5wimaxmacphy.dll'
108	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
109	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
110	'4512,dumpcap.exe'
111	'4520,conhost.exe'
112	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
113	'4932,FoxitReader.exe'
114	'4964,FoxitReaderUpdater.exe'
115	'4416,SearchProtocolHost.exe'
116	'4404,SearchFilterHost.exe'
117	'mssprxy.dll,C:Windowssystem32mssprxy.dll'

118	'4704,mintty.exe'
119	'4792,conhost.exe'
120	'4796,XXX'
121	'4848,bash.exe'
122	'5700,simpress.exe'
123	'5712,soffice.exe'
124	'5720,soffice.bin'
125	'5512,firefox.exe'
126	'6592,audiodg.exe'
127	'7064,java.exe'
128	'7060,conhost.exe'
129	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
130	'6320,dllhost.exe'
131	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
132	'6856,dllhost.exe'
133	'6992,consent.exe'
134	'6328,dllhost.exe'
135	'IDStore.dll,C:WindowsSystem32IDStore.dll'
136	'6656,dllhost.exe'
137	'6752,cmd.exe'
138	'6196,rundll32.exe'
139	'6692,conhost.exe'
140	'7108,powershell.exe'
141	'6844,dllhost.exe'
142	'7464,audiodg.exe'
143	'6772,SearchProtocolHost.exe'
144	'profapi.dll,C:Windowssystem32profapi.dll'
145	'7016,SearchFilterHost.exe'
146	'6808,cmd.exe:0'
147	'7188,SearchProtocolHost.exe'
148	'7196,SearchFilterHost.exe'
149	'7640,svchost.exe'
150	'8516,dumpcap.exe'
151	'8524,conhost.exe'
152	'8588,slui.exe'
153	'8656,dllhost.exe'
154	'8720,notepad.exe'
155	'8884,taskhost.exe'
156	'8904,WinRAR.exe'
157	'7820,StikyNot.exe'
158	'9264,SearchProtocolHost.exe'

159	'9284,SearchFilterHost.exe'
160	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
161	'rtffilt.dll,C:Windowssystem32rtffilt.dll'
162	'9720,pingsender.exe'
163	'9732,conhost.exe'
164	'9320,SearchProtocolHost.exe'
165	'9856,calc.exe'
166	'oleacc.dll,C:Windowssystem32oleacc.dll'
167	'356,XXX'
168	'368,csrss.exe'
169	'408,wininit.exe'
170	'416,XXX'
171	'428,csrss.exe'
172	'464,winlogon.exe'
173	'508,services.exe'
174	'532,lsm.exe'
175	'524,lsass.exe'
176	'netutils.dll,C:Windowssystem32netutils.dll'
177	'632,svchost.exe'
178	'836,svchost.exe'
179	'892,svchost.exe'
180	'credssp.dll,C:WindowsSystem32credssp.dll'
181	'1004,audiodg.exe'
182	'940,svchost.exe'
183	'appinfo.dll,c:windowssystem32appinfo.dll'
184	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
185	'wer.dll,C:Windowssystem32wer.dll'
186	'324,svchost.exe'
187	'996,svchost.exe'
188	'psapi.dll,C:Windowssystem32psapi.dll'
189	'1240,spoolsv.exe'
190	'1268,svchost.exe'
191	'1380,svchost.exe'
192	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
193	'1408,FoxitConnectedPDFService.exe'
194	'1928,svchost.exe'
195	'1512,taskhost.exe'
196	'2076,sppsvc.exe'
197	'2320,userinit.exe'
198	'2328,dwm.exe'
199	'2352,explorer.exe'

200	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
201	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
202	'FunDisc.dll,C:Windowssystem32FunDisc.dll'
203	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
204	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
205	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
206	'2440,VBoxTray.exe'
207	'2452,MySQLNotifier.exe'
208	'2524,StikyNot.exe'
209	'2532,XXX'
210	'2640,jusched.exe'
211	'2776,WmiPrvSE.exe'
212	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
213	'2856,SearchIndexer.exe'
214	'2228,mintty.exe'
215	'2176,conhost.exe'
216	'1352,XXX'
217	'1460,bash.exe'
218	'2424,taskmgr.exe'
219	'1196,wmpnetwk.exe'
220	'2988,XXX'
221	'2152,dllhost.exe'
222	'2300,XXX'
223	'2268,driver_endpoint_netconn.exe'
224	'1112,dllhost.exe'
225	'2620,taskmgr.exe'
226	'2680,dllhost.exe'
227	'3204,svchost.exe'
228	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
229	'3492,dllhost.exe'
230	'3764,SearchProtocolHost.exe'
231	'3784,SearchFilterHost.exe'
232	'3876,dllhost.exe'
233	'4060,soffice.exe'
234	'4076,soffice.bin'
235	'3444,WMIADAP.exe'
236	'3720,WmiPrvSE.exe'
237	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
238	'4556,SearchProtocolHost.exe'
239	'4576,SearchFilterHost.exe'
240	'5044,cmd.exe'

