International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017) pp. 7902-7911

Detecting and Neutralizing Encrypting Ransomware Attacks by Using Machine-Learning Techniques: A Literature Review

Edgar P. Torres P. and Sang Guun Yoo

Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Ladrón de Guevara, E11-253, Quito, Ecuador.

Abstract

Almost immediately after the initial design and implementation of first computers systems accessible to the general public and businesses, computer programs so called viruses and malware appeared into computing and informatics scenario, representing a big threat to normal informatics applications operation, and in most cases causing loss of time, data, and huge amount of money. Therefore a lot of research has been done to produce software capable of protecting businesses an individual user from this terrible and annoying menace. Among these viruses and malware threats, one has gotten a lot of attention lately, namely, ransomeware malware, which is capable of avoiding most of important and expensive antivirus and antimalware applications, and starts encrypting and modifying files and directories, with the purpose of asking for money in exchange of some key needed to be able to hopefully recover the affected data in the computer system. The present research work is focused in investigating current literature in this field in order to determine the state of the art regarding malware prevention, detection, and recovery (curing) when a computer system is attacked by virus and malware, and in particular by the so called ransomware one.

Keywords: Malware, Ransomware, Machine Learning, Malware Detection Algorithms.

INTRODUCTION

Regarding computer attacks caused by malware, one of the most destructive and devastating is the one caused by the so-called encrypting ransomware, which is a program that infiltrates computers and, without user knowledge, changes the name of files and encrypts their contents. Afterwards, the affected user is asked to pay a very high ransom fee in order to be able to regain access to the encoded information, by means of a secret key which is supplied by the malware manufacturer after the payment. The user is told that he hopefully will be able to recover part or all of the stolen information if he complies with such malware payment demands. The purpose of this paper is to review researches related to detecting ransomwares and proceeding to disable such type of attack, giving to the user the opportunity to prevent the loss his valuable information. Previous researches have used many methods to detect a ransomware type of malware. Basically we can think of two types of ransomware detection approaches: first is to device different methods to analyze executing files in order to determine whether they pose some kind of risk by the time of being executed in a computer, second is to analyze the type of actions some executing file is producing on the computer, for example the type of I/O file activity, file modification or renaming, etc., in order to determine if these actions are related to suspicious attack patterns typical of a ransomware type of attack.

A modern and useful approach in order to achieve the ways of ransomware detection, previously explains, is by using different kinds of machine learning (ML) techniques, which will allow us to learn the type of behavior a ransomware activity is like, therefore a suitable defense may be implemented. Using ML we can learn normal day to day operation of the computer system by a typical user of such system, afterwards this valuable information could be used to identify suspicious ransomware behavior not typical of a typical user of a specific computer. Basically in this kind of approach, a method using machine-learning techniques is developed in order to monitor the computer in search for abnormal processes that might be initiating suspicious changing activities in files and directories of a computer. These highly suspicious processes will then be compared with typical ransomware file modification attack patterns, which will be quite different from those present under normal operation of the computer.

In summary we can identify two types of malware detection approaches for this kind of menace. First one is based on analyzing the coding of an unknown program, in order to determine the associated risk this program represents when being executed in the system. In case the file poses a risk, the file will be eliminated or reported to the user for instruction on how to proceed further. On the other hand if the unknown program starts executing and turns out to exhibit a typical ransomeware behavior, then the program might be stopped and reported to user, providing him with relevant information about the suspicious activity, so that he will have opportunity to decide what kind of action is to be taken in every case.

Also it will be advisable to explore the possibility of using some kind of special backing up operation in order to protect the

information that is being processed, and therefore minimize the negative effects produced by the malware attack during the time it was taking place, and until its action was detected and stopped. Of course various kinds of information systems and operating platforms may be attacked, therefore we have to be aware of the various possibilities that might appear.

This paper is organized as follows. Section 2 explains basic idea of the research methodology used in this work, which allowed to find hundreds of papers related to this area, and next filter them so that we keep the most important ones for our discussion, namely 62 selected papers in total. After that, various methods (criteria) of classification are defined and presented in section 3, which will then be used in order to do a cross-referencing of important information from all selected papers. Then, in section 4, a classification of selected research documents is worked and Table 1 is presented as the result of it. An important analysis is done for selected papers using table 1 and the papers themselves, and valuable comments are issued as a result of this analysis. Finally section 5 presents several important conclusions obtained throughout the work done in this research, and final section provides the corresponding list of references.

RESEARCH METHODOLOGY

Because of the popularity of researches related to malware and viruses, hundreds of documents would be found if none specific criteria were applied at the moment of looking for papers in such subjects. Therefore, it is important to state some kind of restrictions on what type of information is really the one we are interested in. To this end, we enumerate the following criteria to filter out the extensive information we are going to be getting.

