Asian Journal of Information Technology 16 (6): 458-464, 2017
ISSN: 1682-3915
© Medwell Journals, 2017

Malware Research Directions: A Look into Ransomware

[1]Mohammed A.F. Salah, [2]Mohd Fadzli Marhusin and [1]Rossilawati Sulaiman
[1]Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM),
43600 Bangi, Selangor, Malaysia
[2]Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM),
Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia

Abstract: In the 21st century, malware is considered to be a major threat for cyber security. Malware writers are very active and as a result there are huge numbers of new malwares getting introduced every day. This is despite the efforts of anti-virus companies who are working hard to detect these malwares. However, many malwares remain undetected. In recent times, a malware called Ransomware has been creating a huge problem for people around the world. In many ways, Ransomware is unique and difficult to handle. That is why, it needs special research attention. For that end this study aims to explore the characteristics of Ransomware and provide possible solutions to deal with it by reviewing the existing malware detection methodologies and by providing future direction for research on Ransomware.

Key words: Malware, Ransomware, CryptoLocker, malware detection, static analysis, dynamic analysis

INTRODUCTION

Cyber threats have become common in our daily life. More than 430 million unique malwares have been detected in 2015 alone (Symantec, 2016; Gandotra *et al*., 2014). Malware can appear in various forms such as worms, viruses, Trojan horses, spam, botnet, spyware, Ransomware and so on (Gandotra *et al*., 2014; Woburn, 2016; Kaur and Sharma, 2014).

These days, Ransomware is on the rise. The victims of Ransomware have to pay money in order to get the stolen data back (Singh and Khurmi, 2014; Gazet, 2010). This study focuses on Ransomware. The main purpose of this study is to review the current methodologies used to analyse malware in general and to give directions specifically to help deal with the risks and threats of Ransomware.

Malware detection analysis: There are three common types of malware analysis techniques. These are static analysis, dynamic analysis and hybrid analysis.

The static analysis is an operation sequence by analysing an executable file without executing it (Egele *et al*., 2012). The static analysis can help us investigate the memory errors and can enhance the execution of the program (Aman, 2014; Chen *et al*., 2004; Feng *et al*., 2004). It also, can be used to check a binary executable with different tools (Aman, 2014; Ligh, 2011). Therefore, the static analysis is secure and fast while analyse multipath malware and the false positive rate is low (accuracy is high). The static analysis can detect unknown or new malware but cannot analyse polymorphic and obfuscated code (Jerlin and Jayakumar, 2015).

By comparison, the dynamic analysis is a technique that can execute a program and observe the action and implication happening to the system during the run-time (Egele *et al*., 2012). The dynamic analysis can detect new or unknown malware and analyse polymorphic malware and obfuscated code.

On the other hand, the dynamic analysis is vulnerable and consumes a lot of time during the analysis. The rate of false positive is high while accuracy is low and not good in analysing the multipath malware (Jerlin and Jayakumar, 2015).

There are many models that are using the dynamic analysis and have been studied and reviewed in recent years. Gandotr *et al*. (2014) proposed a malware detection tool using the spatio-temporal information from API Call to extract statistical data and features from a malware.

The extracted information is fed into a machine learning algorithm-based detector that builds a model for malware detection (Priyadarshi, 2011). Also, an advanced malware writer will use AV to scan for their code to see whether it will be flagged and eventually updated so that it will not get detected once being used.

Moreover, because of the limitations of the static analysis and the dynamic analysis, a hybrid approach is used in analysing malware. This approach combines the

Corresponding Author: Mohammed A.F. Salah, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), 43600 Bangi, Selangor, Malaysia

characteristics of both static and dynamic analyses. The hybrid approach aims to overcome the limitations of the static and dynamic analysis (Mathur and Hiranwal, 2013).

MATERIALS AND METHODS

Malware detection techniques: Malware detection techniques can be divided into signature-based and behaviour-based (Kharraz *et al*., 2015).

The signature-based detection method is the most famous, fastest and most accurate and common technique used to detect the malware. A signature is a sequence of bytes which is unique to a specific malware (Tobergte and Curtis, 2013). So, by matching the signature available in the anti-virus database with the signature of a malware the anti-virus can decide whether this is a legitimate program or a malware.