241	'5048,conhost.exe'
242	'4240,java.exe'
243	'5188,firefox.exe'
244	'5364,firefox.exe'
245	'5900,cmd.exe'
246	'5908,conhost.exe'
247	'5944,NETSTAT.EXE'
248	'6076,notepad++.exe'
249	'5516,Wireshark.exe'
250	'msimtf.dll,C:Windowssystem32msimtf.dll'
251	'6116,dumpcap.exe'
252	'5816,conhost.exe'
253	'6160,audiodg.exe'
254	'6632,FoxitReader.exe'
255	'6788,SearchProtocolHost.exe'
256	'6820,SearchFilterHost.exe'
257	'6464,mintty.exe'
258	'6504,conhost.exe'
259	'6540,XXX'
260	'6564,bash.exe'
261	'6940,SearchProtocolHost.exe'
262	'6972,SearchFilterHost.exe'
263	'6444,simpress.exe'
264	'6432,soffice.exe'
265	'6408,soffice.bin'
266	'8288,taskhost.exe'

Table 134: Poweliks Malware Instance 2 - Edge IDs and Names.

Edge ID	Parent Node of Edge	Child Node of Edge
1	'0,XXX'	'4,System'
2	'4,System'	'288,smss.exe'
3	'288,smss.exe'	'ntdll.dll,C:WindowsSYSTEM32ntdll.dll'
4	'352,XXX'	'364,csrss.exe'
5	'352,XXX'	'404,wininit.exe'
6	'364,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
7	'412,XXX'	'424,csrss.exe'
8	'412,XXX'	'460,winlogon.exe'
9	'424,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
10	'424,csrss.exe'	'2396,conhost.exe'
11	'424,csrss.exe'	'3920,conhost.exe'
12	'424,csrss.exe'	'4120,conhost.exe'
13	'424,csrss.exe'	'4520,conhost.exe'
14	'424,csrss.exe'	'4792,conhost.exe'
15	'424,csrss.exe'	'7060,conhost.exe'
16	'424,csrss.exe'	'6692,conhost.exe'
17	'424,csrss.exe'	'8524,conhost.exe'
18	'424,csrss.exe'	'9732,conhost.exe'
19	'404,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
20	'404,wininit.exe'	'504,services.exe'
21	'404,wininit.exe'	'528,lsm.exe'
22	'404,wininit.exe'	'520,lsass.exe'
23	'460,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
24	'504,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
25	'504,services.exe'	'636,svchost.exe'
26	'504,services.exe'	'700,VBoxService.exe'
27	'504,services.exe'	'764,svchost.exe'
28	'504,services.exe'	'860,svchost.exe'
29	'504,services.exe'	'904,svchost.exe'
30	'504,services.exe'	'944,svchost.exe'
31	'504,services.exe'	'368,svchost.exe'
32	'504,services.exe'	'1004,svchost.exe'
33	'504,services.exe'	'1160,spoolsv.exe'
34	'504,services.exe'	'1204,svchost.exe'
35	'504,services.exe'	'1372,svchost.exe'
36	'504,services.exe'	'1404,FoxitConnectedPDFService.exe'
37	'504,services.exe'	'1872,svchost.exe'
38	'504,services.exe'	'1492,sppsvc.exe'
39	'504,services.exe'	'1840,svchost.exe'

