The Rise of Ransomware

Wira Zanoramy A. Zakaria
MyCERT, Cybersecurity Malaysia, Sapura@MINES, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Malaysia
wira@cybersecurity.my

Mohd Faizal Abdollah, Othman Mohd
Faculty of Information & Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
{faizalabdollah, mothman}@utem.edu.my

Aswami Fadillah Mohd Ariffin
Cybersecurity Responsive Services, Cybersecurity Malaysia, Sapura@MINES, Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Malaysia
aswami@cybersecurity.my

ABSTRACT
Ransomware continues to be one of the most crucial cyber threats and is actively threatening IT users around the world. In recent years, it has become a phenomenon and traumatic threat to individuals, governments and organizations. Ransomwares not only penalized computational operations, it also mercilessly extorts huge amount of money from the victims if the victims want to regain back access to the system and files. As such, the cybercriminals are making millions of profits and keep on spreading new variants of ransomware. This paper discusses about ransomware and some related works in fighting this threat.

CCS Concepts
Security and privacy → Malware and its mitigation

Keywords
Malware; Ransomware; Ransomware detection

1. INTRODUCTION TO MALWARE
Malware attacks is increasing. It is directly and indirectly cause damages to businesses, industries, banking. Malware infections affects labour costs, costs of repairing and cleaning infected systems, loss of productivity, loss of business reputations [1]. Some examples of the negative effects are information leakage, incur costs to recover from malware outbreak, system downtime leading to potential lost in revenue, system damages and so on. Computer network exploitation and breaches consumes resources and denial of service (DoS). These are some examples of effects towards IT systems and critical IT infrastructures if the malware spread is not stopped within the shortest timeframe [2].

2. WHAT IS MALWARE?
The term malware is a combination of the word "malicious" and "software". It is one of major threat lurking in the Internet today. A piece of software created with a harmful intention towards victims' computer, network and data. It is intended to illegally gain access to IT systems, network resources and data without the consent of the owner. Bring damage to IT operations and stealing confidential information. Types of malware includes: virus, worm, trojan, rootkit, botnet, spyware, adware, ransomware [3].

ICSEB 2017, December 28–30, 2017, Hong Kong, Hong Kong

ACM ISBN 978-1-4503-5488-2/17/12…$15.00
DOI: https://doi.org/10.1145/3178212.3178224

Malware is constantly growing in numbers and keeps on evolving, becoming more sophisticated in attacking computing platforms and mobile devices [3]. Malware are designed with mutation capabilities such as polymorphism and metamorphism contribute to the exponential growth of malware variants lurking on the Internet [4]. Polymorphic malware is the malware that has the capability to encrypt and decrypt the code in runtime. Meanwhile, metamorphic malware is the malware can do modification to the code to avoid detection [5]. As time goes by, new malwares are more targeted, persistent and unknown. Meanwhile, the advanced malwares are targeted, unknown, zero-day and stealthy compares to traditional malwares [3]. Nowadays, there are so many malwares than we can possibly analyze.

3. MALWARE CATEGORIES
Virus is a type of malware that spreads to other computers by replicating and attaching itself to other files, executable programs or even a USB flashdrive [5], [6]. Viruses do not have the capability to execute independently. It waits for an action trigger to execute and spread.

Rootkits a collection of tools that is used by the attacker to hide its capability to maintain root access of the computing platform without the system owner's consent [6 - 9]. Besides that, rootkit also can hide its presence and avoid being detected [10]. Unlike viruses, worms self-duplicate itself, execute and spread to other computing platforms and networks without attaching itself to a host file [11].

Trojan horse is a rogue software that looks like a legitimate software, but it is embedded with malicious instructions to bring harm to the infected computing platform. Once infected, the impact of a trojan attack is severe because the attack is originating from the inside. Examples of trojans horses are Backoffice, Netbus and Nuker [5].

