

# PRIVACY, SECURITY AND TRUST

Fourteenth Annual Conference

12 - 14 DECEMBER, 2016, AUCKLAND, NEW ZEALAND



# Taxonomy of Malware Detection Techniques: A Systematic Literature Review

Hanif Mohaddes Deylami <sup>a,1</sup>, Ravie Chandren Muniyandi <sup>a,2</sup>  
Iman Tabatabaei Ardekani <sup>b,3</sup>, Abdolhossein Sarrafzadeh <sup>b,4</sup>

<sup>a</sup> School of Computer Science, Faculty of Information Science and Technology,  
Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Malaysia.

<sup>b</sup> Cybersecurity Research Center, Unitec Institute of Technology,  
Private Bag 92025, Victoria Street West, Auckland 1142, New Zealand.

<sup>1</sup> [hmdeilami@gmail.com](mailto:hmdeilami@gmail.com), <sup>2</sup> [ravie@ukm.edu.my](mailto:ravie@ukm.edu.my)

<sup>3</sup> [iardekani@unitec.ac.nz](mailto:iardekani@unitec.ac.nz), <sup>4</sup> [hsarrafzadeh@unitec.ac.nz](mailto:hsarrafzadeh@unitec.ac.nz)

**Abstract** - Malware is an international software disease. Research shows that the effect of malware is becoming chronic. To protect against malware detectors are fundamental to the industry. The effectiveness of such detectors depends on the technology used. Therefore, it is paramount that the advantages and disadvantages of each type of technology are scrutinized analytically. This study's aim is to scrutinize existing publications on this subject and to follow the trend that has taken place in the advancement and development with reference to the amount of information and sources of such literature. Many of the malware programs are huge and complicated and it is not easy to comprehend the details. Dissemination of malware information among users of the Internet and also training them to correctly use anti-malware products are crucial to protecting users from the malware onslaught. This paper will provide an exhaustive bibliography of methods to assist in combating malware.

**Keywords** - *Malware; Malicious code; Taxonomy; Anomaly-based; Signature-based; System requirements.*

## I. INTRODUCTION

Computers and information technologies (IT) have played a major role in the advancement of the last twenty years. Computer-based crimes using malware involve personal computers, private information of users which could be 'sensitive', network infrastructure, mobile platforms, and other internet based programs. Malware development is on the increase and enables an attack on much of a user's information without distinction. Malware has had a tremendous impact on the world, as we know it. Since 1988 [1, 2] the increase in the number of computer based security breaches confirms that malicious software has reached almost unmanageable levels. Taking into consideration the extent of potential damage caused by malicious software, its detection alone has caused significant problems for both the investigators and general population. Detection systems created by investigators are regularly put to

extensive use in detection exercises. This paper is dedicated to researching malicious software detection methodologies.

### A. Research Motivation

The structure of malware analysis and services has become an even more attractive target for potential attackers. A sequential methodology reveals the make-up of the malicious software and the way it operates. During analysis a critical procedure called 'behavior monitoring' is employed using "dynamic coarse-grained binary instrumentation" on the target system. 'Profiling' [3] is the terminology used to describe the first collection of malicious software for investigation. A malicious software detection system itself can be a target for attack - the confidentiality, integrity, availability of its information bank, data and the virtualized infrastructure could be used by the malware to initiate fresh onslaughts on the detector system. The situation would become virtually unmanageable if a powerful computing system, with a huge storage volume, were attacked by internal malware.

On January 7, 2014 Fox IT, which is headquartered in Holland, published a report stating that many Yahoo.com visitors were corrupted via Java exploit. The advertising arm of Yahoo - Ads.Yahoo.com - had been compromised and a virus broadcast to their users. It was estimated by Fox IT that by December 30, almost 300,000 users per hour were affected by the virus, with approximately 27,000 suffering serious consequences. In this instance, Yahoo's advertising system was transmitting a so-called 'exploit kit'. Fox IT determined that the 'exploit kit' would focus on weaknesses in the Java program to exploit and download all types of malicious software programs on the user's computer. The malware supplier has yet to be detected, but it is speculated that they may have made large financial gains via selling information from the affected systems to third parties [4, 5]. Due to the

need for absolute control over the system structure, the ability to detect malicious software has been greatly affected. Absolute control plays a significant part in safeguarding surfers' data in the Internet environment. This paper collates the problems faced by experts in preventing the development of malware in the Internet industry. An attempt is made to pull together the resources experts use and consolidate the fragmented work that is currently being done so that a robust and concerted effort can be made to combat the proliferation of malicious software. This concerted effort will focus on developing the required detection technology.

### B. Research Boundaries and Limitations

"Multi-purpose" detection systems - which are more comprehensive in their functions - are being considered and proposed in this research. In an attempt to reduce false-positive rates, a number of researchers are concentrating on a dedicated detection process path to narrow down on a particular type of malicious code.

Since malicious software detection is the key focus of this paper, much concentration is being put on recent updated literature and systems. The result of studies is based on the taxonomy of malware as explained in the following section. Irrespective of the extent to which the science and technology of malware detection has progressed, this paper has based its investigations on the following research questions:

- RQ1. What requirements should malicious software detectors comply with to be effective?
- RQ2. What is the taxonomy of the malware detection technique?
- RQ3. What are the strengths and weaknesses of existing solutions for malware detection?