40	'504,services.exe'	'1772,SearchIndexer.exe'
41	'504,services.exe'	'1636,taskhost.exe'
42	'504,services.exe'	'1812,wmpnetwk.exe'
43	'504,services.exe'	'7640,svchost.exe'
44	'504,services.exe'	'8884,taskhost.exe'
45	'528,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
46	'520,lsass.exe'	'wkscli.dll,C:Windowssystem32wkscli.dll'
47	'636,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
48	'636,svchost.exe'	'2868,WmiPrvSE.exe'
49	'636,svchost.exe'	'6320,dllhost.exe'
50	'636,svchost.exe'	'6856,dllhost.exe'
51	'636,svchost.exe'	'6328,dllhost.exe'
52	'636,svchost.exe'	'6656,dllhost.exe'
53	'636,svchost.exe'	'8588,slui.exe'
54	'636,svchost.exe'	'8656,dllhost.exe'
55	'700,VBoxService.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
56	'764,svchost.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
57	'860,svchost.exe'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
58	'860,svchost.exe'	'2624,audiodg.exe'
59	'860,svchost.exe'	'6592,audiodg.exe'
60	'860,svchost.exe'	'7464,audiodg.exe'
61	'904,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
62	'904,svchost.exe'	'2356,dwm.exe'
63	'944,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
64	'944,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
65	'944,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
66	'944,svchost.exe'	'6992,consent.exe'
67	'368,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
68	'368,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
69	'368,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
70	'1004,svchost.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
71	'1004,svchost.exe'	'ncrypt.dll,C:Windowssystem32ncrypt.dll'
72	'1160,spoolsv.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
73	'1204,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
74	'1204,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
75	'1372,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
76	'1404,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
77	'1872,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
78	'1492,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
79	'1840,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'

80	'1772,SearchIndexer.exe'	'NLSLexicons000a.dll,C:WindowsSystem32NLSLexicons000a.dll'
81	'1772,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
82	'1772,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
83	'1772,SearchIndexer.exe'	'NLSLexicons000c.dll,C:WindowsSystem32NLSLexicons000c.dll'
84	'1772,SearchIndexer.exe'	'NLSLexicons001b.dll,C:WindowsSystem32NLSLexicons001b.dll'
85	'1772,SearchIndexer.exe'	'3224,SearchProtocolHost.exe'
86	'1772,SearchIndexer.exe'	'1684,SearchFilterHost.exe'
87	'1772,SearchIndexer.exe'	'4416,SearchProtocolHost.exe'
88	'1772,SearchIndexer.exe'	'4404,SearchFilterHost.exe'
89	'1772,SearchIndexer.exe'	'6772,SearchProtocolHost.exe'
90	'1772,SearchIndexer.exe'	'7016,SearchFilterHost.exe'
91	'1772,SearchIndexer.exe'	'7188,SearchProtocolHost.exe'
92	'1772,SearchIndexer.exe'	'7196,SearchFilterHost.exe'
93	'1772,SearchIndexer.exe'	'9264,SearchProtocolHost.exe'
94	'1772,SearchIndexer.exe'	'9284,SearchFilterHost.exe'
95	'1772,SearchIndexer.exe'	'9320,SearchProtocolHost.exe'
96	'1636,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
97	'2356,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
98	'2340,XXX'	'2376,explorer.exe'
99	'2376,explorer.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
100	'2376,explorer.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
101	'2376,explorer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
102	'2376,explorer.exe'	'zipfldr.dll,C:Windowssystem32zipfldr.dll'
103	'2376,explorer.exe'	'MAPI32.dll,C:Windowssystem32MAPI32.dll'
104	'2376,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
105	'2376,explorer.exe'	'wpdshext.dll,C:Windowssystem32wpdshext.dll'
106	'2376,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
107	'2376,explorer.exe'	'fdWNet.dll,C:Windowssystem32fdWNet.dll'
108	'2376,explorer.exe'	'2500,VBoxTray.exe'
109	'2376,explorer.exe'	'2516,MySQLNotifier.exe'
110	'2376,explorer.exe'	'1896,mintty.exe'
111	'2376,explorer.exe'	'3932,cmd.exe'
112	'2376,explorer.exe'	'3260,firefox.exe'
113	'2376,explorer.exe'	'4112,cmd.exe'
114	'2376,explorer.exe'	'4260,notepad++.exe'
115	'2376,explorer.exe'	'4364,Wireshark.exe'
116	'2376,explorer.exe'	'4932,FoxitReader.exe'
117	'2376,explorer.exe'	'4704,mintty.exe'
118	'2376,explorer.exe'	'5512,firefox.exe'
119	'2376,explorer.exe'	'6752,cmd.exe'
120	'2376,explorer.exe'	'8720,notepad.exe'