Ransomware is a type of malware that is capable to lock and encrypt victim's computer system and files. For the victim to gain back the system or data access, the victim need to pay an amount of ransom, usually in the form of crypto-currency and bitcoin [12]. This threat is not just limited to desktop computing platforms, it is also affecting mobile and Internet of Things (IoT) devices [13].

The remaining sections of this paper is organized as follow. Section 2 discussed generally about malware. Section 3 discussed the categories of malware. Section 4 discussed about some background on ransomware. Section 5 explained about the ransomware infection vectors. Section 6 discussed about the categories of ransomware. Section 7 discussed about the phases of

a ransomware attack. Section 8 shared about the related works done by other researchers in ransomware detection, classification, recovery and prevention. Finally, Section 9 concludes this paper.

4. RANSOMWARE

The term "ransomware" is created from the word ransom and malware [16]. Ransomware attack is not a new concept because it has been around years ago since 1989 [17], [18]. The first ransomware was released under the name of AIDS Trojan [18]–[20]. Furthermore, according to Symantec, the earliest trend of modern ransomware had started with Trojan.Gpcoder in 2005 [7].

Ransomware is currently gaining popularity in recent years. It is utilized by cybercriminals to gain fame and profit. This kind of malware is also falls under the category of crimeware [14]. It is class of malicious software created to facilitate in illegal online activity and cyber extortions. It is also reported that it is almost impossible to reverse the damage done by a ransomware. While in other literature, ransomware is categorized as scareware, in which it is a group of malwares that tricks and make full use of scare tactics towards the victim by intentionally displaying fake warning notes purportedly representing a law enforcement agency claiming that the victim had downloaded an illegal content [15].

It is very clear that, the evil cybercriminals had diversified their effort in making money online. Besides than advertising fake products and services on online retail portals and luring users into using fake mobile banking application, cybercriminals are currently utilizing ransomware to extort money from victims. The creation of e-currency such as Bitcoin is one the reason of the increasing cases of ransomware attacks [12], [18]. Nowadays, ransomwares had become the chosen profit-making weapon for the cybercriminals [21].

Figure 1. Ransom note used by Wannacry ransomware (source: source: www.mycert.org.my).

In recent years, ransomware has become a serious threat to IT users and it is becoming worsen year by year [16]. As reported by Symantec, ransomware has dominated the global threat landscape in 2016 with the increase rate of 267% [7]. For example, one ransomware named as CryptoWall 3.0 is reported as the most profitable ransomware family. The calculated damage that it has done around the globe is USD350 million [17]. Meanwhile, according to Kaspersky's report in 2016, individuals and businesses were being attacked by ransomware at an average of every 40 seconds [22]. Various entities had been infected by ransomware – individuals, universities, government agencies, financial institutions, healthcare centers and corporations [12]. Figure 1 and 2 shows some example of ransom note created by the ransomware on any infected platform. While other type of malware prefers to stay low profile and avoid being detected, ransomwares purposely want the infection to be known by the victim. This is as a part of the extortion process towards the victim.

Figure 2. Ransom note used by Cryptolocker ransomware (source: blog.malwarebytes.com).

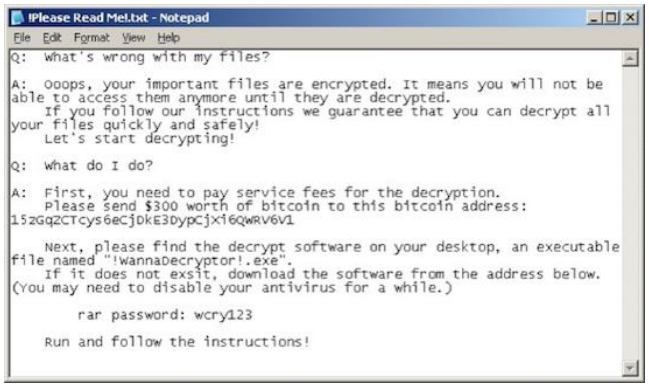

Figure 3. A text file created by Wannacry ransomware on infected desktop computer (source: www.mycert.org.my).