## II. MALWARE DETECTION SYSTEM DEFINITIONS AND TAXONOMY

'Mal' in the Spanish language means 'bad'. 'Malware' is described by other terms such as malicious software, malicious code, or malcode. The following definitions represent the different explanation of malware by some of the researchers.

- a) Malware's intention is to be destructive [6].
- b) Malicious code is any code introduced into a system to sabotage the system [7].
- c) 'Malware' is a specific name used for a category of software codes that is malicious. This would include "Viruses, Worms, Trojans, and Spywares" (Table I & II). People, who develop malware, employ generators, include jargon, and also use other people's codes. The need to exchange information exists among malware developers and many are focused on knowing all about the best ways to introduce malwares [8].
- d) Malicious software is designed to penetrate and operate in one's computer and carry out the instructions of the developer [9].

- e) The original definition of a malware in 1983 was: "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself". This definition was later updated in 'Computer Viruses - Theories and Experiments' [10].

TABLE I. Various Computer Security Terms

Type	Definition
Malware	When a software attacker intends to corrupt someone's computer he/she sends out a malware, which consist of Virus, Worms, Trojans, Adwares, Backdoors, Spywares, Bots, Rootkits and so on. Most malicious software's are generally termed viruses. Anti-viruses sold in the open market are also called anti-malwares.
Spam	The term used to describe abuse/misuse of internet mail (IM) services is Spam. This also includes mail that is not requested or asked for and these are called 'e-mail spam'. Included in this portfolio are IM spam, blog spam, discussion forum spam, spam in hand-held phones, etc.
Phishing	Phishing is defined as a malicious activity using social engineering techniques. For example, abuse of internet commercial and financial services is termed phishing. Phishing also includes attempts to acquire sensitive information such as usernames, passwords, and online banking information.
Exploits	When a weakness or loophole occurs in a computerized system or software, an attacker usually unloads a series of instructions, called Exploits, to take advantage of that weakness to corrupt the system without the host user's knowledge, this can happen to both software and hardware. The main aim of this exploit is to gain absolute control of the host's electronic or computer system.

TABLE II. Various Malware Terms

Type	Definition
Virus	A computer virus, duplicates or reproduces itself, usually corrupting or maligning other programs installed in the hosts' system. Without personal assistance, it may be a bit difficult for a virus to reproduce itself.
Worm	A worm is slightly different from a virus in the sense that it does not need external help to reproduce or duplicate itself on computer networks. It operates on its own.
Trojan	Trojan Horses or Trojans are usually 'wolves in sheep's clothing' because they attack or malign a computer system in disguise.
Spyware	Spyware is any program or software that is mounted clandestinely in someone's computer to not allow the user to do what he/she wants. The user, most of the time, is not aware of the installed spyware.
Others	Most other malicious programs, including: logic bombs - that look like legal programs but malign the actual program; rootkits - that consist of tools for hacking and also malign the proper operation of any software; backdoor - a term used to describe a process that prevents or interferes with the authorized operation of a system.

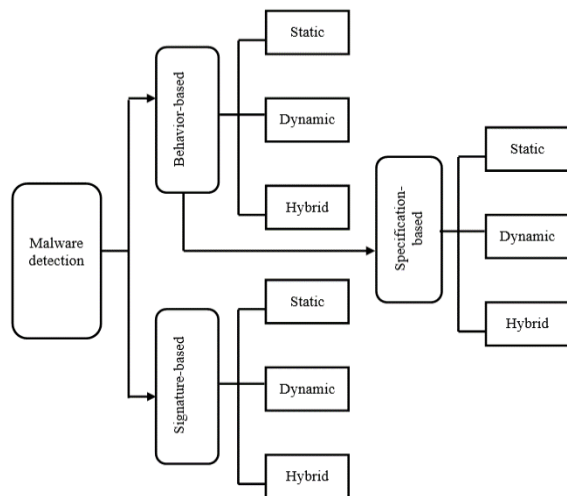
The concept of a ‘computer virus’ takes its name from a fictional science based novel where a computer program named “virus” was able to mutate. In the educational field it was used by Cohen in his thesis “Experiments with Computer Viruses” [10] however, literature on viruses can be found earlier than Cohen’s first usage. Apple II computers were among the first to be attacked by viruses in 1981 and 1982. The first recorded incidence of a virus was called Elk Cloner in mid-1981. This was followed by ‘Brain’ in 1986, a boot sector virus.

Science fiction also gave birth to ‘Worm’, this name was first used by John Brunner who wrote the novel ‘Shockwave Rider’ to depict a program that broadcasts itself on a network. But Shoch says he was the first to introduce the term in the academia [11].

### A. Organization of Malware Detection

Malicious software detection is split in two ways: Signature- and Behavior- based technologies and each technology can be used with static, dynamic or hybrid analysis [12]. The particular methodology for an anomaly- or signature- based procedure is based on how the technology collates the information to detect malicious software [13-15]. How malicious software detection is managed is shown in Fig. 1.

Fig. 1. Ecosystem of malware detection.



