Borneo International Journal eISSN 2636-9826; Vol. 4 (1); 2021; 12-18
Published by *Majmuah Enterprise*
www.majmuah.com

Survey on Technique to Prevent Ransomware Attack

KU AMIRIYAH KU OTHMAN , MOHAMAD FADLI ZOLKIPLI
School of computing, Universiti Utara Malaysia (UUM), Sisiran Sintok 1, Sintok, 06010, Changlun, Kedah.
Email: ku_amiriyah_ku@soc.uum.edu.my, m.fadli.zolkipli@uum.edu.my

Received: May 04, 2021
Accepted: May 07, 2021
Online Published: May 11, 2021

Abstract

As the number usage of technology has increased these days. The number of ransomware attacks have also significantly increased throughout the years. Ransomware is an attack made on the device and the victim data or file. It will lock until the victim pays for it. This article is constructed to survey on the technique to prevent the ransomware attack. This article also covers the history and type of ransomware attack. This research is done by reviewing the related articles and categorizing them in a table.

Keywords: ransomware, attack, prevent, crypto, locker

1. Introduction

Ransomware comes from a combination of two words which is ransom and malware (Zakaria et al., 2017). While the number of technology usage among users has increased it means that the number of the cybercrime will also increase (Lee et al., 2016). Ransomware attack is a malicious code that will attack or infect the system or machine, where it will not allow the user to access their device or their data until they pay for it. It is usually asked the victims to pay the ransom using bitcoin. This ransomware basically has two common types which is Crypto and Locker (Richardson, 2017). The rest of the ransomware attack is discussed below.

In 2020, it is recorded by Statista (2020) that approximately 304 million of the ransomware attacks. It is the second highest after the ransomware attack in 2016 which is 638 million attacks. Many large and small organizations have been attacked by this threat. Majority the industries that are getting attacked by the ransomware recorded by PurpleSec (2020) are the government. And the second highest was recorded are form manufacturing. These two big industries are reasonable why they are being targeted by the attacker because of the value of money they will get after the attack. Even so, it is recorded by PurpleSec (2020) that 85% small businesses are getting attacked. This is because the small business cannot afford to set up the cybersecurity to their organization that makes them being easily targeted by this ransomware attack.

Therefore, this survey was conducted to identify the technique to prevent the ransomware attack. The results were obtained through reviewing related articles which were mainly obtained through surfing the Internet. The article is divided into several sections. Section 2 provides information about the history or background of the ransomware attack. Section 3 discussed the type of ransomware attack. Technique to prevent the ransomware attack is presented in Section 4. Finally, followed by section 5 is conclusion and reference.

2. History of ransomware attack

Ransomware was born in 1989 and to be known as PC Cyborg or other name as Trojan (Herrera et al., 2016). The first ransomware virus was created by Joseph L. Popp (Richardson, 2017). But the attack was not that strong like these days. This is because, during that time, there is a limitless use of the internet. The code was distributed using the floppy disk to attack the WHO international conference on AIDS. Until 2005, the modern ransomware has been created because of the existence of IoT at that time (Humayun et al., 2018). During that time, the latest of the ransomware virus has been created and it is called GPCoder. This threat has been spread using the email, once victims open the mail it will encrypt the data inside the machine (Richardson, 2017).

In 2006, a new ransomware virus called Trojan Cryzip evolved. Different from the first ransomware virus, this type of attack also locks the victim password. And in the same year, the Trojan Cryzip has mitigated and the new one was created called Trojan archiveus. Each year, new ransomware have been created. In 2007, locker ransomware. 2008, new mitigation of GPCoder has evolve called HPCode,AK, (Humayun et al., 2018). While, in 2010 Winlock one of the ransomware attack has appeared. Instead lock the victim's data or file, this ransomware lock the victim's device by

displaying a blurry image. Fast forward, in 2013 the most famous and the main of the ransomware attack was born called CryptoLocker (Richardson, 2017).