By using several types of attacking vectors such as social engineering, spam emails, botnet distribution, evading detections, self-propagating and attacking towards computing platform, ransomware is a dangerous threat to organizations especially the critical sectors [17], [18]. After it manage to land on the victim's computing platform, it will lock the files, folder or even the whole computer [17]. The victim is unable to access the files or system until an amount of requested ransom is paid to the attacker.

5. INFECTION VECTORS

Cyber criminals used many ways to spread ransomware. It involves multiple different elements. For example, an attack could begin with a spam email that contains hyperlinks that will redirect the victims to a malicious website which contains exploits codes that make use of the system's vulnerabilities to download the ransomware. Described below are two methods on spreading ransomwares:

- Emails – ransomware that is spread through emails can be in the form of downloaded suspicious attachment or by clicking malicious links within the email.
- Drive-by download – this is a slick way to infect a victim's PC. Victims are lured to a compromised website and the malicious code hidden on the website is executed. This technique are used by cyber criminals to run exploit kits towards vulnerable systems.

6. RANSOMWARE CATEGORIES

Basically, there are two types of ransomware - locker and crypto [18], [21]. Another literature reported that there is another type of ransomware, which is a combination of locker and crypto ransomware. It is called as hybrid ransomware [13].

6.1 Locker

Locker ransomware locks the device and denies user access to the device and system functionalities, without modifying the files stored on it [7], [13], [21]. In case of IoT devices, a locker ransomware may modify the functionality of the device such as disabling the user interfaces, deactivate the built-in sensors and activating a denial of service (DoS) attack to disrupt the device performance [13]. Example of this kind of ransomware are AIDS trojan, Petya, GoldenEye, LockerPin and Cryptowall [13], [21].

6.2 Crypto

Crypto ransomware encrypts all or selected files and folders on the infected computing platform. In other words, it locks the user from accessing the data [7]. In most cases crypto ransomwares make use of the public-private key relationship – data is encrypted using public key and private key is used to decrypt the data [13]. After it infects the system, it disables user's access to files by encrypting all the targeted files. Later, the victim will be prompted with a threatening ransom note that contains a message about what has happened to the files and instructions on how to make the ransom payment to obtain the decryption key [21], [23]. In the note, the victim is told that by paying the ransom, there will be possibility to regain back the access to all the encrypted files. To ensure that the authorities cannot trace the transactions of ransom, usually the required payment to be made is in the form of Bitcoin [13], [15], [18], [22], [24]. Cryptolocker, CryptoDefense, KeRanger, ZCryptor, Crysis, zCrypt and WannaCry are some examples of crypto ransomware [21]. Figure 4 below shows an example of files that got encrypted by a ransomware on a Windows platform.

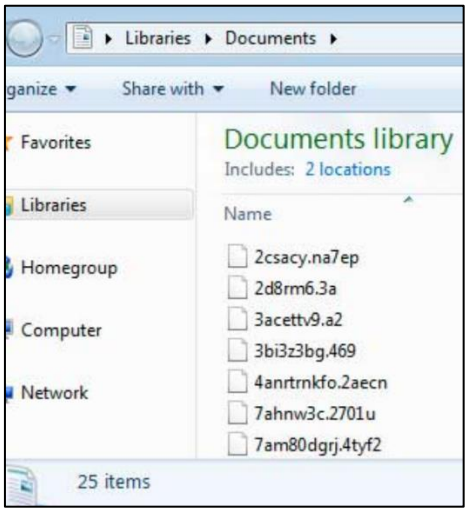

Figure 4. Screenshot showing a list of encrypted files on infected Windows platform (source: www.tekiegeek.com).

6.3 Hybrid

Hybrid ransomware contains both attack mechanisms: it locks the system from user's access and it encrypts the targeted data. This is more dangerous because the system and data are compromised at the same time. As for IoT devices, hybrid ransomware has the potential to compromised both front-end and back-end of the devices. Curve-Tor-Bitcoin (CTB) Locker is one example of hybrid ransomware [13].