121	'2376,explorer.exe'	'8904,WinRAR.exe'
122	'2376,explorer.exe'	'7820,StikyNot.exe'
123	'2376,explorer.exe'	'9856,calc.exe'
124	'2500,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
125	'2516,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
126	'2544,XXX'	'2664,jusched.exe'
127	'2664,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
128	'2868,WmiPrvSE.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
129	'2868,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
130	'2868,WmiPrvSE.exe'	'WMI.DLL,C:Windowssystem32WMI.DLL'
131	'2868,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
132	'1812,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
133	'1896,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
134	'2396,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
135	'2848,XXX'	'1156,bash.exe'
136	'1156,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
137	'2492,XXX'	'2756,taskmgr.exe'
138	'2756,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
139	'3224,SearchProtocolHost.exe'	'VERSION.dll,C:Windowssystem32VERSION.dll'
140	'1684,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
141	'3392,XXX'	'3408,driver_endpoint_netconn.exe'
142	'3408,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
143	'3932,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
144	'3932,cmd.exe'	'3172,java.exe'
145	'3920,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
146	'3172,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
147	'3172,java.exe'	'7064,java.exe'
148	'3260,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
149	'3260,firefox.exe'	'980,firefox.exe'
150	'3260,firefox.exe'	'5700,simpress.exe'
151	'3260,firefox.exe'	'9720,pingsender.exe'
152	'980,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
153	'4112,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
154	'4112,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
155	'4112,cmd.exe'	'4156,NETSTAT.EXE'
156	'4120,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
157	'4156,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
158	'4156,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
159	'4260,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
160	'4364,Wireshark.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
161	'4364,Wireshark.exe'	'wimaxmacphy.dll,C:Program FilesWiresharkplugins2.0.5wimaxmacphy.dll'

162	'4364,Wireshark.exe'	'DEVRTL.dll,C:Windowssystem32DEVRTL.dll'
163	'4364,Wireshark.exe'	'qtaccessiblewidgets.dll,C:Program FilesWiresharkaccessibleqtaccessiblewidgets.dll'
164	'4364,Wireshark.exe'	'4512,dumpcap.exe'
165	'4364,Wireshark.exe'	'8516,dumpcap.exe'
166	'4512,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
167	'4520,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
168	'4932,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
169	'4932,FoxitReader.exe'	'4964,FoxitReaderUpdater.exe'
170	'4964,FoxitReaderUpdater.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
171	'4416,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
172	'4404,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
173	'4704,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
174	'4792,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
175	'4796,XXX'	'4848,bash.exe'
176	'4848,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
177	'5700,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
178	'5700,simpress.exe'	'5712,soffice.exe'
179	'5712,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
180	'5712,soffice.exe'	'5720,soffice.bin'
181	'5720,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
182	'7064,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
183	'7060,conhost.exe'	'uxtheme.dll,C:Windowssystem32uxtheme.dll'
184	'6320,dllhost.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
185	'6856,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
186	'6328,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
187	'6656,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
188	'6752,cmd.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
189	'6752,cmd.exe'	'6196,rundll32.exe'
190	'6752,cmd.exe'	'6808,cmd.exe:0'
191	'6196,rundll32.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
192	'6196,rundll32.exe'	'7108,powershell.exe'
193	'7108,powershell.exe'	'6844,dllhost.exe'
194	'6844,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
195	'6772,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
196	'7016,SearchFilterHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
197	'6808,cmd.exe:0'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
198	'7188,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
199	'7196,SearchFilterHost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'
200	'7640,svchost.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
201	'8516,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
202	'8524,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'