In 2014, it is reported that there were 500, 000 victims were attacked by this CryptoLocker (Richardson, 2017). This type of attack will outspread to the victims through the attachment inside the email (Humayun et al., 2018). In the same year, a new variation of Locker appeared called CTB Locker (Pazik, 2017). Throughout 2015 until 2017, more ransomware attacks have emerged. For instance, Cryptowall 3.0 CryptoWall 4.0, TeslaCrypt, Locky, Mamba, Petya (Humayun et al., 2018). This can be a proof that is related to the statistics that are mentioned in the introduction section, where there are 638 million attacks recorded during that year, (Statista, 2020).

3. Type of ransomware attack

Type of ransomware attack according to each article were identified and demonstrated in Table 1.

Table 1: Sort of the Ransomware Attack

Type of ransomware attack	Reference
1. PC Cyborg 2. Scareware 3. CryptoLocker 4. Locky 5. CryptoWall 6. KeyRanger 7. Samam 8. TeslaCrypt 9. others	(Brewer, 2016)
1. 1.GrandCrab 2. Alphacrypt 3. Jigsaw 4. Locky 5. Bat rabbit 6. Petya 7. WannaCry 8. Others	(Herrera et al., 2016)
1. Cypto 2. Locker	(Humayun et al., 2018)
Common ransomware 1. Cypto ransomware 2. Locker ransomware	(Richardson et al., 2017)
1. Non-Cryptogrphic ransomware or NCR 2. Cryptographic ransomware of CGR	(Gonzalez et al., 2017)
1. Locker ransomware 2. Crypto ransomware	(Vinayakumar et al., 2020)
1. Cryptowall 2. CryptoLocker 3. CTB-Locker 4. TeslaCrypt 5. Lock generate the fill	(Lee et al., 2016)
1. Lock Screen Ransomware 2. Encryption ransomware 3. Master Boot Record 4. Ransomware encrypting web servers 5. Android mobile device web servers 6. Iot ransomware	(Sen et al., 2020)
1. Locky 2. Tesla Crypt 3. Crypto ransomware (data	(Mishra et al., 2017)

locker) 4. Locker ransomware (computer) 5. Crypto wall	
1. Locker ransomware attacks 2. Crypto ransomware attacks	(Sajjan et al., 2016)

There are many types of ransomware attacks. But the two common or main ransomware attacks are the Crypto and Locker. Vinayakumar et al (2020) said that Crypto are the attacks that encrypt the user file using the function of the cryptography which means users can still use their system or device but only cannot access their file and folders. While Locker means that, the ransomware attacks the user's device. Where users cannot access their device until they make payment to the attacker. Richardson et al (2017) said it is not worth paying the attacker if it is a Locker ransomware attack because the data can easily be recovered. This is because the Locker attacks only lock the device but it did not touch the file inside. These two main attacks will start to attack users by sending the email attachment, and it will start active when the user opens the mail (Humayun et al., 2018). This statement can also be supported by Sajjan et al (2016), he said that this attack can be easily removed from the system as this type of attack still keeps the file and the data is untouched.

Furthermore, other than these two main types of ransomware attack which is Crypto and Locker. There are many more examples of ransomware attacks. Based on an article written by Brewer (2016), he discusses the example of ransomware attack which is PC Cyborg, CryptoLocker, CryptoWall, SamSam TeslaCrypt. Herrera et al (2016) said that new families of ransomware attacks were emerging. For instance, GrandCrab, Alphacrpyt, Jigsaw, Bat Rabbit Petya etc. He also discussed the example of the famous ransomware attack which is EternalBlue and WannaCry. This type of attack can infect the computer by spreading the malware.