The main disadvantage of this technique is that for a malware to be automatically detected in all computers elsewhere, it must be found by someone, reported and eventually updated by a central antivirus company for its signature to be useful for detection (Priyadarshi, 2011).

On the other hand, the behaviour-based detection method studies and examines the behaviour of a malware by executing it and detecting it by using some techniques (Jacob *et al*., 2008). A behaviour-based detection method is effective against zero-day malware attacks; since, it can detect malware that generates devious execution behaviour during a run-time.

However, a challenge is that the technique is susceptible to a false positive rate when a legitimate program is classified as a malicious program (Woburn, 2016).

Ransomware: A Ransomware is a kind of malware which demands payment in exchange of a stolen functionality (Kim *et al*., 2015). Ransomware appeared for the first time in 1989 (Kim *et al*., 2015; Savage *et al*., 2015). A malware called AIDS Trojan was the first malware with Ransomware. AIDS Trojan was propagated through a disk called "AIDS information introductory diskette" (Gazet, 2010). However, the first real attack of Ransomware occurred in 2005 (Savage *et al*., 2015).

Ransomware aims to decrypt the users file or lock their machines according to Savage *et al*. (2015). Additionally, according to Scott and Spaniel (2016) there are two major types of Ransomware: CryptoLocker and Ransomware Locker. These are described here.

CryptoLocker Ransomware or data locker: The CryptoLocker or data locker Ransomware is designed to target the user's data. The affected system will function normally without any limitations. All critical and important functions will continue its work.

However, the user's data and files will be encrypted and become unusable. The user will not be able to open or use any of the files. Afterwards, CryptoLocker Ransomware will demand a ransom in exchange for the key to unlock all the data. Finally, the data locker will search for the user data with different extensions such as DOC, TXT, XLS, JPG, MPEG, RTF PPT MP3, FLV, CPP, PDF and MDB:

Ransomware locker or computer locker: The computer locker Ransomware is created to attack the user's devices, such computers and mobile phones. The locker Ransomware locks the system without touching the user's data and files. The user will have a very limited access to the system.

For example, the Malware may lock the mouse but will allow the user to access to keyboard to enter the payment amount of the demanded ransom. The computer locker Ransomware keeps all valuable data of the user clean and untouched. It is easy to remove this Ransomware by restoring the system to the last system restore point (Savage *et al*., 2015). Ultimately, it is easier to remove the computer locker Ransomware compared with the data locker.

According to Zowarsky and Lindskog (2016), the appearance of Ransomware was noticed mainly in the mid-2000's. Crypto Ransomware has evolved gradually between 2005 and 2012. However, in 2013 a new family of crypto Ransomware has appeared with enhanced encryption mechanisms.

These include CryptoLocker, CryptoLocker 2, Ransomcrypt, Crilock and Dirty Decrypt. Moreover, in 2015, a new variant of crypto Ransomware showed up with more sophisticated encryption techniques such as TelsaCrypt, CryptoLocker, Ransomweb, Pclock, Cryptowall 3, Cryptoblocker and Cryptowall 4.

Early in 2016, some new families of Crypto Ransomware started to appear. These included HPRansm. B, Locky, Ransom 32, HydraCrypt, CryptoLocker. N and Cerber. Hence, all new families and variants of Crypto Ransomware are now using highly sophisticated encryption techniques.

Ransomware threat landscape: The number of users infected by Ransomware is increasing (Kim Soh and Kim, 2015). For example, between April, 2015 and were infected by Ransomware. In comparison this number is 5.5 times greater than the previous year. Ransomware can be propagated in different ways such as e-mail attachments,

network traffic and social engineering toolkits which some can be very convincing to the victims. The main motivation of Ransomware creators is the financial benefits. There are many different targets. However, the main target is a group of people who is ready to pay in order to get stolen data back (Scott and Spaniel, 2016).

Since 2013, Ransomware has moved into different levels of financial payment. Now a days, the minimum ransom starts from $300 for a single computer user. This evolvement has happened since 2013 because of the new techniques and methods used to create and encrypt the Ransomware threat (Savage *et al*., 2015).