Procedures employed for detecting malicious software can be summarized into two parts:

### A. Anomaly-Based Detection

An anomaly-based detection draws upon its information base to determine the presence of normal behavior to decide the strength of the malware under investigation. Another form of anomaly-based detection could be called specification-based detection. Anomaly-based detection investigation takes places in two situations:

- A training or learning situation. While in the training situation the detector tries to learn the normal behavior. It is quite possible that the

detector is learning the host’s behavior or the PUI’s or maybe both combined. The main benefit of the anomaly-based detection is its capability to detect zero-day intrusions.

- A detection or monitoring situation.

The two essential drawbacks of this procedure are:

- High false alarm rates: It is prone to excessive false alarm rates, which is defined as ‘normal’ outputs categorized as (false positive) and divided by the total number of ‘normal’ behavior.
- The difficulty in ensuring what parameters need to be learned in the training situation.

### a) Specification-Based Detection

To deal with high false alarm incidence that goes with many anomaly-based detection procedures, a specification-based detection, which is similar to an anomaly-based unit, is utilized. Due to the fact that specification-based detection is derived from anomaly-based detection, it is used to estimate the requirements for a system, rather than trying to estimate the execution of an end-use for a system. Moreover, in specification-based detection the training situation is the guideline, which dictates or forecasts all outcomes that any behavior of a program may show for that particular system being safeguarded or under investigation. The major drawback of specification-based detection is that it is not easy to predict all the acceptable outcomes fully and precisely that a system will manifest.

### B. Signature-Based Detection

Signature-based detection utilizes its technology-based personality to discern a malware and consequently confirm the malevolent nature of a program under investigation. Putting it another way, the signature-based detection tries to create a benchmark using the malware and subsequently uses this as a reference for detecting other malicious software.

In grouping all these models, the signature-based detection generates a database for itself. In a perfect system, it is imperative that the signature should recognize any program manifesting a behavior fitting the signature’s malicious database. This database contains all information needed by the signature to detect malicious software. This database is consulted whenever there is a potential problem with the PUI.

One of the main problems of the signature-based detection method is its inability to recognize ‘zero-day’ intrusions. A zero-day intrusion is a situation where there is no similar signature in the database to compare with. Also an experienced person is probably needed to design the signature. Aside from giving way to operator error it is a tedious process if the design and installation is not set up to function automatically. Due to the fact that certain malware is able to proliferate the ability to design and install a more precise signature is

extremely critical. Developers of such signatures, which function on an automatic mode, could be found without much effort, but significantly more energy needs to be put in to doing this. However, all detection procedures could use one of three various methodologies.

- **Static:** As in language, static analysis uses the structure or formatting of the programming to uncover the malware under investigation. Generally, a static methodology strives to uncover malware prior to the program under investigation being implemented.
- **Dynamic:** During pre- or post- program implementation malware can be detected utilizing a dynamic methodology.
- **Hybrid:** Hybrid procedures are available which combines the two methodologies, meaning both static and dynamic databases are used to uncover malicious software.

### III. MALWARE DETECTOR

As set out in the introduction, a malicious software detector is a device that uses technology to detect malware. The function of the detector is to recognize malevolent software using signatures and other problem solving skills. One example of a detector is for instance, an antivirus scanner. Malware detectors are the first line of defense in combating viruses. Its function is to safeguard the system against any intrusion. The detector could be located in the host or outside. The detection system functions via the established technology and performs an observed evaluation of malware detecting skills [15, 16]. The efficacy of a similar detector depends on the skills it possesses.

There are dual inputs to any malware detector. The first such output is its ability to recognize the malware in question. In anomaly-based detection the detector has less information in the initial phase of its operation and gains in confidence at the top of the learning curve.

Therefore, a deviant behavior could easily be detected by an anomaly-based detection system due to its skills [17]. Due to the inherent nature of the detection system any deviant behavior is assumed to be malevolent and is therefore captured by the anomaly-based detector. If the detector is of a signature-based type, its reaction is triggered by its memory base. This memory base is usually brought up to currency by designated people who are able to recognize malware and manifest it in a format acceptable to the signature database and eventually readable by the relevant equipment [18, 19].

The malware detector has to have another input and that is the program under investigation. The moment the detector knows what it terms as malevolent behavior (normal behavior) and the program under investigation, it will call upon its database to consider whether the program is malevolent or not.

### IV. METHODOLOGY

The authors [20-27] have recommended that for the purpose of writing a literature review paper the following method be adopted to source material for review:

The beginning stage for the review should include the doctoral research papers from universities around the world since they have been scrutinized at higher levels. Online libraries have often been the resource centers for postgraduate research. “Malware” and “malware analysis” are keywords that have been utilized to relate to various theses for research. The next stage should include journals and papers presented at forums worldwide since these have been vetted by people possessing expertise in the field and have been accepted for publications or discussions.

The list of research papers (from serial number 1-11) and theses (from serial number 12-18) included in the review and their classifications with respect to their topics and contributions have been summarized in Table III.