Besides, Non-Cryptographic or NCR and the Cryptographic Ransomware or CGR are discovered inside the article discussed by Gonzales et al (2017). The NCR did not use the encryption therefore it is weak and is not worth the ransom. While the CGR uses encryption, it will encrypt the user's files and will decrypt until it is paid. CryptoLocker, CTB-Locker, TeslaCrypt, Lock generate the fill were discovered in an article written by Lee et al (2016). Mishra (2017) discussed that type of ransomware attack is Locky, Teslacrypt, Crypto ransomware or data lock, locker ransomware or computer lock and lastly the Cryptowall. Hence, the ransomware attacks are divided into two types which is the lock screen and also the encryption ransomware. Saurabh et al (2020) also added other examples of ransomware attack which is Master boot record, device android, server encrypted and lastly the IoT ransomware. Therefore, it is concluded that the two main types of the ransomware attack that were discovered through the article review are the crypto and the Locker. In figure 1 below are a few examples of recent ransomware attacks. HabanaLabs was attacked and their data related to the business document was leaked by the attacker (Lawrence, 2020).

```
/* SPDX-License-Identifier:     GPL-2.0+
 *
 * Copyright (C) 2017-2020 HabanaLabs Ltd.
 * All Rights Reserved.
 *
 */

#ifndef ZEPHYR_INCLUDE_WATCHDOG_H_
#define ZEPHYR_INCLUDE_WATCHDOG_H_

#define WDT_DEV_NAME         DT_LABEL(DT_ALIAS(watchdog0))
#define WD_TIMEOUT       5000U    /* 5 sec */
#define STACK_SIZE       1024
#define WD_THREAD_PRIORITY  3

int hl_watchdog_init(void);
void hl_feed_wd(void *p1, void *p2, void *p3);

#endif /* ZEPHYR_INCLUDE_WATCHDOG_H_ */
```

Figure 1: Image above shows the leaked source code of the HabanaLabs (Lawrence, 2020)

4. Technique to prevent the ransomware attack

The ways to prevent the ransomware attack according to each article was identified and demonstrated in Table 2

Table 1: Sort of the Ransomware Attack

Type of ransomware attack	Reference
1. Preparation 2. Detection 3. Containment 4. Eradication 5. Recovery	(Brewer, 2016)
Four recommendations to prevent being attacked by ransomware: 1. Backup all data 2. Avoid the email attachment 3. Update the security of the software 4. Turn off the machine if infected	(Herrera et al., 2016)
1. Limited the privileged or access 2. Backup frequently 3. Disable the micro 4. Software policies restriction 5. Awareness among the employee 6. Frequently update the security of software	(Humayun et al., 2018)
1. Back up data 2. Avoid attachment or link from email 3. Patch and block 4. Drop and roll Best way for the company or organizations: 1. Understand the risk of attacks 2. Adequate policies 3. Institute best practice among users	(Richardson et al., 2017)
1. Monitor the file system 2. Use decoy files	(Gonzalez et al., 2017)
1. Update software 2. Verify the back-up 3. Train the employee 4. Use anti-virus 5. Network sandboxing	(Malecki, 2019)
1. Email filtering 2. Properly configure the firewall 3. Use browser protection 4. Backup data or files 5. Immediately delete suspicious activity 6. Scan the downloaded software	(Aurangzeb et al., 2019)
1. Update Pc 2. Backup PC and data 3. Sites security check 4. Setting the system security 5. Setting as read only folder	(Vinayakumar et al., 2017)
1. Categorize the characteristic of ransomware 2. Access control 3. Recovery 4. Trap the attacker	(Alshaikh et al., 2020)
1. Use honeypot technique 2. Heldroid 3. Cryptolock 4. Sand-box	(Surati et al., 2017)
1. Install license anti-virus 2. Backup data	(Mishra, 2017)

3. Download things from trusted sources 4. Scan email attachment 5. Update the software 6. Browse protection 7. Use a sand-box 8. Use HTTPS 9. Others	
1. Firewall 2. Proxy servers and web filters 3. Filters the spam 4. Segment the network 5. Do patching 6. Permit file	(Pazik, 2017)
1. Details of the technical 2. Spread the awareness of ransomware attacks	(Han et al., 2018)