The Ransomware creators can target anyone such as normal users, enterprises and governmental or public agencies. Additionally, Ransomware can target different systems such as Personal Computers (PCs), smart phones and servers.

Ransomware propagation: Ransomware can be propagated through several different methods and channels. Some of these can be a service, a malicious advertisement, social engineering, phishing e-mails or e-mail attachments. A detailed discussion on Ransomware propagation methods is presented here (Bhardwaj *et al*., 2016).

Traffic direction systems: By using the traffic direction system, the attacker can direct the users to their intended server. It is generally done through posting a malicious advertisement or asking the users to click on different links containing a video streaming or application upgrade which activates malware. When the user accesses these sites, the malware will affect his/her operating system using the available vulnerabilities.

Social engineering: Through the social engineering technique, the attacker makes an attempt to get into the users system through a legitimate application. This application contains the malware. After the application gets into the system, it will install the malware into the user's system. For example, a fake anti-virus.

Spam e-mails: Phishing e-mails and spam e-mails are some of the major sources which spread the malware into different systems and networks. These e-mails are misleading as they appear as legitimate and friendly e-mails. However, the links and attachments given in the e-mail are infected with malware. When the user clicks on the link or clicks to install the attachment, the malware gets delivered into the network.

Ransomware as a Service (RaaS): Ransomware as a Service ensures mutual benefits between the Ransomware creators and the cyber-criminal attackers. The Ransomware creators hire the cyber-criminal attackers to do their business through the cloud service. Both the malware creators and the cyber-criminal get the benefits by sharing the money.

Targets of Ransomware: The Ransomware creators can target different types of users such as normal users, enterprises and governmental or public agencies. There are three groups which can be targeted by Ransomware (Savage *et al*., 2015).

Normal users: Normal users can be a suitable target of Ransomware as the home users do not have full awareness about the current trends in viruses and malwares. Accordingly, they can be an easy target of the attackers.

Enterprises: Business organizations are considered to be one of the major targets of Ransomware since, they are the sources of valuable information such as customer's sensitive information, databases, reports, source code, forms and so on.

Governmental or public agencies: Governmental and public institutions can also, be major targets of Ransomware. Educational institutions can also, become targets of Ransomware. Important data of the students (such as student grades) and those of administrative staff get affected. For example, the new Jersey school District has been attacked by Ransomware and the attacker asked for ransom payment of 500 bitcoins (US$124,000).

Other than that, Ransomware can target different systems such as Personal Computers (PCs), smartphones and servers, described as follows (Savage *et al*., 2015; Scott and Spaniel, 2016).

Personal Computers (PCs): Normal and average computer users are easy targets for Ransomware. In most of the cases, the normal users do not have sufficient background knowledge regarding computer security. Usually, they get the Ransomware through the social engineering techniques. Many users pay the ransom since there is no other option to get their data back.

Smart phones: Smart phones are widely used devices. More than 80% of the smart phones in use are operated through Android. Millions of tablets and mobile phones are getting operated by Android all around the world. The huge landscape of these devices and the openness of the Android system, gives the opportunity for the malware creators to attack Android users. Ransomware has already

targeted the Android system. In 2013, Android smart phones got infected by Android. Fakedefender through an anti-virus application. In this case, after the user installs the antivirus, the malware locks the smartphone. After that, the attackers ask for the ransom payment.

Servers: Servers are widely used in different kinds of organizations. They contain all the sensitive information and important data related to customers and employees. The organization's servers may include the client list, database, reports, intellectual property documents and so on. Attacking the servers of an organization can put the whole organization in Jeopardy and also can affect the organization's reputation. Ransomware also uses Distributed Denial of Service attack (DDoS) to attack the main servers and the backup servers. Once they take all servers down they ask for a huge amount of money (in general, 10-15 times than the rate they charge for normal users).

RESULTS AND DISCUSSION

Going against Ransomware and the way forward: Lee *et al.* (2017) proposed an advanced prevention and detection system, based on the suspicious and abnormal behaviour of the Ransomware in a cloud analysis system called CloudRPS. The proposed system can monitor servers, files and networks during the run time. Moreover, the system can perform in-depth detection and prevention against various Ransomware attacks.