TABLE III: Classification of Existing Related Papers Based on Malware Detection Technique

No.	Title	Authors and Date of publication	Contribution
1	The Effects of Different Representations on Static Structure Analysis of Computer Malware Signatures [29].	Ajit Narayanan, et al. (2013)	The objective of this research is to ascertain the feasibility of a stand-alone discussion of ‘malware-modeling’ utilizing the expanding and accessible signature storehouse. It is to demonstrate that should malware signatures be coded according to their biometric identity, it is possible to use benchmarked ‘sequence alignment’ procedures from bioinformatics to enhance the precision of differentiating worm and virus biometrics. In addition, “aligned signature sequences” can be excavated by means of preset excavation processes to obtain future biometrics that will aid to differentiate between worm and virus signatures.
2	An approach for detection and family classification of malware based on behavioral analysis [30].	S. S. Hansen, et al. (2016)	This study tackles the problem of analyzing, detecting and classifying the vast amount of malware in a scalable, efficient and accurate manner. They propose a novel approach for detecting malware and classifying it to either known or novel.
3	Method and apparatus for detecting malware infection [31].	Gu, Guofei, et al. (2015)	The present invention generally relates to network security, and more particularly relates to the detection of malware infection.

4	Malware Analysis and Classification: A Survey [36].	Gandrota, E., et al. (2014)	This research delivers a summary of procedures for assessment and categorizing the malicious software.
5	Survey on malware detection methods [32].	Vinod, P., et al. (2009)	The research concentrated on different malicious software detection methodologies such as signature-based detection, program comprehension, of non-understandable information (codes) to detect malware.
6	Detection & Preservation of New & Unknown Malware using Honeypots [84].	Kumar, Pant (2009)	A system to set up and make known a program to trap unsuspecting malware and to cure affected programs.
7	Classes of Vulnerabilities and Attacks [89].	Pascal Meunier (2008)	This research focuses on what details are useful, and how they fail to meet researcher criteria. A list of security problems and discussed and various classification methods are reviewed by considering security concepts.
8	Malware Forensics-Detecting the Unknown [35].	Martin, Overton (2008)	The study researched what methods are available or generated to assess the malware in question. Also concentrated on an organized strategy to assess the complete scenario regarding questionable files.
9	A Survey of Malware Detection Techniques [12].	Nwokedi Idika, Aditya P. Mathur (2007)	This research assessed 45 malicious software detection methodologies to afford a chance to measure the similarity or dissimilarity of one system versus the other to establish a tight, dependable system.
10	TT Analyze: A tool for analyzing malware [37].	Bayer, Kruegel, Kirda (2006)	It's an available technique called TT Analyzer for the purpose of dynamically assessing the mannerisms of Windows Executables.
11	Behavior based Approach for Intrusion Detection Systems [38].	Andrey Dolgikh (2013)	This research presents the cyber experimentation and behavior based Intrusion detection. The results of experiments show high detection rate and low overhead for both approaches. Such results suggest that modern sophisticated malware can be automatically detected and suppressed with these systems.
12	Malware Variant Detection [39].	Khalid Mohamed Abdelrahman Y Alzarooni (2012)	In this research a new technique that defeats the downside of current malicious software detection processes was postulated by examining the meaning of known malware codes. The procedures involve three significant investigation techniques: "the proposing of a semantic signature", "slicing analysis", and "test data generation analysis".
13	An Integrated Malware Detection and Classification System [40].	Ronghua Tian (2011)	The aims of this thesis are to develop effective and efficient methodologies, which can be applied to continuously improve the performance of detection and classification on malware collected over an extended period of time.
14	Dealing with next generation Malware [41].	Roberto Paleari (2011)	This group proposed a new architecture for enhancing behavior based investigation of dubious programs that affords the end-user to entrust security labs with the implementation and investigation of a program and to coerce the program to acquit itself as though it was implemented by the end-user.
15	Robust & Efficient Malware Analysis and host based monitoring [42].	Monirul I. Sharif (2010)	1) Efficient Methods for enabling static malware analysis. 2) Making dynamic analysis approaches more robust. 3) Reversing emulator based obfuscation. 4) Anticipating obfuscations that hide trigger based behavior.
16	Data mining methods For malware detection [14].	Siddiqui (2008)	The author postulated a data-extraction architecture to detect malware.
17	Behavioral and Structural Properties of Malicious Code [44].	Christopher Kruegel (2007)	In this thesis, approaches to distinguish behavioral and structural properties of binary codes were postulated. These approaches could be utilized to produce nebulous, and meaningful accounts of malicious software and to distinctively classify malware in lieu of isolated happenings.

## V. MALWARE DETECTION SYSTEM REQUIREMENTS

The system requirements for malware detection are as follows:

### R1. Detect Variety of Attacks with Least False Positive Rates

The proliferation of computer intrusions, with increasing intricacies and unforeseen circumstances means it is imperative for the system to identify new intrusions and their predatory designs in order to select the appropriate preemptive strategy.

The requirement is that the system should be teachable and be able to be learnt. Also the system

should be able to be upgraded regularly to accommodate every conceivable malevolent activity with relatively few false-positive alarms.

The design has to have a pre-agreed performance level and also be secure and should require the minimum computation assets because computational potential affects the effectiveness of cloud services. Hence, the effectiveness of such capabilities should be harnessed to manage false positive alarms while ensuring an acceptable level of detection performance.

### R2. Super-Fast Detection and Prevention

Extremely quick detection and prevention is very critical for efficient detection of malware because it affects the complete system performance and is also

critical to supply service previously agreed upon (QoS).

### R3. Malware Detection System Scalability

Any good malware detection system should be expandable so that it can manage the huge number of network nodes that could be free in cyberspace and their communication and computational burden. The inclusion of a detection and correlation manager also has a bearing on the expandability and performance of malware detection systems. It is a critical central requirement for malware systems, which limits the basic infrastructure ability to changing demands such as the quantity and magnitude of data used in applications.