- Only those articles that have been published formally in journals and conferences are to be taken into account. Also some material published on the web, will be considered as long as it is highly technical and precise.
- Only those article which are related to ransomware type of malware are to be considered, since this is the main objective of our technical review.
- Masters and Doctoral Dissertations, books, technical information published on the web, might be considered as long as the material is of the high quality type.
- For this research, we will focus only on those solutions applicable for the Microsoft Windows platform. (preferably for servers and desktop devices)

Following this criteria, many papers and documents were discarded, and less than one hundred of them remained to be reviewed and studied in more detail.

METHOD OF CLASSIFICATION

Various aspect of the malware and virus detection and prevention field have been considered at the moment of classifying selected papers. In the following, we present those aspects that have been taken into account. We will provide a short description of the technical aspect that will considered and the kind of information that will be saved for further analysis.

- **Mobile devices**: Even though we are mainly interested in papers regarding server and desktop devices, we have also considered many papers dealing with mobile devices, which are subject to be attacked by viruses and malware in general. This field has had a big development throughout last years, and many of the techniques and approaches used for dealing with the ransomware menace are also applicable or adaptable to the servers and desktop case.
- **Machine Learning (ML):** Actually one key feature to be considered in our research is the one related to Machine Learning. This aspect is very important to us, since one of our purposes is to investigate the role artificial intelligence represents in dealing with various kinds of viruses and malware. We consider that Machine Learning techniques are very important in this field because they allow us to develop procedures that will be capable of learning and becoming more powerful and effective as they are used. Therefore when time comes to start fighting against viruses and malware, ML algorithms are even capable of under covering suspicious programs, that now days are mutating in order to avoid been detected by standard antivirus detection techniques. Different kind of machine learning models can be used. Among them we can mention the supervised type, which requires some appropriate training data sets to be used for ML training purposes. Also we have the unsupervised model which adapts while it is operating. Finally we have some mix of the two previous ones, as the so called semi supervised learning machine type having specific advantages and disadvantages.
- **Recovery Methods:** When a computer system is attacked by a ransomware type of malware, files and information in general are seriously affected in different ways, for example data may have been deleted, blocked, encrypted, renamed, replaced, etc. Recovering Methods are the one that will be used in order to recover the compromised dada as much as possible, and regain control of a healthy computer system environment. Of course there are many recovery methods, some of them are designed to be used when a virus has actually been prevented of attacking the computer system. In this case virus and malware cleaning procedures will have to be run in order to get rid of infecting software. In other cases, the malware and viruses may have remained undetected, therefore they might have actually affected our computer, causing devastating effects, depending the amount of time they were allowed to operate. It is clear that also in this case some type of

appropriate procedure needs to be used in order to minimize the damage caused by the attack.