CloudRPS gathers information from different resources such as the devices and log file. After that, the system will analyse the gathered data to defend against different Ransomware attacks. The main purpose of the proposed system is to prevent and detect the user's system from Ransomware.

Other than this Kharraz *et al.* (2016) investigated a wide range of Ransomware samples from 2006-2014. Through this investigation they could stop Ransomware attacks in spite of the advanced use of cryptography techniques and methods. Through this, they were able to analyse and classify different types of Ransomware. The main idea of their technique is based on monitoring the abnormal system activity by examining I/O request and by providing the protection for the Master File Table (MTF) in the NTFS file system. It is possible to prevent and detect zero-day Ransomware attacks with this technique.

Ahmadian *et al.* (2015) proposed a novel approach to detect and prevent Ransomware attacks. By applying the Domain Generation Algorithm (DGA) and by using connection-monitor and connection breaker, the strongest type of Ransomware called the High Survivable Ransomware (HSR) can be detected. They provided a comprehensive classification of Ransomware: Non encrypted Ransomware (NCR), encrypted Ransomware (CGR), Personal encryption Ransomware (PrCR), Public encryption Ransomware (PuCR) and Hybrid encryption Ransomware (HCR). Based on the main characteristics and in the key exchange protocol, High Survivable Ransomware (HSR) was discovered. The proposed model was successful in preventing the encryption of the user's data and to detect different Ransomware.

Scaife *et al.* (2016) proposed a quantification model that can help in preventing and detecting CryptoLocker in PCs. This model is based on social engineering techniques (perception and behavioural of the attackers). According to the researchers when there is a CryptoLocker in order to protect the user data, a pre-detection (rather than post detection) is necessary.

Zavarsky and Lindskog (2016) investigated different Ransomware families on both the platforms: windows and Android. The researchers studied the evolution of Ransomware from its beginning up to 2016. They found that although Ransomware almost have the same characteristics and behaviour they use different payloads.

In their analysis, the researchers identified that over the years Ransomware has improved the encryption techniques and methods. The analysis shows that it is possible to detect Ransomware in the Windows platform by monitoring the abnormal file system and registry activity. By comparison in the Android platform the risk of Ransomware can be mitigated by paying more attention to permissions requested by the Android application. Moreover, Kharaz *et al.* (2016) proposed a novel dynamic analysis system called UNVEIL. The proposed model is able to detect and analyse the Ransomware attacks and model their behaviour.

The researchers performed a long-term and a large scale analysis by analysing a huge dataset containing 148,223 malware samples. The UNVEIL was able to detect 13,673 Ransomware sample out of a dataset of 148,223 general malwares. The evaluation showed that the proposed model detected new and unknown samples of Ransomware that were not detected by the traditional and current anti-viruses.

Moreover, the newly discovered Ransomware samples were not reported previously by the security companies. The researchers presented a novel approach to detect the CryptoLocker (file locker) Ransomware through monitoring the file system access, combined with artificial user environments for triggering the Ransomware. Additionally, the researchers presented another technique to detect the screen lockers Ransomware, through studying and analysing different