203	'8588,slui.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
204	'8656,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
205	'8720,notepad.exe'	'dwmapi.dll,C:Windowssystem32dwmapi.dll'
206	'8884,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
207	'8904,WinRAR.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
208	'7820,StikyNot.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
209	'9264,SearchProtocolHost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
210	'9264,SearchProtocolHost.exe'	'SHELL32.dll,C:Windowssystem32SHELL32.dll'
211	'9284,SearchFilterHost.exe'	'actxprxy.dll,C:Windowssystem32actxprxy.dll'
212	'9284,SearchFilterHost.exe'	'rtffilt.dll,C:Windowssystem32rtffilt.dll'
213	'9320,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
214	'9856,calc.exe'	'oleacc.dll,C:Windowssystem32oleacc.dll'
215	'356,XXX'	'368,csrss.exe'
216	'356,XXX'	'408,wininit.exe'
217	'368,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
218	'408,wininit.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
219	'408,wininit.exe'	'508,services.exe'
220	'408,wininit.exe'	'532,lsm.exe'
221	'408,wininit.exe'	'524,lsass.exe'
222	'416,XXX'	'428,csrss.exe'
223	'416,XXX'	'464,winlogon.exe'
224	'428,csrss.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
225	'428,csrss.exe'	'2176,conhost.exe'
226	'428,csrss.exe'	'5048,conhost.exe'
227	'428,csrss.exe'	'5908,conhost.exe'
228	'428,csrss.exe'	'5816,conhost.exe'
229	'428,csrss.exe'	'6504,conhost.exe'
230	'464,winlogon.exe'	'DAVHLPR.dll,C:WindowsSystem32DAVHLPR.dll'
231	'464,winlogon.exe'	'2320,userinit.exe'
232	'508,services.exe'	'wship6.dll,C:WindowsSystem32wship6.dll'
233	'508,services.exe'	'700,VBoxService.exe'
234	'508,services.exe'	'764,svchost.exe'
235	'508,services.exe'	'632,svchost.exe'
236	'508,services.exe'	'836,svchost.exe'
237	'508,services.exe'	'892,svchost.exe'
238	'508,services.exe'	'940,svchost.exe'
239	'508,services.exe'	'324,svchost.exe'
240	'508,services.exe'	'996,svchost.exe'
241	'508,services.exe'	'1240,spoolsv.exe'
242	'508,services.exe'	'1268,svchost.exe'
243	'508,services.exe'	'1380,svchost.exe'

244	'508,services.exe'	'1408,FoxitConnectedPDFService.exe'
245	'508,services.exe'	'1928,svchost.exe'
246	'508,services.exe'	'1512,taskhost.exe'
247	'508,services.exe'	'2076,sppsvc.exe'
248	'508,services.exe'	'2856,SearchIndexer.exe'
249	'508,services.exe'	'1196,wmpnetwk.exe'
250	'508,services.exe'	'3204,svchost.exe'
251	'508,services.exe'	'8288,taskhost.exe'
252	'532,lsm.exe'	'ADVAPI32.dll,C:Windowssystem32ADVAPI32.dll'
253	'524,lsass.exe'	'netutils.dll,C:Windowssystem32netutils.dll'
254	'632,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
255	'632,svchost.exe'	'2776,WmiPrvSE.exe'
256	'632,svchost.exe'	'1112,dllhost.exe'
257	'632,svchost.exe'	'2680,dllhost.exe'
258	'632,svchost.exe'	'3492,dllhost.exe'
259	'632,svchost.exe'	'3876,dllhost.exe'
260	'632,svchost.exe'	'3720,WmiPrvSE.exe'
261	'836,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
262	'836,svchost.exe'	'netutils.dll,C:Windowssystem32netutils.dll'
263	'836,svchost.exe'	'1004,audiodg.exe'
264	'836,svchost.exe'	'6160,audiodg.exe'
265	'892,svchost.exe'	'NTDSAPI.dll,C:Windowssystem32NTDSAPI.dll'
266	'892,svchost.exe'	'credssp.dll,C:WindowsSystem32credssp.dll'
267	'892,svchost.exe'	'2328,dwm.exe'
268	'940,svchost.exe'	'rasman.dll,C:Windowssystem32rasman.dll'
269	'940,svchost.exe'	'AVRT.dll,c:windowssystem32AVRT.dll'
270	'940,svchost.exe'	'aelupsvc.dll,c:windowssystem32aelupsvc.dll'
271	'940,svchost.exe'	'appinfo.dll,c:windowssystem32appinfo.dll'
272	'940,svchost.exe'	'WMsgAPI.dll,C:Windowssystem32WMsgAPI.dll'
273	'940,svchost.exe'	'wer.dll,C:Windowssystem32wer.dll'
274	'940,svchost.exe'	'3444,WMIADAP.exe'
275	'324,svchost.exe'	'ieproxy.dll,C:Program FilesInternet Explorerieproxy.dll'
276	'324,svchost.exe'	'comctl32.dll,C:WindowsWinSxSamd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9accomctl32.dll'
277	'324,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
278	'324,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
279	'996,svchost.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
280	'1240,spoolsv.exe'	'netutils.dll,C:Windowssystem32netutils.dll'
281	'1268,svchost.exe'	'WTSAPI32.dll,C:Windowssystem32WTSAPI32.dll'
282	'1268,svchost.exe'	'WINSTA.dll,C:Windowssystem32WINSTA.dll'
283	'1380,svchost.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'