- **Behavioral-Based Approach:** This feature has to do with the way viruses or malware are going to be detected. In order to deal with this kind of problem, one has to know the way viruses or malware really operate. As mentioned before, basically we identify two type of strategies when attempting to detect and eliminate the infecting software, namely the preventive and reactive ones. Behavioral approach is a very important one, and is focused in knowing the way ransomeware attacks; using this knowledge this approach allow us to determine whether the suspicious software is actually of the ransomware type, and also, in case the malware ran undetected, it will be possible to determine as soon as possible that the computer system is actually under attack. In any case this will permit us to take appropriate correcting actions.
- **Testing Malware Detectors:** In this case we are concerned with testing the various kind of malware detector that have been devised, and specifically the ones which we are going to be using in our solution. Therefore we will be considering and designing appropriate malware testing environments, that will allow us to test real virus and malware attacks, visualize attacking patterns, and test the quality and effectiveness of malware detector solutions that we are using.
- **Malware Detector Evaluation:** In this case we are interested in evaluating various kinds of Malware Detectors, comparing the different approaches and technologies we are using, and clearly establish the specific advantages and disadvantages encountered.
- **Infrastructure Evaluation:** This features has to do with evaluating the infrastructure that we are using in our computer system. For example we are going to be interested in knowing how robust the infrastructure is in relation to dealing with malware and viruses attacks. Also we can evaluate whether the type of infrastructure we are using is resistant to certain type of malware attacks or not. It is good to mention that it is known to be certain firewalls which are able to stop and block certain type of suspicious or attacking patterns.
- **Analytical Results:** This aspect has to do with the way data and information, collected or studied in various papers, is analyzed in order to produce knowledge and get to important conclusions. Therefore in this case we are interested in statistics and reports that will give us further insight into the various aspects under consideration in a specific paper.
- **Semantic Detection Methods:** This is a quite different approach to the usual ones, in this kind of approach we analyze design and implement the detection task from the semantic point of view, that is to say from the meaning of the actions intended by the attacker. Of course this way of focusing the detection of an attack has advantages and disadvantages compared to all other method in this field.
- **Dynamic Analysis:** This is a very important aspect of our research since this approach focuses on analyzing what and how attacking actions are being taken place in real time, thus allowing us to understand how the attacking virus is actually delivering its harmful actions to our computer system. Then we will be able to use this knowledge at the time of devising, designing, and implementing appropriate detection methods being capable of stopping and eliminating unwanted and dangerous programs from our computer system as soon as possible.
- **Static Analysis:** This kind of approach allow us to determine, studying and analyzing the structure and binary code of a suspicious program, the way it is designed to perform and whether it is harmful or not for our computer system. It is consider a static approach because the analysis is not performed during actual operation of the threatening program.
- **Detect Metamorphic Viruses:** In this case we are interested in detecting malware and viruses which are capable of translating, editing, and rewriting its own code several times, impeding in this way antivirus programs to properly detect them. It is good to note that this case is different to the polymorphic virus which has the ability of encrypting its original code so that it goes undetected by most antivirus programs.
- **Comparative Analysis:** This feature has to do with papers and documents of interest that concentrates on studying and comparing various types of known viruses. Therefore some useful study can presented about comparisons among specific malware and viruses, allowing us in this way to gain better insight and knowledge about these dangerous programs and its behavior.
- **Algorithms:** In this case we are concerned with papers and documentation of interest that suggest or present algorithms to be used in this field. We can mention some of these algorithm, for example encrypting algorithms, detecting algorithms, machine learning algorithms, etc.
- **Real Time Protection:** This one is a very important feature to be considered, it has to do with the way we can implement malware and virus protection, and thus effectively giving real time protection to our computer system before some damage is produce to our data and information. That is to say, not waiting until it is too late and the damage is big.

Classification of Selected Research Documents

In order to classify selected researched documents we use the 15 methods of classification presented in section 3. To this end we consider all selected papers using the criteria stated before,

and carefully cross-reference them with every classification method. Table 1 has been designed to properly show the result of this procedure. It is worth to note that in order to mark every one of the cross-referenced boxes in table 1, we have taken into account to what extent the associated concept or aspect is treated in a specific paper.

Therefore in Table 1 we can see the aspects that most meet the information contained in each paper, these aspects appear marked with a "Y", in the corresponding Colum of the chart. The purpose of this chart is to get knowledge about information treated in selected papers. For example we can see which and how many papers meet every criterion under consideration. This information is extremely valuable since it will allow us to get to know how much information is available in the field considered, and what aspects of such information are more treated in the scientific research and documentations available.

Table 1: Cross-reference between selected papers and various aspects of interest as described in section 3

References	MOBILE DEVICES	MACHINE LEARNING	RECOVERY METHODS	BEHAVIOURAL-BASED APPROACH	TESTING MALWARE DETECTORS	MALWARE DETECTORS EVALUATION	INFRAESTRUCTURE EVALUATION	ANALYTICAL RESULTS	SEMANTIC DETECTION METHODS	DYNAMIC ANALYSIS	STATIC ANALYSIS	DETECT METAMORPHIC VIRUS	COMPARATIVE ANALYSIS	ALGORITHMS	REAL TIME PROTECTION
[1]			Y	Y		Y									
[2]									Y		Y		Y		
[3]		Y												Y	
[4]		Y		Y		Y				Y					
[5]													Y		
[6]												Y			
[7]			Y	Y											Y
[8]						Y	Y	Y					Y		
[9]						Y					Y	Y			
[10]						Y									Y
[11]						Y		Y	Y						
[12]			Y	Y						Y					Y
[13]					Y	Y	Y	Y					Y		
[14]			Y	Y			Y	Y		Y					
[15]				Y		Y		Y		Y					
[16]				Y						Y					
[17]	Y			Y							Y				
[18]						Y		Y		Y					
[19]		Y		Y						Y					
[20]		Y		Y		Y				Y					
[21]		Y		Y		Y				Y					
[22]					Y	Y	Y								
[23]			Y					Y							
[24]			Y			Y								Y	