Table 1: The advantages and disadvantages of the reviewed models

Publication	Advantages	Disadvantages	Methods
CloudRPS: a cloud analysis based enhanced Ransomware prevention system	The proposed system is widely available and has timely response The system conducts a real time backup for the user's data to protect it from the Ransomware attacks	None so far	Monitoring network, file and server
Cutting the gordian knot: a look under the hood of Ransomware attacks	Proposed a method that can detect and prevent the zero-day Ransomware attacks	None so far	Behavioural analysis and monitoring the system file activity
Connection-monitor and connection-breaker: a novel approach for prevention and detection of high survivable Ransomwares	The proposed framework considered the first one to detect High Survivable Ransomwares (HSR) through monitoring suspicious connections	The proposed framework can stop only the HSR while the non-HSR can finish taking over the users data	Monitoring suspicious connections
Experimental analysis of Ransomware on Windows and Android platforms: evolution and characterization	The analysis shows that Ransomware can be detected on the Windows platform by continually watching file system activity and registry activity. Moreover, the analysis by Android applications shows that Ransomware can be stopped on the android platform by watching the administration privileges	Small size of Ransomware samples	Monitoring abnormal file systems and registry activity in windows. Monitoring permissions requested
CryptoLock (and drop it): stopping Ransomware attacks on user data	An early warning system developed to detect Ransomware. High rate of true positive. Detects Ransomware through three predefined primary indicators	Cryptodrop cannot ascertain the purpose of change that it investigates	Behavioural analysis
UNVEIL: a large-scale, automated approach to detecting Ransomware	UNVEIL introduced a newly automated, large scale and specific approach to detect Ransomware during the dynamic analysis. UNVEIL could detect a large scale of malware where 13,673 Ransomware files were detected	Ransomware may run at the kernel level using the administration privileges to control some of the hooks that UNVEIL uses to monitor the system files	Behavioural analysis and dynamic analysis

screenshots taken before, during and after executing the malware. Table 1 shows the advantages and disadvantages of the reviewed models. Thus, it seems that once someone becomes a victim, the only way out is to pay the money being asked for. But some victims claimed that they could not recover their data despite paying the amount.

It is only feasible to say that from users point of view, always back up your data into multiple units. Yet, we might lose some very recent versions of data if that happens. Ransomware is spreading quickly on both PCs and smartphones. Enterprises became a crucial target for Ransomware attackers. Thus, in order to ensure the security of the organization, an information security plan should be implemented. Moreover, introducing educational and awareness programs for the employees is also important. Through awareness and training, information security response teams and backup and recovery plans, enterprises can mitigate the risk of Ransomware attacks (Scott and Spaniel, 2016; Savage *et al.*, 2015).

From a research perspective, behaviour based detection seems to be the way to go. This can be done via. detecting any devious execution patterns, especially those that resemble the encryption of files or storage disks. Classification of behaviours from Ransomware datasets is very important towards achieving this goal. Some threats to this approach were mentioned in detail (Kharaz *et al.*, 2016; Marhusin, 2012).

CONCLUSION

The main idea of this study is to look into the current methods and techniques used to analyse and detect the malware and propose a new direction to deal with Ransomware. Both static and dynamic analyses have their own advantages and disadvantages.

The use of dynamic analysis is more desirable against zero-day Ransomware than the static analysis. However, the use of both the signature-based detection and behaviour-based detection techniques are very much possible to get a good result. Right now, there are many new types of malware as mentioned in the study. Ransomware is spreading quickly into computer systems and does great damage in today's cloud based systems. That is why dealing with Ransomware should be an important concern for future researchers.

ACKNOWLEDGMENT

This research is partially funded under The Ministry of Higher Education, Malaysia with grant No: [FRGS/1/2015/ICT01/USIM/02/1].

REFERENCES

Ahmadian, M.M., H.R. Shahriari and S.M. Ghaffarian, 2015. Connection-monitor and connection-breaker: A novel approach for prevention and detection of high survivable Ransomwares. Proceedings of the 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC'15), September 8-10, 2015, IEEE, Rasht, Iran, ISBN:978-1-4673-7609-9, pp: 79-84.

Aman, W., 2014. A framework for analysis and comparison of dynamic malware analysis tools. Intl. J. Netw. Secur. Appl., 6: 63-74.

Bhardwaj, A., V. Avasthi, H. Sastry and G.V.B. Subrahmanyam, 2016. Ransomware digital extortion: A rising new age threat. Indian J. Sci. Technol., 9: 1-5.

Chen, H., D. Dean and D. Wagner, 2004. Model checking one million lines of C code. Proceedings of the 11th Annual Symposium on Network and Distributed System Security (NDSS'04) Vol. 4, February 5-6, 2004, Catamaran Resort Hotel and Spa, San Diego, California, pp: 171-185.

Egele, M., T. Scholte, E. Kirda and C. Kruegel, 2012. A survey on automated dynamic malware-analysis techniques and tools. ACM Comput. Surveys, Vol. 44. 10.1145/2089125.2089126

Feng, H.H., J.T. Giffin, Y. Huang, S. Jha, W. Lee and B.P. Miller, 2004. Formalizing sensitivity in static analysis for intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy, May 9-12, 2004, Berkeley, CA., USA., pp: 194-208.