284	'1380,svchost.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
285	'1380,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
286	'1408,FoxitConnectedPDFService.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
287	'1928,svchost.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
288	'1512,taskhost.exe'	'midimap.dll,C:Windowssystem32midimap.dll'
289	'2076,sppsvc.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
290	'2320,userinit.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
291	'2320,userinit.exe'	'2352,explorer.exe'
292	'2328,dwm.exe'	'MSASN1.dll,C:Windowssystem32MSASN1.dll'
293	'2352,explorer.exe'	'SensApi.dll,C:Windowssystem32SensApi.dll'
294	'2352,explorer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
295	'2352,explorer.exe'	tquery.dll,C:Windowssystem32query.dll'
296	'2352,explorer.exe'	'MLANG.dll,C:Windowssystem32MLANG.dll'
297	'2352,explorer.exe'	'FXSRESM.DLL,C:Windowssystem32FXSRESM.DLL'
298	'2352,explorer.exe'	'hcproviders.dll,C:WindowsSystem32hcproviders.dll'
299	'2352,explorer.exe'	'FunDisc.dll,C:Windowssystem32FunDisc.dll'
300	'2352,explorer.exe'	'SNTSearch.dll,C:Windowssystem32SNTSearch.dll'
301	'2352,explorer.exe'	'EhStorAPI.dll,C:Windowssystem32EhStorAPI.dll'
302	'2352,explorer.exe'	'DeviceCenter.dll,C:Windowssystem32DeviceCenter.dll'
303	'2352,explorer.exe'	'2440,VBoxTray.exe'
304	'2352,explorer.exe'	'2452,MySQLNotifier.exe'
305	'2352,explorer.exe'	'2524,StikyNot.exe'
306	'2352,explorer.exe'	'2228,mintty.exe'
307	'2352,explorer.exe'	'2424,taskmgr.exe'
308	'2352,explorer.exe'	'4060,soffice.exe'
309	'2352,explorer.exe'	'5044,cmd.exe'
310	'2352,explorer.exe'	'5188,firefox.exe'
311	'2352,explorer.exe'	'5900,cmd.exe'
312	'2352,explorer.exe'	'6076,notepad++.exe'
313	'2352,explorer.exe'	'5516,Wireshark.exe'
314	'2352,explorer.exe'	'6632,FoxitReader.exe'
315	'2352,explorer.exe'	'6464,mintty.exe'
316	'2440,VBoxTray.exe'	'RpcRtRemote.dll,C:WindowsSystem32RpcRtRemote.dll'
317	'2452,MySQLNotifier.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
318	'2524,StikyNot.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
319	'2532,XXX'	'2640,jusched.exe'
320	'2640,jusched.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
321	'2776,WmiPrvSE.exe'	'fwpuclnt.dll,C:Windowssystem32fwpuclnt.dll'
322	'2776,WmiPrvSE.exe'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
323	'2776,WmiPrvSE.exe'	'POWRPROF.dll,C:Windowssystem32POWRPROF.dll'
324	'2856,SearchIndexer.exe'	'SXS.DLL,C:Windowssystem32SXS.DLL'