[25]						**Y**					**Y**				
[26]		**Y**	**Y**		**Y**						**Y**				
[27]		**Y**			**Y**						**Y**				
[28]						**Y**		**Y**			**Y**				**Y**
[29]						**Y**						**Y**			
[30]		**Y**	**Y**	**Y**				**Y**		**Y**					
[31]		**Y**	**Y**	**Y**						**Y**					
[32]	**Y**		**Y**	**Y**				**Y**		**Y**					
[33]			**Y**	**Y**				**Y**							
[34]			**Y**					**Y**			**Y**				
[35]	**Y**		**Y**					**Y**			**Y**				
[36]		**Y**		**Y**	**Y**			**Y**		**Y**					
[37]					**Y**								**Y**		
[38]		**Y**			**Y**			**Y**			**Y**				
[39]					**Y**	**Y**									
[40]			**Y**			**Y**		**Y**		**Y**					
[41]			**Y**	**Y**		**Y**									
[42]			**Y**					**Y**							
[43]			**Y**	**Y**				**Y**							
[44]		**Y**					**Y**								
[45]	**Y**	**Y**													
[46]		**Y**		**Y**											
[47]	**Y**	**Y**													
[48]	**Y**	**Y**								**Y**					
[49]	**Y**					**Y**									
[50]		**Y**	**Y**								**Y**			**Y**	
[51]						**Y**				**Y**					
[52]	**Y**	**Y**	**Y**			**Y**					**Y**				
[53]		**Y**		**Y**	**Y**			**Y**							
[54]	**Y**	**Y**			**Y**					**Y**					
[55]			**Y**		**Y**			**Y**							
[56]			**Y**		**Y**			**Y**							
[57]	**Y**	**Y**				**Y**									
[58]					**Y**								**Y**	**Y**	
[59]			**Y**			**Y**	**Y**	**Y**							
[60]						**Y**					**Y**		**Y**		
[61]	**Y**										**Y**				
[62]		**Y**				**Y**								**Y**	
TOTAL	**11**	**22**	**22**	**20**	**13**	**26**	**6**	**22**	**2**	**17**	**14**	**3**	**7**	**5**	**4**

Looking at the information supplied by Table 1, row labeled TOTAL, we can see the total number of papers meeting a selected aspect or classification criterion. For example criterion 3.2 labeled as Machine Learning, has a total of 22 papers out of 62, which represents a 35.48 % of the total papers in Table 1.

A further analysis shows us, for example, that columns labeled with criterions 3.2, 3.3, 3.4, 3.6, 3.8 represents more than 35.48 % each, out of all papers considered; whereas columns involving criterions 3.7, 3.9, 3.12, 3.13, 3.14, 3.15, represents less than 11.29 % each, out of all selected papers also referenced in Table 1.

Continuing reviewing the cross-referenced literature considered in Table 1, we can also point out some more issues as follows:

- A total of 11 papers [17,32,35,45,47,48,49,52,54,57,61] out of 62 are focused on mobile devices, representing 17.7 %, showing that this field has undergone a big development and so has the malware and viruses threats and attacks to the mobile platform. As already mentioned, even though we are more interested in desktops, a lot of interesting information can be reviewed in this papers, and many techniques and problems solved references can be applied or adapted to the fixed platforms; just to see two examples take in consideration: 100 research works (from 2010 to 214) are studied in paper [17], four groups are considered (static features, dynamic features, hybrid features and applications metadata); a malware detection system for android based mobile devices is presented in paper [32], the system takes into account four key features of the mobile platform, and it is assured to solve about 96% of typical threats, and focuses on malware behavior to detect and stop malicious threats.
- Most of the selected papers considered in this research addresses at the same time many of the features regarded as classification criteria (section 3). Just to show some examples let us consider the following: paper [4] the so called EldeRan application is presented which consists of a ML implementation capable of dynamically analyze and classify ransomeware malware. At the same time behavioral-based approach, and malware detectors evaluation are considered; paper [34] addresses recovery methods (detection, prevention, and cure), also at the same time considers static analysis, and show analytical results.
- Reviewing the selected papers, very few papers as compared to the total reviewed, were related to semantic detection methods (2), and metamorphic virus detection (3).
- It is interesting to note that 6 papers [45,47,48,52,54,57] of 11 papers, some 54.5%, focused on mobile devises, and at the same time addresses the Machine Learning criterion, showing the importance of ML techniques for malware detection.
- There are many papers, 20 out of 62 representing some 32.3%, addressing the behavioral-based approach criterion [1,4,7,12,14,15,16,17,19,20, 21,30,31,32,33,36,41,43,46,53] but most of them focuses in prevention and detection of a typical malware attack that is about to happen, but few concentrate on the ransomware detection once the attack is initiated.

CONCLUSIONS

Several valuable conclusions can be obtained from the present literature review.