7. PHASES OF A RANSOMWARE ATTACK

Traditional malwares tend to hide itself from detection. So, it can covertly cause harm to the targeted platform with the owner's consent. Some of the reasons to remain stealth are to silently collect the sensitive data, banking credentials, confidential documents, deleting system files or even capturing keystrokes [17]. In contrast to this, ransomwares exhibit different behavior. It purposely showing up its presence on the infected computing platform by locking system, encrypting files and prompting a ransom note.

The main motive here is to tell the victim about the infection, access to files or system has been blocked and the amount of the ransom that need to be paid to revert the access. This is to inform the victim that he is being infected by a ransomware [17]. There are many variants of ransomware and they operates in different ways, from locking computer systems to encrypting all its files [17], [21]. According to [24], a ransomware attack is divided into five phases:

a) exploitation and infection

b) delivery and execution

c) backup spoliation

d) file encryption

e) user notification and clean up

8. RELATED WORKS

Based on our literature survey, we found out that there are a few areas of interest that is related to this kind of threat. The domains are ransomware detection [17, 24], classification [15, 18, 20, 23, 25], recovery and prevention [24]. Figure 4 shows a tree chart representing all the main active areas of research interest in ransomware.

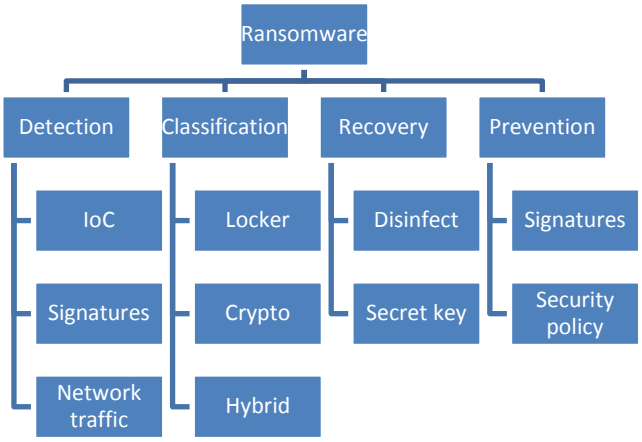

Figure 4. Shows the important areas of research in ransomware domain.

8.1 Detection

Early detection can minimize the impact of a ransomware outbreak. Organizations can implement good signatures and indicators of compromise (IoCs) into their intrusion detection systems (IDS) or any other network devices. Threat intelligence feeds can be used to mine for important threat information so that this can be used to identify, block or at least alert regarding the presence of ransomware activity within the network [18, 24]. Another way of detecting ransomware is by analyzing their communication characters in the networks [25].

8.2 Classification

There are thousands of ransomwares being released from time to time. Though some of the ransomware is a variant of an earlier version but with some modifications. It is very hard for malware analyst and security practitioners to cope up with identifying the ransomware and which action to take to reduce the response time. Classification is very much needed to understand which family does the ransomware falls in. different ransomware family have different way of handling it.

8.3 Recovery and Prevention

The most crucial part here is to get back the clean version of the data from backup and to get back to operational as soon as possible. By knowing which infection vectors that was used by the ransomware can help organizations to improve their perimeter defense and detection mechanisms [24]. Either the infection originated from phishing emails or web-based attack kit, both has different way to prevent it.

9. CONCLUSION

Ransomware is a dangerous threat to individuals, organizations, businesses and governments. Due to this, a lot of work need to be done in detecting this kind of threat from it manage to bring down critical operations. This paper discussed an overview of the ransomware threat and listed some of the related works done by security researchers in detection, classification and prevention of ransomware.

10. REFERENCES

[1] W. Liu and S. Zhong, “Web malware spread modelling and optimal control strategies,” Sci. Rep., vol. 7, no. February, p. 42308, 2017.

[2] A. Leon, “Impacts of Malicious Cyber by,” no. August, 2015.

[3] E. Gandotra, D. Bansal, and S. Sofat, “Malware Analysis and Classification: A Survey,” J. Inf. Secur., vol. 5, no. 2, pp. 56–64, 2014.