Preventing the attack of ransomware at earlier stages are better than never. This is to avoid being the victims of the attacker, also avoid paying the ransomware attacker. Therefore Brewer (2016) discussed in his article that there are five steps or ways to prevent this ransomware attack. Firstly, do preparation by knowing the vulnerabilities in our system. For instance, the vulnerability is not using a firewall. If the vulnerabilities are eliminated the malware will not have the way to enter inside the system. Secondly, Brewer (2016) said is detection. Use detection tools like screening to scan the email attachment. Third is do the containment, containment means taking action of the attack to be under control. Fourth is eradication, after the malicious is being detected and under containment. It is better to destroy it by replacing the machine or system. Lastly is recovery, recover from the attack by knowing the weaknesses in the system this is to avoid being attacked in the future.

Herrera et al (2016) recommended four ways to prevent the attack. Which is to backup for the files or data inside our system, avoid the email with a link or attachment, regularly update the software and lastly turn off the machine if it's infected. This statement can be supported by Humayun et al (2018). He discussed that to prevent the ransomware attack is to frequently update the software, limit the privilege or the access inside the system, frequently backup, train the employee about the ransomware attack etc. Moreover, Richardson et al (2017) discussed in their study about the ways to prevent the ransomware attack. Which is, do back up. The needs of doing the backup for data or files is to avoid paying the attacker in order to get back the data. Next, avoid opening an email that contains a link and attachment or it is called a phishing attack that is used to spread the ransomware. Patching, drop and roll are the other techniques that were also found in that article. Hence, Richardson et al (2017) also suggested the way to prevent ransomware for organization. For instance, understanding the risk of the ransomware attack do to their organization, enhance the policies of adequate, and lastly is do the awareness among the employee inside the organization.

Likewise, Gonzalez and Hayanieh (2017) suggested that monitor the file system and use decoy files. By doing the monitoring, the suspicious activity can be detected and this can prevent the ransomware attack. A study conducted by Malecki (2019) suggested that keep updating the software inside the machine and if it too olds to be updated, demolish it. Do educate the employee about the attack as the employer needs to bear in mind that not all his or her employees are good in tech-savvy to understand the malware things. Apart from that, keep updating the software, if its organization increases restrictions to the admin account, use antivirus as an endpoint protection.

On the other hand, Lee et al (2017) suggested to prevent the ransomware attack is to keep the PC update, backup the server data, use security for the sites or web pages, setting the security of the system and lastly set up a setting to read-only folder. While Alshaikh et al (2020) suggested in their study to categorize the characteristics of the ransomware, use access control or policy, recover after being infected by the ransomware and lastly trap the attacker. Different from others' suggestions, Surati & Prajapati (2017) suggested using Honeypot, Heldroid, Cryptolocker and Sand-box techniques to prevent the ransomware attack. Honeypots are being used by the network admin to detect suspicious access inside the system, heldroid use to detect the ransomware correctly, cryptolocker use to prevent the process of ransomware from mitigate inside the system and lastly sand-box is used for a program that runs separately.

Instead of using tools and specific techniques to prevent the ransomware attack, it is discovered that Misha (2017) suggested a way that everyone can easily understand and use it. As a proof, he discussed installing the antivirus that has a license, back up the data, use trusted sources to download the file or data, scan the email attachment before downloading it, frequently update the system software, use protection to the browser, surf the sites that have HTTPS etc. Pazik (2017) found that to prevent the ransomware attack is to use the firewall, firewalls help to track the

suspicious threat before it enters into the system. Next, use proxy servers, filtering spams, do segmentation of the network, do patching and lastly setting the file permissions. Han et al (2018) suggested using extension to prevent the ransomware attack. The extension functions to filter and detect the sites that the users surfing is secure or not. In addition, Han et al (2018) suggested spreading awareness of the ransomware attack in order to prevent it. With the high of awareness, the chance to get attacked by the ransomware attack can be decreased.