- We can easily notice that a good amount of information is available for aspects of interest such as Machine learning (22 papers), Recovery Methods (22 papers), Behavioral Approach (20 papers), Malware Detection Evaluation (26 papers), and Analytical results (22 papers); all of these criteria represent over 35 % each, out of all selected papers.
- Machine Learning Techniques have become very powerful tools at the moment of doing behavioral-based detection; the importance of ML resides, among other reasons, in being capable of learning and adapting to many varying conditions, such as those created by metamorphic viruses and malware, which are capable of changing their code by reprogramming themselves and successfully avoiding detection by most of standard detection techniques.
- The least amount of papers in Table 1 corresponds to Semantic Detection Methods (2 papers).
- Also we can notice that the behavioral-based detection approach is important since allow us to perform a dynamic analysis and detection of the virus and malware.
- Additionally, mobile devised have gotten big attention and we think that this field will develop fast in the future.
- Cross-referenced information contained in Table 1 is very important and helpful at the time to get many other conclusions of the selected papers reviewed in the present work, and of course many charts providing valuable insight in malware and virus detection, could be obtained using these results.
- Finally it is worth to mention that according section 4, issue number 5, there is a good and very important opportunity of increasing research about detection and

curing techniques required in case a ransomware malware was successful avoiding antivirus software action, and has already started to attack data in computer systems.

REFERENCES

[1] Wecksten, Mattias, Jan Frick, Andreas Sjostrom, and Eric Jarpe. 2017. "A Novel Method for Recovery from Crypto Ransomware Infections." *2016 2nd IEEE International Conference on Computer and Communications, ICCC 2016 - Proceedings*, 1354–58. doi:10.1109/CompComm.2016.7924925.

[2] Preda, Mila Dalla, Mihai Christodorescu, Somesh Jha, and Saumya Debray. 2008. "A Semantics-Based Approach to Malware Detection." *ACM Transactions on Programming Languages and Systems* 30 (5): 1–54. doi:10.1145/1387673.1387674.

[3] Hosfelt, Diane Duros. 2015. "Automated Detection and Classification of Cryptographic Algorithms in Binary Programs through Machine Learning." http://arxiv.org/abs/1503.01186.

[4] Sgandurra, Daniele, Luis Muñoz-González, Rabih Mohsen, and Emil C. Lupu. 2016. "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection." doi:10.15199/48.2015.11.48.

[5] Gazet, Alexandre. 2010. "Comparative Analysis of Various Ransomware Virii." *Journal in Computer Virology* 6 (1): 77–90. doi:10.1007/s11416-008-0092-2.

[6] Daoud, Essam Al, Ih Jebril, and Belal Zaqaibeh. 2008. "Computer Virus Strategies and Detection Methods." *International Journal Open Problems Computer and Mathematics* 1 (2): 122–29. http://www.emis.ams.org/journals/IJOPCM/files/IJOPCM(vol.1.2.3.S.08).pdf.

[7] Scaife, Nolen, Henry Carter, Patrick Traynor, and Kevin R.B. Butler. 2016. "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data." *Proceedings - International Conference on Distributed Computing Systems* 2016–Augus: 303–12. doi:10.1109/ICDCS.2016.46.

[8] Cabaj, Krzysztof, Piotr Gawkowski, Konrad Grochowski, and Amadeusz Kosik. 2016. "Developing Malware Evaluation Infrastructure." *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)* 8: 981–89. doi:10.15439/2016F490.

[9] You, Ilsun, and Kangbin Yim. 2010. "Malware Obfuscation Techniques: A Brief Survey." *Proceedings - 2010 International Conference on Broadband, Wireless Computing Communication and Applications, BWCCA 2010*, no. November 2010: 297–300. doi:10.1109/BWCCA.2010.85.

[10] Kharraz, Amin, and Engin Kirda. n.d. "Redemption: Real-Time Protection Against Ransomware at End-Hosts." http://www.ccs.neu.edu/home/mkharraz/publications/raid2017redemption.pdf.

[11] Christodorescu, Mihai, Somesh Jha, Sanjit A. Seshia, Dawn Song, and Randal E. Bryant. 2005. "Semantics-Aware Malware Detection." *Proceedings - IEEE Symposium on Security and Privacy*, 32–46. doi:10.1109/SP.2005.20.

[12] Continella, Andrea, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, and Federico Maggi. 2016. "ShieldFS: A Self-Healing, Ransomware-Aware Filesystem." *Proceedings of the 32nd Annual Conference on Computer Security Applications - ACSAC '16*, 336–47. doi:10.1145/2991079.2991110.

[13] Christodorescu, Mihai, and Somesh Jha. 2004. "Testing Malware Detectors." *ACM SIGSOFT Software Engineering Notes* 29: 34. doi:10.1145/1013886.1007518.

[14] Kharaz, Amin, Sajjad Arshad, Collin Mulliner, William Robertson, Collin Mulliner, and William Robertson. 2016. "UNVEIL : A Large-Scale , Automated Approach to Detecting Ransomware," 1–36. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kharaz.