Gandotra, E., D. Bansal and S. Sofat, 2014. Malware analysis and classification: A survey. J. Inf. Sec., 2014: 1-9.

Gazet, A., 2010. Comparative analysis of various Ransomware virii. J. Comput. Virol., 6: 77-90.

Jacob, G., H. Debar and E. Filiol, 2008. Behavioral detection of malware: From a survey towards an established taxonomy. J. Comput. Virol., 4: 251-266.

Jerlin, M.A. and C. Jayakumar, 2015. A dynamic malware analysis for windows platform-a survey. Indian J. Sci. Technol., 8: 1-5.

Kaur, P. and S. Sharma, 2014. Literature analysis on malware detection. Intl. J. Electron. Electr. Eng., 7: 717-722.

Kharraz, A., W. Robertson, D. Balzarotti, L. Bilge and E. Kirda, 2015. Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In: Detection of Intrusions and Malware and Vulnerability Assessment, Almgren, M., V. Gulisano and F. Maggi (Eds.). Springer, Cham, Switzerland, ISBN:978-3-319-20549-6, pp: 3-24.

Kharraz, A., S. Arshad, C. Mulliner, W.K. Robertson and E. Kirda, 2016. UNVEIL: A large-scale, automated approach to detecting Ransomware. Proceedings of the 25th Symposium on USENIX Security, August 10-12, 2016, USENIX, Austin, Texas, ISBN:978-1-931971-32-4, pp: 757-772.

Kim, D., W. Soh and S. Kim, 2015. Design of quantification model for prevent of CryptoLocker . Indian J. Sci. Technol., 8: 203-207.

Lee, J.K., S.Y. Moon and J.H. Park, 2017. CloudRPS: A cloud analysis based enhanced Ransomware prevention system. J. Supercomputing, 73: 3065-3084.

Ligh, M.W., 2011. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. John Wiley & Sons, Hoboken, New Jersey, USA., Pages: 716.

Marhusin, M.F., 2012. Improving the effectiveness of behaviour-based malware detection. Ph.D Thesis, University of New South Wales, Kensington, New South Wales.

Mathur, K. and S. Hiranwal, 2013. A survey on techniques in detection and analyzing malware executables. Intl. J. Adv. Res. Comput. Sci. Software Eng., 3: 422-428.

Priyadarshi, S., 2011. Metamorphic detection via emulation. Master's Thesis, San Jose State University, San Jose, California, USA.

Savage, K., P. Coogan and H. Lau, 2015. Security response: The evolution of Ransomware. Symantec, Mountain View, California, USA. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-Ransomware.pdf.

Scaife, N., H. Carter, P. Traynor and K.R. Butler, 2016. Cryptolock (and drop it): Stopping Ransomware attacks on user data. Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS'16), June 27-30, 2016, IEEE, Nara, Japan, ISBN:978-1-5090-1484-2, pp: 303-312.

Scott, J. and D. Spaniel, 2016. ICIT Ransomware report. Master Thesis, Institute for Critical Infrastructure Technology, Washington, DC., USA.

Singh, N. and D.S.S. Khurmi, 2015. Malware analysis, clustering and classification: A literature review. Intl. J. Comput. Sci. Technol., 6: 68-72.

Symantec, 2016. ICIT Ransomware report. Symantec, Mountain View, California, USA.

Tobergte, D.R. and S. Curtis, 2013. Improved docking of polypeptides with glide. J. Chem. Inf. Model., 53: 1689-1699.

Woburn, M.A., 2016. Crypto-ransomware attacks rise five-fold to hit over 700,000 users in one year. Kaspersky Lab, Moscow, Russia. https://www.kaspersky.com/about/news/virus/2016/crypto-ransomware-attacks-rise-five-fold-to-hit-718-thousand-users-in-one-year.

Zavarsky, P. and D. Lindskog, 2016. Experimental analysis of Ransomware on windows and android platforms: Evolution and characterization. Procedia Comput. Sci., 94: 465-472.