5. Conclusions

Ransomware attacks have emerged even before the Internet is not that powerful yet. As discussed above, we can see that there are many types of ransomware that mitigate every year. We come to a conclusion that there are many techniques to prevent from being one of the ransomware attacks. Even though the ransomware attack seems threatening, we could prevent it by following the technique mentioned above. It is better to prevent then recover after being infected. Moreover, in hope that this article will help to close the gap related to the topic.

Acknowledgments

The authors would like to thank all School of Computing members who were involved in this study. This study was conducted for the purpose of the System and Network Security Research Project. This work was supported by the Ministry of Higher Education Malaysia and Universiti Utara Malaysia.

References

Alshaikh, H., Ramadan, N., & Hefny, H. A. Ransomware Prevention and Mitigation Techniques. *International Journal of Computer Applications*, *975*, 8887.

Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: a survey and trends. *Journal of Information Assurance & Security*, *6*(2), 48-58.

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*, *2016*(9), 5-9.

Gonzalez, D., & Hayajneh, T. (2017, October). Detection and prevention of crypto-ransomware. In *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)* (pp. 472-478). IEEE.

Han, J. W., Hoe, O. J., Wing, J. S., & Brohi, S. N. (2017, December). A conceptual security approach with awareness strategy and implementation policy to eliminate ransomware. In *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence* (pp. 222-226).

Herrera Silva, J. A., Barona López, L. I., Valdivieso Caraguay, Á. L., & Hernández-Álvarez, M. (2019). *Remote Sensing*, *11*(10), 1168.

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2020. *Egyptian Informatics Journal*.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.

Lee, J. K., Moon, S. Y., & Park, J. H. (2017). CloudRPS: a cloud analysis based enhanced ransomware prevention system. *The Journal of Supercomputing*, *73*(7), 3065-3084.

Lawrence, A. (202). Intel's Habana Labs hacked by Pay2Key ransomware, data stolen. Retrieved on May, 3, 2021. https://www.bleepingcomputer.com/news/security/intels-habana-labs-hacked-by-pay2key-ransomware-data-stolen/

Malecki, F. (2019). Best practices for preventing and recovering from a ransomware attack. *Computer Fraud & Security*, *2019*(3), 8-10.

Mishra, R. Strategies: To Defeat Ransomware Attacks.

Pazik, E. (2017). *Ransomware: Attack Vectors, Mitigation and Recovery* (Doctoral dissertation, Utica College).

PurpleSec (2020). T**he Growing Threat Of Ransomware. Retrieved on April, 22, 2021.** https://purplesec.us/resources/cyber-security-statistics/ransomware/#:~:text=81%25%20of%20cyber%20security%20experts,social%20actions%2C%20such%20as%20phishing.&text=Ransomware%20attacks%20increased%2041%25%20in,lost%20access%20to%20their%20files**.**

Sajjan, R. S., & Ghorpade, V. R. (2017, March). Ransomware attacks: Radical menace for cloud computing. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 1640-1646). IEEE

Sen, S.K, Chourey. N. A Study of Ransomware Detection and Prevention at Organizations. *International Research Journal of Engineering and Technology (IRJET) 2*001-2008

Surati, S. B., & Prajapati, G. I. (2017). A Review on Ransomware Detection & Prevention. *International Journal of Research and Scientific Innovation*, *4*(9), 2321-2705.

Statista (2020) Annual number of ransomware attacks worldwide from 2014 to 2020. Retrieved on April, 22, 2021. https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

Vinayakumar, R., Soman, K. P., Velan, K. S., & Ganorkar, S. (2017, September). Evaluating shallow and deep networks for ransomware detection and classification. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 259-265). IEEE.

Zakaria, W. Z. A., Abdollah, M. F., Mohd, O., & Ariffin, A. F. M. (2017, December). The rise of ransomware. In *Proceedings of the 2017 International Conference on Software and e-Business* (pp. 66-70).

Zakaria, W. Z., Abdollah, M. F., & Ariffin, A. M. On Ransomware Detection. In *Proceedings of the Seventh International Conference on Informatics and Applications (ICIA2018)* (pp. 12-17).