[15] Yoshiro Fukushima, Akihiro Sakai, Yosjiaki Hori, and Kouichi Sakurai. 2010. "A Behavior Based Malware Detection Scheme for Avoiding False Positive." *2010 6th IEEE Workshop on Secure Network Protocols (NPSec)*, 79–84. http://ieeexplore.ieee.org.wam.seals.ac.za/xpl/articleDetails.jsp?tp=&arnumber=5634444&queryText=a+behavior+based+malware.

[16] Trinius, Philipp, Carsten Willems, Thorsten Holz, and Konrad Rieck. 2011. "A Malware Instruction Set for Behavior-Based Analysis." *Sicherheit Schutz Und Zuverlässigkeit SICHERHEIT*, no. TR-2009-07: 1–11. doi:10.1.1.370.9032.

[17] Feizollah, Ali, Nor Badrul Anuar, Rosli Salleh, and Ainuddin Wahid Abdul Wahab. 2015. "A Review on Feature Selection in Mobile Malware Detection." *Digital Investigation* 13 (March). Elsevier Ltd: 22–37. doi:10.1016/j.diin.2015.02.001.

[18] Egele, Manuel, Theodoor Scholte, Engin Kirda, and Christopher Kruegel. 2012. "A Survey on Automated Dynamic Malware-Analysis Techniques and Tools." *ACM Computing Surveys* 44 (2): 1–42. doi:10.1145/2089125.2089126.

[19] Hansen, Steven Strandlund, Thor Mark Tampus Larsen, Matija Stevanovic, and Jens Myrup Pedersen. 2016. "An Approach for Detection and Family Classification of Malware Based on Behavioral Analysis." *2016 International Conference on Computing, Networking and Communications, ICNC 2016*. doi:10.1109/ICCNC.2016.7440587.

[20] Firdausi, Ivan, Charles Lim, Alva Erwin, and Anto Satriyo Nugroho. 2010. "Analysis of Machine Learning Techniques Used in Behavior-Based Malware Detection." *2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies*, 201–3. doi:10.1109/ACT.2010.33.

[21] Rieck, Konrad, Philipp Trinius, Carsten Willems, and Thorsten Holz. 2011. "Automatic Analysis of Malware Behavior Using Machine Learning." *Journal of Computer Security* 19 (4): 639–68. doi:10.3233/JCS-2010-0410.

[22] Cohen, Fred. 1987. "Computer Viruses Theory and Experiments." *International Journal of Security and Its ...* 6 (211): 22–35. doi:10.1007/978-3-540-74203-6.

[23] Ahmadian, Mohammad Mehdi, Hamid Reza Shahriari, and Seyed Mohammad Ghaffarian. 2016. "Connection-Monitor & Connection-Breaker: A Novel Approach for Prevention and Detection of High Survivable Ransomwares." *12th International ISC Conference on Information Security and Cryptology, ISCISC 2015*, 79–84. doi:10.1109/ISCISC.2015.7387902.

[24] Young, A., and Moti Yung. 1996. "Cryptovirology: Extortion-Based Security Threats and Countermeasures." *Proceedings 1996 IEEE Symposium on Security and Privacy* 5111 (C): 129–40. doi:10.1109/SECPRI.1996.502676.

[25] Alazab, Mamoun, Sitalakshmi Venkatraman, Paul Watters, Moutaz Alazab, and Ammar Alazab. 2012. "Cybercrime: The Case of Obfuscated Malware." *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering* 99 LNICST: 204–11. doi:10.1007/978-3-642-33448-1_28.

[26] Shabtai, Asaf, Robert Moskovitch, Yuval Elovici, and Chanan Glezer. 2009. "Detection of Malicious Code by Applying Machine Learning Classifiers on Static Features: A State-of-the-Art Survey." *Information Security Technical Report* 14 (1). Elsevier Ltd: 16–29. doi:10.1016/j.istr.2009.03.003.

[27] Sharif, Monirul, Vinod Yegneswaran, Hassen Saidi, Phillip Porras, and Wenke Lee. 2008. "Eureka: A Framework for Enabling Static Malware Analysis." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 5283 LNCS: 481–500. doi:10.1007/978-3-540-88313-5-31.

[28] Chen, Kai, Peng Wang, Yeonjoon Lee, XiaoFeng Wang, Nan Zhang, Heqing Huang, Wei Zou, and Peng Liu. 2015. "Finding Unknown Malice in 10 Seconds: Mass Vetting for New Threats at the Google-Play Scale." *24th USENIX Security Symposium (USENIX Security 15)*, 659–74. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/chen-kai.

[29] Wong, Wing, and Mark Stamp. 2006. "Hunting for Metamorphic Engines." *Journal in Computer Virology* 2 (3): 211–29. doi:10.1007/s11416-006-0028-7.