### R4. Resistance to Compromise

In estimating its own assessment and preservation in the event it is affected by an attacker, a malware detection system must shield itself from rouge infiltration. A malware detection system should have the ability to approve normal behavior and responds abnormal behavior.

## VI. STRENGTHS AND WEAKNESSES OF EXISTING MALWARE DETECTION TECHNIQUES

There are pros and cons of such detection methods which need to be compared in order to evaluate and make objective decisions for each situation. In the previous section of this research it was pointed out that attacks could happen due to a flaw in the system. When an intrusion is detected an alarm ensues. How well the system detects an intrusion depends on the preciseness and currency of the database. The more current the knowledge of the database the lower the rate of false alarms. In addition, the environmental analysis, as postulated by the malicious software, is comprehensive and therefore it is possible to take corrective steps. However, this approach runs into some problems, namely, the continuity of the malware detection database updating periodically, the fact that it is very focused and hence lack of peripheral vision, and lastly, to detect intrusion from internal sources.

Regarding the next option, the behavior-based procedure is a standard procedure obtained from published information. Any ongoing program is referenced against this standard procedure and any variance is considered a malicious intrusion. This methodology can detect attempted intrusions into unsuspecting victims and may be able to uncover new onslaughts before they occur. Though, it may not affect so much the available technical databases, it will help to protect misuse of privileged information or information that possesses certain rights or immunity. It has, however, two drawbacks: firstly, the high incidence of false alarms and secondly, that it requires online retraining from time to time. This could result in additional exposure to attacks to the detection system or false alarms (Table IV).

TABLE IV: Categorization Based on Strengths and Weaknesses of Existing Malware Detection Techniques

Technique	Advantage	Disadvantage
Signature-based	<ul style="list-style-type: none"> <li>Recognized known attack precisely.</li> <li>Minimum system resources are needed to detect attack mode.</li> <li>Concentrates on normal behavior.</li> </ul>	<ul style="list-style-type: none"> <li>Un-recognized unknown attack method.</li> <li>Impotent to act against invisible signatures.</li> </ul>
Anomaly-based	<ul style="list-style-type: none"> <li>Can detect new attack modes.</li> <li>Concentrates on normal behavior to defeat unrecognized intrusions.</li> </ul>	<ul style="list-style-type: none"> <li>Necessary to renew information regarding the users' behavior and statistics in normal usage.</li> <li>Difficult to predict the most suitable solution to detect the oncoming attacks.</li> <li>CPU time, memory and storage space required additionally.</li> <li>False positive alarm increased.</li> </ul>
Specification-based	<ul style="list-style-type: none"> <li>First time (Unknown) attacks detected.</li> <li>Incidence of false positive alarm minimal.</li> </ul>	<ul style="list-style-type: none"> <li>Anomaly detection is more effective in detecting unknown attacks. Better at network probing and denial-of-service intrusions.</li> <li>Takes too much time to propose specifications with fine details.</li> <li>Increase false negative due to attacks may be missed.</li> <li>Possibility of missing increasing false negative alarms due to intrusions.</li> </ul>

## VII. DISCUSSION

In spite of the fact that there are two significant methodologies in place for the analysis of malicious software, there is a shortcoming in the application due to a vast spectrum of scenarios that allow malware to go undetected.

In answer to the first research question (RQ1. What requirements should malicious software detectors comply with to be used effectively?) a list of essentials was assembled (in Section V) with reference to the attributes of malicious software detection systems. In addition, in Section II, the current classification of malicious software detection methodologies into groups is discussed to elicit a response to the second research question (RQ2. What is taxonomy of malware detection technique?). In response to the third question (RQ3. What are the strengths and weaknesses of existing solutions to malware detection?) a list of the advantages and disadvantages that meet the list of malware detection techniques are discussed (in Section VI).

## VIII. CONCLUSION

This research enumerated a detailed classification of first class malicious software detection and avoidance programs for researchers to 'bite into'. Dedicated importance was assigned to malicious software requirements and recognition given to the essentials of malware detection and avoidance procedures.

## ACKNOWLEDGEMENT

The corresponding authors are thankful to the Ministry of Higher Education (Malaysia) for providing financial support by the Fundamental Research Grant Scheme (FRGS/1/2012/SG05/UKM/02/3).

## REFERENCES

- [1] Barbara Guttman, Edward A. Roback. "An Introduction to Computer Security: The NIST Handbook". Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-0001, October 1995. <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf> [Accessed February 18, 2016].