[4] M. Ahmadi, D. Ulyanov, S. Semenov, M. Trofimov, and G. Giacinto, “Novel Feature Extraction, Selection and Fusion for Effective Malware Family Classification,” Proc. Sixth ACM Conf. Data Appl. Secur. Priv. - CODASPY ’16, pp. 183–194, 2016.

[5] S. Chakraborty, “A Comparison study of Computer Virus and Detection Techniques,” vol. 2, no. 1, pp. 236–240, 2017.

[6] J. Kaur and S. Sharma, “Study of Malware Based On Pattern Matching Techniques,” vol. 3, no. 2, pp. 1178–1180, 2015.

[7] Symantec, “Internet Security Threat Report,” Symantec, vol. 21, no. 2, pp. 1–3, 2016.

[8] M. F. A. Razak, N. B. Anuar, R. Salleh, and A. Firdaus, “The rise of ‘malware’: Bibliometric analysis of malware study,” J. Netw. Comput. Appl., vol. 75, pp. 58–76, 2016.

[9] S. Romana, A. K. Jha, H. Pareek, and P. R. L. Eswari, “Evaluation of open source anti-rootkit tools,” WATeR 2013 - Proc. 2013 IEEE Work. Anti-Malware Test. Res., no. July 2015, 2013.

[10] S. Pai, F. Di Troia, C. A. Visaggio, T. H. Austin, and M. Stamp, “Clustering for malware classification,” J. Comput. Virol. Hacking Tech., vol. 13, no. 2, pp. 95–107, 2017.

[11] D. Of, P. In, and C. Science, “Evaluation of Hidden Markov Model for Malware Behavioral,” no. October 2016.

[12] J. Voas and I. Fellow, “Do Crypto-,” pp. 11–15, 2017.

[13] I. Yaqoob et al., “The rise of ransomware and emerging security challenges in the Internet of Things,” Comput. Networks, vol. 0, pp. 1–15, 2017.

[14] A. Zimba, Z. Wang, and H. Chen, “Reasoning crypto ransomware infection vectors with Bayesian networks,” 2017 IEEE Int. Conf. Intell. Secur. Informatics, pp. 149–151, 2017.

[15] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, “Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection,” 2016.

[16] M. M. Ahmadian, H. R. Shahriari, and S. M. Ghaffarian, “Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares,” 12th Int. ISC Conf. Inf. Secur. Cryptology, Isc. 2015, pp. 79–84, 2016.

[17] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, C. Mulliner, and W. Robertson, “UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware This paper is included in the Proceedings of the,” 2016.

[18] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, and R. Khayami, “Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence,” IEEE Trans. Emerg. Top. Comput., vol. 6750, no. c, pp. 1–1, 2017.

[19] K. Savage, P. Coogan, and H. Lau, “The Evolution of Ransomware,” Secur. Response, p. 57, 2015.

[20] A. Gazet, “Comparative analysis of various ransomware virii,” J. Comput. Virol., vol. 6, no. 1, pp. 77–90, 2010.

[21] P. B. Pathak and Y. M. Nanded, “A Dangerous Trend of Cybercrime: Ransomware Growing Challenge,” Int. J. Adv. Res. Comput. Eng. Technol., vol. 5, no. 2, pp. 371–373, 2016.

[22] Z. A. Genç G. Lenzini and P. Y. A. Ryan, “The Cipher, the Random and the Ransom: A Survey on Current and Future Ransomware.”

[23] A. Continella et al., “ShieldFS: A Self-healing , Ransomware-aware Filesystem,” 2016.

[24] R. Brewer, “Ransomware attacks: detection, prevention and cure,” Netw. Secur., vol. 2016, no. 9, pp. 5–9, 2016.

[25] Cabaj, K., Gregorczyk, M., & Mazurczyk, W. (2015). Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics. Retrieved from https://arxiv.org/ftp/arxiv/papers/1611/1611.08294.pd