[30] Zamboni, Diego, and Christopher Kruegel. 2006. "Recent Advances in Intrusion Detection." http://books.google.co.uk/books?id=9iv9UpdyjhUC&pg=PA266&lpg=PA266&dq=node+speed+is+increased+more+message+overhead+to+confront+these+changes.&source=bl&ots=RWGPVAtRU4&sig=Kj8v6FDOfVmSY5wztRAsOw7S-_8&hl=en&sa=X&ei=h1deULzBMfC20QWw14HoDA&ved=0CDAQ6AEwAA#v=onepage&q=node speed is increased more message overhead to confront these changes.&f=false.

[31] Kolter, Jeremy Z., and Marcus A. Maloof. 2004. "Learning to Detect Malicious Executables in the Wild." *Proceedings of the 2004 ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD '04* 57 (11): 470. doi:10.1145/1014052.1014105.

[32] Saracino, Andrea, Daniele Sgandurra, Gianluca Dini, and Fabio Martinelli. 2016. "MADAM: Effective and Efficient Behavior-Based Android Malware Detection and Prevention." *IEEE Transactions on Dependable and Secure Computing* 5971 (c): 1–1. doi:10.1109/TDSC.2016.2536605.

[33] Richardson, Ronny, and Max North. 2017. "Ransomware: Evolution, Mitigation and Prevention." *International Management Review* 13 (1): 10–22. doi:http://dx.doi.org/10.1108/17506200710779521.

[34] Brewer, Ross. 2016. "Ransomware Attacks: Detection, Prevention and Cure." *Network Security* 2016 (9). Elsevier Ltd: 5–9. doi:10.1016/S1353-4858(16)30086-1.

[35] Mercaldo, Francesco, Vittoria Nardone, and Antonella Santone. 2016. "Ransomware inside out." *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 628–37. doi:10.1109/ARES.2016.35.

[36] Santos, Igor, Javier Nieves, and Pablo G. Bringas. 2011. "Semi-Supervised Learning for Unknown Malware Detection." *Advances in Intelligent and Soft Computing* 91: 415–22. doi:10.1007/978-3-642-19934-9_53.

[37] Cabaj, Krzysztof, Marcin Gregorczyk, and Wojciech Mazurczyk. 2015. "Software-Defined Networking-Based Crypto Ransomware Detection Using HTTP Traffic Characteristics." https://arxiv.org/ftp/arxiv/papers/1611/1611.08294.pdf.

[38] Nath, Hiran V., and Babu M. Mehtre. 2014. "Static Malware Analysis Using Machine Learning Methods," 440–50. doi:10.1007/978-3-642-54525-2_39.

[39] A, Gandhi Krunal (Laxmi Institute of Sarigam, Valsad), and Valsad) D, Patel Viral Kumar (Laxmi Institue of Sarigam. 2017. "Survey on Ransomware : A New Era of Cyber Attack." *International Journal of Computer Applications* 168 (3): 38–41.

[40] Willems, Garsten, Thorsten Holz, and Felix Freiling. 2007. "Toward Automated Dynamic Malware Analysis Using CWSandbox." *IEEE Security and Privacy* 5 (2): 32–39. doi:10.1109/MSP.2007.45.

[41] Koch, R. 2011. "Towards next-Generation Intrusion Detection." *2011 3rd International Conference on Cyber Conflict*, 1–18.

[42] Sittig, D. F., and H. Singh. 2016. "A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks." *Applied Clinical Informatics* 7 (2): 624–32. doi:10.4338/ACI-2016-04-SOA-0064.

[43] Siddiqui, Muazzam, Morgan C. Wang, and Joohan Lee. 2008. "A Survey of Data Mining Techniques for Malware Detection Using File Features." *Proceedings of the 46th Annual Southeast Regional Conference on XX - ACM-SE 46*, 509. doi:10.1145/1593105.1593239.

[44] Stevanovic. 2016. *Machine Learning for Network-Based Malware Detection*. doi:10.5278/vbn.phd.engsci.00088.

[45] Hyo-Sik Ham, and Mi-Jung Choi. 2013. "Analysis of Android Malware Detection Performance Using Machine Learning Classifiers." *2013 International Conference on ICT Convergence (ICTC)*, 490–95. doi:10.1109/ICTC.2013.6675404.

[46] Bose, Abhijit, Xin Hu, Kang G. Shin, and Taejoon Park. 2008. "Behavioral Detection of Malware on Mobile Handsets." *Proceeding of the 6th International Conference on Mobile Systems, Applications, and Services - MobiSys '08*, no. January 2008: 225. doi:10.1145/1378600.1378626.