- [2] Howard F. Lipson. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. PhD CERT @ Coordination Center, Networked Systems Survivability Program, November 2002. <http://www.cert.org/archive/pdf/02sr009.pdf> [Accessed June 22, 2016].
- [3] Aquilina J, Casey E., & Malin, C. Malware Forensics Investigating and Analyzing Malicious Code. Burlington; MA: Syngress; 2008.
- [4] Fox IT, Joostbijnl, Malicious advertisements served via Yahoo, <http://blog.fox-it.com/2014/01/03/malicious-advertisements-served-via-yahoo/> [Accessed February 04, 2016].
- [5] Carol. Spyware, viruses, & security forum: NEWS. CNET, 2014. [http://forums.cnet.com/7723-6132\\_102-609717/news-january-06-2014/](http://forums.cnet.com/7723-6132_102-609717/news-january-06-2014/) [Accessed February 07, 2016].
- [6] Christodorescu M, Jha S, Seshia A S, Song X D, Bryant E R. Semantics aware malware detection. In IEEE Symposium on Security and Privacy; pages 32-46, 2005.
- [7] McGraw G, Morrisett G. Attacking malicious code: A report to the infosec research council. IEEE Software; 33-44.26; 2003.
- [8] Arief, B. & Besnard, D. Technical and human issues in computer-based systems security. University of Newcastle upon Tyne (CS-TR-790), 2003.
- [9] Skoudis E, Zeltser L. Malware Fighting Malicious Code. New Jersey: Prentice Hall, 2004.
- [10] Cohen F. "Experiments with Computer Viruses". 1984.
- [11] Shoch F J, Hupp A J. "The Worm Program-Early Experience with a Distributed Computation", pages 172-180, 1982.
- [12] Nwokedi Idika, Aditya P. Mathur. A Survey of Malware Detection Techniques. Department of Computer Science Purdue University, West Lafayette, IN 47907, 2007.
- [13] Hao, S., Wang, W., Lu, H. and Ren, P. "AutoMal: automatic clustering and signature generation for malwares based on the network flow". Security Comm. Networks, 2014. doi: 10.1002/sec.1029.
- [14] Muazzam Ahmed Siddiqui. Data mining methods for malware detection. PhD thesis, College of Sciences, University of Central Florida, Orlando, Florida, 2008.
- [15] Xue, L., Sun, G. "Design and implementation of a malware detection system based on network behavior". Security Comm. Networks, 2014. doi: 10.1002/sec.993.
- [16] Zhao, Z., Wang, J. and Wang, C. "An unknown malware detection scheme based on the features of graph". Security Comm. Networks; 6: 239-246; 2013. doi: 10.1002/sec.524.
- [17] Eskandari, M. and Raesi, H. Frequent sub-graph mining for intelligent malware detection. Security Comm. Networks, 2014. doi: 10.1002/sec.902.
- [18] Pektaş, A., Acarman, T. A dynamic malware analyzer against virtual machine aware malicious software. Security Comm. Networks, 2013. doi: 10.1002/sec.931f.
- [19] Chia-Mei Chen, et al. "A proactive approach to intrusion detection and malware collection". Security Comm. Networks; 6: 844-853; 2013. doi: 10.1002/sec.619.
- [20] Reed, L.E. "Performing a literature review". 28th Annual Frontiers in Education Conference, FIE'98; Vol. 1, pp. 380-3; 1998.
- [21] Webster, J. and Watson, R.T. "Analyzing the past to prepare for the future: writing", 2002.
- [22] Green, B.N., Johnson, C.D. and Adams, A. "Writing narrative literature reviews for peer-reviewed journals: secrets of the trade". Journal of Chiropractic Medicine; Vol. 5 No. 3, 101-17; 2006.
- [23] Levy, Y. and Ellis, T.J. "A systems approach to conduct an effective literature review in support of information systems research". Informing Science Journal; Vol. 9, 181-212; 2006.
- [24] Armitage, A. and Keeble-Allen, D. "Undertaking a structured literature review or structuring a literature review: tales from the field". The Electronic Journal of Business Research Methods; Vol. 6 No. 2, pp. 103-14; 2008.
- [25] EBSE Technical Report, Guidelines for performing Systematic Literature Reviews in Software Engineering; Ver. 2.3; 2007.
- [26] Tiago Oliveira, et al. Literature Review of Information Technology Adoption Models at Firm Level, 2011.
- [27] Anders Kofod-Petersen. How to do a Structured Literature Review in computer science, Ver. 0.1. October 1, 2012.
- [28] Christoph Alme, et al. McAfee@ Labs 2014 Threats Predictions. Report MacAfee Lab, 2014. <http://www.mcafee.com/uk/resources/reports/rp-threats-predictions-2014.pdf> [Accessed July 10, 2016].
- [29] Ajit Narayanan, et al. The Effects of Different Representations on Static Structure Analysis of Computer Malware Signatures, 2013.
- [30] S. S. Hansen, T. M. T. Larsen, M. Stevanovic and J. M. Pedersen, "An approach for detection and family classification of malware based on behavioral analysis," International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, pp. 1-5, 2016.
- [31] Gu, Guofei, Phillip Andrew Porras, and Martin Fong. "Method and apparatus for detecting malware infection." U.S. Patent No. 8,955,122. 10 Feb. 2015.
- [32] Vinod, P., et al. "Survey on Malware Detection Methods", 2009.
- [33] Gerrold D. When Harlie Was One. Doubleday, 1972.
- [34] Wang, C. Malware Detection. 1<sup>st</sup> Edn., Springer, New York, pp: 311; 2006.
- [35] Martin Overton. Malware Forensics-Detecting the Unknown. Virus Bulletin conference, Westin Hotel, Ottawa, Canada, 2008.
- [36] Ekta Gandotra, Divya Bansal, Sanjeev Sofat. Malware Analysis and Classification: A Survey. Journal of Information Security; 5, 56-64; 2014. <http://dx.doi.org/10.4236/jis.2014.52006> [Accessed August 10, 2016].
- [37] U. Bayer, C. Kruegel, E. Kirda. "TT Analyze: A tool for analyzing malware". Ikarus Software & Technical University of Vienna, 2006.
- [38] Dolgikh, Andrey. Behavior based Approach for Intrusion Detection Systems. PhD report. State University of New York at Binghamton; pages; 3590786; 2013.
- [39] Khalid Mohamed Abdelrahman Y Alzarooni. Malware Variant Detection. PhD report. Department of Computer Science, University College London, 2012.
- [40] Tian, Ronghua. An integrated malware detection and classification system, PhD thesis, School of Information Technology, Deakin University, 2011.
- [41] Roberto Paleari. Dealing with next generation Malware. PhD thesis, Facolta di Scienze Matematiche, Fisiche e Naturali, UNIVERSITA DEGLI STUDI DI MILANO, 2011.
- [42] Monirul I. Sharif. "Robust & Efficient Malware Analysis and host based monitoring". PhD thesis, School of Computer Science, Georgia Institute of Technology, 2010.
- [43] Lejun Fan, Yuanzhuo Wang, et al. "Privacy theft malware multi-process collaboration analysis". Security Comm. Networks, 2013. doi: 10.1002/sec.705.
- [44] Christopher Kruegel. Behavioral and Structural Properties of Malicious Code. Springer Science, Advances in Information Security; Volume 27, pp 63-83; 2007.
- [45] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiware, A., & Yang, H., "Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions". ACM Computer and Communication Security Conference, 2002.
- [46] M. Szczepanik and I. Jozwiak. "Detecting New and Unknown Malwares Using Honeynet". Wroclaw University of Technology, Institute of Informatics, Poland; p 173; 2010.
- [47] R. Richardson. CSI Computer Crime & Security Survey. Computer Security Institute, 2008.
- [48] Garfinkel T, Rosenblum M. "A virtual machine introspection based architecture for intrusion detection". In Proceedings of the Symposium on Network and Distributed Systems Security (NDSS); San Diego, CA, USA, February 2003.