325	'2856,SearchIndexer.exe'	'DEVOBJ.dll,C:Windowssystem32DEVOBJ.dll'
326	'2856,SearchIndexer.exe'	'NLSLexicons0009.dll,C:WindowsSystem32NLSLexicons0009.dll'
327	'2856,SearchIndexer.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
328	'2856,SearchIndexer.exe'	'3764,SearchProtocolHost.exe'
329	'2856,SearchIndexer.exe'	'3784,SearchFilterHost.exe'
330	'2856,SearchIndexer.exe'	'4556,SearchProtocolHost.exe'
331	'2856,SearchIndexer.exe'	'4576,SearchFilterHost.exe'
332	'2856,SearchIndexer.exe'	'6788,SearchProtocolHost.exe'
333	'2856,SearchIndexer.exe'	'6820,SearchFilterHost.exe'
334	'2856,SearchIndexer.exe'	'6940,SearchProtocolHost.exe'
335	'2856,SearchIndexer.exe'	'6972,SearchFilterHost.exe'
336	'2228,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
337	'2176,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
338	'1352,XXX'	'1460,bash.exe'
339	'1460,bash.exe'	'authz.dll,C:Windowssystem32authz.dll'
340	'2424,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
341	'2424,taskmgr.exe'	'2620,taskmgr.exe'
342	'1196,wmpnetwk.exe'	'FirewallAPI.dll,C:Windowssystem32FirewallAPI.dll'
343	'2988,XXX'	'2152,dllhost.exe'
344	'2152,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
345	'2300,XXX'	'2268,driver_endpoint_netconn.exe'
346	'2268,driver_endpoint_netconn.exe'	'wshtcpip.dll,C:WindowsSystem32wshtcpip.dll'
347	'1112,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
348	'2620,taskmgr.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
349	'2680,dllhost.exe'	'IDStore.dll,C:WindowsSystem32IDStore.dll'
350	'3204,svchost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'
351	'3204,svchost.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
352	'3204,svchost.exe'	'CLBCatQ.DLL,C:Windowssystem32CLBCatQ.DLL'
353	'3492,dllhost.exe'	'PROPSYS.dll,C:Windowssystem32PROPSYS.dll'
354	'3764,SearchProtocolHost.exe'	'profapi.dll,C:Windowssystem32profapi.dll'
355	'3784,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
356	'3876,dllhost.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
357	'4060,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
358	'4060,soffice.exe'	'4076,soffice.bin'
359	'4076,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
360	'3444,WMIADAP.exe'	'psapi.dll,C:Windowssystem32psapi.dll'
361	'3444,WMIADAP.exe'	'WLDAP32.dll,C:Windowssystem32WLDAP32.dll'
362	'3720,WmiPrvSE.exe'	'wmiprov.dll,C:Windowssystem32wbemwmiprov.dll'
363	'4556,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
364	'4576,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
365	'5044,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'

366	'5044,cmd.exe'	'4240,java.exe'
367	'5048,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
368	'4240,java.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
369	'5188,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
370	'5188,firefox.exe'	'5364,firefox.exe'
371	'5188,firefox.exe'	'6444,simpress.exe'
372	'5364,firefox.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
373	'5900,cmd.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
374	'5900,cmd.exe'	'MSCTF.dll,C:Windowssystem32MSCTF.dll'
375	'5900,cmd.exe'	'5944,NETSTAT.EXE'
376	'5908,conhost.exe'	'CRYPTBASE.dll,C:Windowssystem32CRYPTBASE.dll'
377	'5944,NETSTAT.EXE'	'winrnr.dll,C:WindowsSystem32winrnr.dll'
378	'5944,NETSTAT.EXE'	'rasadhlp.dll,C:Windowssystem32rasadhlp.dll'
379	'6076,notepad++.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
380	'5516,Wireshark.exe'	'wimaxmacphy.dll,C:Program FilesWiresharkplugins2.0.5wimaxmacphy.dll'
381	'5516,Wireshark.exe'	'msimtf.dll,C:Windowssystem32msimtf.dll'
382	'5516,Wireshark.exe'	'6116,dumpcap.exe'
383	'6116,dumpcap.exe'	'dhcpcsvc.DLL,C:Windowssystem32dhcpcsvc.DLL'
384	'5816,conhost.exe'	'SHLWAPI.dll,C:Windowssystem32SHLWAPI.dll'
385	'6632,FoxitReader.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
386	'6788,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
387	'6820,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
388	'6464,mintty.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
389	'6504,conhost.exe'	'sechost.dll,C:WindowsSYSTEM32sechost.dll'
390	'6540,XXX'	'6564,bash.exe'
391	'6564,bash.exe'	'apphelp.dll,C:Windowssystem32apphelp.dll'
392	'6940,SearchProtocolHost.exe'	'authz.dll,C:Windowssystem32authz.dll'
393	'6972,SearchFilterHost.exe'	'mssprxy.dll,C:Windowssystem32mssprxy.dll'
394	'6444,simpress.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
395	'6444,simpress.exe'	'6432,soffice.exe'
396	'6432,soffice.exe'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
397	'6432,soffice.exe'	'6408,soffice.bin'
398	'6408,soffice.bin'	'wow64cpu.dll,C:WindowsSYSTEM32wow64cpu.dll'
399	'8288,taskhost.exe'	'XmlLite.dll,C:WindowsSystem32XmlLite.dll'