[47] Kurniawan, Harry. 2015. "Android Anomaly Detection System Using Machine Learning Classification." *The 5th International Conference on Electrical Engineering and Informatics*, no. 10: 288–93.

[48] Amos, Brandon, Hamilton Turner, and Jules White. 2013. "Applying Machine Learning Classifiers to Dynamic Android Malware Detection at Scale." *2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013*, 1666–71. doi:10.1109/IWCMC.2013.6583806.

[49] Yang, Tianda, Yu Yang, Kai Qian, Dan Chia Tien Lo, Ying Qian, and Lixin Tao. 2015. "Automated Detection and Analysis for Android Ransomware." *Proceedings - 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security and 2015 IEEE 12th International Conference on Embedded Software and Systems, H*, no. 1: 1338–43. doi:10.1109/HPCC-CSS-ICESS.2015.39.

[50] Alazab, Mamoun, Robert Layton, Sitalakshmi Venkataraman, and Paul Watters. 2010. "Malware Detection Based on Structural and Behavioural Features of API Calls." *Proceedings of the 2010 International Cyber Resilience Conference*, no. August: 1–10. http://ro.ecu.edu.au/icr/1/.

[51] Petsas, Thanasis, Giannis Voyatzis, Elias Athanasopoulos, Michalis Polychronakis, and Sotiris Ioannidis. 2014. "Rage Against the Virtual Machine: Hindering Dynamic Analysis of Android Malware." *Proceedings of the Seventh European Workshop on System Security*, 5:1--5:6. doi:10.1145/2592791.2592796.

[52] Shabtai, Asaf, Yuval Fledel, and Yuval Elovici. 2010. "Automated Static Code Analysis for Classifying Android Applications Using Machine Learning." *Proceedings - 2010 International Conference on Computational Intelligence and Security, CIS 2010*, 329–33. doi:10.1109/CIS.2010.77.

[53] Markel, Zane, and Michael Bilzor. 2014. "Building a Machine Learning Classifier for Malware Detection." *2014 Second Workshop on Anti-Malware Testing Research (WATeR)*, 1–4. doi:10.1109/WATeR.2014.7015757.

[54] Wu T A - Wen-Chieh. 2014. "DroidDolphin: A Dynamic Android Malware Detection Framework Using Big Data and Machine Learning." 43 NI-LG. doi:10.1145/2663761.2664223.

[55] Kalaimannan, Ezhil, Sharon K John, Theresa Dubose, Anthony Pinto, Ezhil Kalaimannan, Sharon K John, Theresa Dubose, and Anthony Pinto. 2017. "Influences on Ransomware ' S Evolution and Predictions for the Future Challenges." *Journal of Cyber Security Technology* 1 (1). Taylor & Francis: 23–31. doi:10.1080/23742917.2016.1252191.

[56] Rieck, Konrad, Thorsten Holz, Carsten Willems, Patrick Düssel, and Pavel Laskov. 2008. "Learning and Classification of Malware Behavior." In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in*

Bioinformatics), 5137 LNCS:108–25. doi:10.1007/978-3-540-70542-0_6.

[57] Shamili, a.S. S Ashkan Sharifi, Christian Bauckhage, and Tansu Alpcan. 2010. "Malware Detection on Mobile Devices Using Distributed Machine Learning." *Pattern Recognition (ICPR), 2010 20th International Conference on* 0: 4348–51. doi:10.1109/ICPR.2010.1057.

[58] Cabaj, Krzysztof, Piotr Gawkowski, Konrad Grochowski, and Dawid Osojca. 2015. "Network Activity Analysis of CryptoWall Ransomware." *Przeglad Elektrotechniczny* 91 (11): 201–4. doi:10.15199/48.2015.11.48.

[59] Hampton, Nikolai. 2015. "Ransomware : Emergence of the Cyber-Extortion Menace" 2015: 47–56.

[60] Monshizadeh, Mehrnoosh, and Zheng Yan. 2014. "Security Related Data Mining." In *Proceedings - 2014 IEEE International Conference on Computer and Information Technology, CIT 2014*, 775–82. doi:10.1109/CIT.2014.130.

[61] Song, Sanggeun, Bongjoon Kim, and Sangjun Lee. 2016. "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform." *Mobile Information Systems* 2016. doi:10.1155/2016/2946735.

[62] Ahmed, Faraz, Haider Hameed, M Zubair Shafiq, and Muddassar Farooq. 2009. "Using Spatio-Temporal Information in API Calls with Machine Learning Algorithms for Malware Detection." *AISec '09 Proceedings of the 2nd ACM Workshop on Security and Artificial Intelligence*, Pages 55-62. doi:10.1145/1654988.1655003.