- [49] M. Aharoni. "Cracking the Perimeter v.1.1". *Anti-Virus Comparative* No. 23, 2009. [http://www.avcomparatives.org/images/stories/test/ondret/avc\\_report23.pdf](http://www.avcomparatives.org/images/stories/test/ondret/avc_report23.pdf) [Accessed October 06, 2016].
- [50] Y. Chen, A. Narayanan, S. Pang, and B. Tao. "Multiple sequence alignment and artificial neural networks for malicious software detection". In *Proceedings of the 8<sup>th</sup> IEEE Conference on Natural Computation*, China; pages 261-265; 2012.
- [51] A. Narayanan, Y. Chen, S. Pang, and B. Tao. "The effects of different representations on malware motif identification". In *Proceedings of the International Conference on Computational Intelligence and Security (CIS '12)*; pages 86-90; 2012.
- [52] A. A. E. Elhadi, M. A. Maarof, and A. H. Osman. "Malware detection based on hybrid signature behavior application programming interface call graph". *American Journal of Applied Sciences*; vol. 9, no. 3, pages 283-288; 2012.
- [53] Brand M, Valli C, Woodward A. A Threat to cyber resilience: A malware rebirthing Botnet. In the *Proceedings of the 2<sup>nd</sup> International Cyber Resilience Conference*, 2011.
- [54] Mohaddes Deylami, H., Ardekani, I. T., Muniyandi, R. C., & Sarrafzadeh, A. Effects of Software Security on Software Development Life Cycle and Related Security Issues. *International Journal of Computational Intelligence and Information Security*, 6(8), pp.4-12, 2015.
- [55] Xufang, L., P.K.K. Loh, and F. Tan. "Mechanisms of Polymorphic and Metamorphic Viruses". In *Intelligence and Security Informatics Conference (EISIC)*, 2011.
- [56] Maria B. Line. Why securing smart grids is not just a straightforward consultancy exercise. Published online in *Wiley Online Library (wileyonlinelibrary.com)*. *Journal of Security and communication networks*; vol.7, pages: 160-174; 2013.
- [57] Chaugule, A., Z. Xu, and S. Zhu. A specification based intrusion detection framework for mobile phones. In *Proceedings of the 9<sup>th</sup> International conference on applied cryptography and network security*, Springer-Verlag: Nerja, Spain; p. 19-37; 2011.
- [58] Peter Denning. *Computers under Attack: Intruders, Worms and Viruses*. Addison-Wesley, Reading, Mass., 1990.
- [59] Robin Sharp. *An Introduction to Malware*. Spring 2013.
- [60] Y. Chen, A. Narayanan, S. Pang, and B. Tao. "Malicious software detection using multiple sequence alignment and data mining". In *Proceedings of 26<sup>th</sup> IEEE International Conference on Advanced Information Networking and Applications (AINA'12)*; pages 8-14; 2012.
- [61] Pinz, C.I., et al. Improving the security level of the FUSION@ multi-agent architecture. *Expert Syst. Appl.*; 39(8): p. 7536-7545; 2012.
- [62] Kevadia Kaushal, P.S., Nilesh Prajapati. *Metamorphic Malware Detection Using Statistical Analysis*. *International Journal of Soft Computing and Engineering (IJSCE)*; 2(3), 2012.
- [63] Bergeron J, Debbabi M, Desharnais J, Erhioui M M, Lavoie Y, Tawbi N. "Static Detection of Malicious Code in Executable Programs". *Symposium on Requirements Engineering for Information Security (SREIS'01)*, 2001.
- [64] Fred Cohen. *Computer Viruses-Theory and Experiments Introduction and Abstract*. 1984.
- [65] M. D Hanif, P. S Yashwant. Cybercrime detection techniques based on support vector machines. *Artificial Intelligence Research*, Vol. 2, No. 1, 2013.
- [66] Mehedy Masud, et al. "Data Mining Tools for Malware Detection". CRC Press is an imprint of Taylor & Francis Group, an Informa business, 2012.
- [67] Dawn Song, et al. "BitBlaze: A new approach to computer security via binary analysis". In *Proceedings of the 4<sup>th</sup> International Conference on In-formation Systems Security (Keynote invited paper)*, Hyderabad, India, 2008.
- [68] Steroids, S.o. "Malware online scanners". <http://cleanbytes.net/malware-online-scanners> [Accessed March 22, 2016].
- [69] Ravi Sahita, et al. "Dynamic software application protection". Technical report, Intel Corporation, 2009.
- [70] Vivek kumar, Sadhna K Mishra, Vineet Ricchariya. "Detection of malicious software by Using Data Mining Tools and Other Techniques-a Survey". *IJCSMR*; vol. 1, issue 4, pages 746-750; 2012.
- [71] Blount, J.J., D.R. Tauritz, S.A. Mulder. *Adaptive Rule-Based Malware Detection Employing Learning Classifier Systems: A Proof of Concept*. In *Computer Software and Applications Conference Workshops (COMPSACW)*, IEEE 35<sup>th</sup> Annual, 2011.
- [72] Ryan Heartfield and George Loukas. 2015. *A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks*. *ACM Comput. Surv.* 48, 3, Article 37, 39 pages, 2015.
- [73] Joanna Rutkowska, Alexander Tereshkin. "IsGameOver() anyone?". *Invisible Things Lab, Black Hat Briefings*, USA, 2007.
- [74] Jay Jacobs, Bob Rudis. "Data-Driven Security: Analysis, Visualization and Dashboards". E-book, Published in *Wiley Online Library (wileyonlinelibrary.com)*, 2014.
- [75] Mark Stamp. "Information Security: Principles and Practice 2<sup>nd</sup> Edition". E-book, Published in *Wiley Online Library (wileyonlinelibrary.com)*, 2011.
- [76] Symantec. "Internet security threat report: 2014 trends", vol.19, Spring 2014. [http://www.symantec.com/security\\_response/publications/threatreport.jsp](http://www.symantec.com/security_response/publications/threatreport.jsp) [Accessed June 16, 2016].
- [77] Peter Teufl, et al. "Malware detection by applying knowledge discovery processes to application metadata on the Android Market (Google Play)". Published online in *Wiley Online Library (wileyonlinelibrary.com)*. *Security Comm. Networks*, 2013. doi: 10.1002/sec.675.
- [78] Ying-Dar Lin, et al. "Secure and transparent network traffic replay, redirect, and relay in a dynamic malware analysis environment". *Security Comm. Networks*; 7: 626-640; 2014. doi: 10.1002/sec.764.
- [79] Shabtai, A., et al. "Monitoring, analysis, and filtering system for purifying network traffic of known and unknown malicious content". *Security Comm. Networks*; 4: 947-965; 2011. doi: 10.1002/sec.229.
- [80] Liu, S., et al. "MalPEFinder: fast and retrospective assessment of data breaches in malware attacks". *Security Comm. Networks*; 5: 899-915; 2012. doi: 10.1002/sec.390.
- [81] Danfeng, Y. A. O., Deian Stefan, and Chehai Wu. "Systems and method for malware detection." U.S. Patent No. 8,763,127. 24 Jun. 2014.
- [82] Ferbrache D. *A Pathology of Computer Viruses*. Springer-Verlag, 1992.
- [83] Lance J. Hoffman. *Rogue Programs: Viruses, Worms, and Trojan Horses (Vnr Computer Library)*. Publisher: Van Nostrand Reinhold, 1990.
- [84] Shishir Kumar, Durgesh Pant. "Detection & Preservation of New & Unknown Malware using Honeypots". *International Journal on Computer Science and Engineering*; vol.1(2), 56-61; 2009.
- [85] Imtithal A Saeed, et al. "A Survey on Malware and Malware Detection Systems". *International Journal of Computer Applications*; 67(16): 25-31; 2013.
- [86] Robert E. Mahan. *Malicious Software Copyright 1998-2001*. November 5, 2001.
- [87] CERT Coordination Center. "Which Best Practices are Right For Me?" Version 1.0. *Software Engineering Institute, Carnegie Mellon University*, January 2004. [http://www.cert.org/archive/pdf/secureit\\_bestpractices.pdf](http://www.cert.org/archive/pdf/secureit_bestpractices.pdf) [Accessed March 28, 2016].
- [88] Grégoire Jacob · Hervé Debar · Eric Filiol. Behavioral detection of malware: from a survey towards an established taxonomy. *Springer-Verlag France, J Comput Virol*; 4:251-266; 2008.
- [89] Pascal Meunier. *Classes of Vulnerabilities and Attacks*. Wiley Handbook of Science and Technology for Homeland Security, 2008.