DETECTION AND MITIGATION OF VIRUS RANSOMWARE

Herny Ramadhani bt Mohd Husny
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
herny@unikl.edu.my

Mohamad Syafiq Bin Md Yussof
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
Syafiqyussof60@gmail.com

Norhaiza Ya bt Abdullah
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
norhaizaya@unikl.edu.my

Wan Hazimah bt Wan Ismail
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
Kuala Lumpur, Malaysia
wanhazimah@unikl.edu.my

***Abstract* -In this era of globalization, ransomware is not something strange. It is a necessity to know about the dangers of this ransomware virus. Ransomware is a form of malware that encrypts files on the computer of a victim and demands payment for restoring the encrypted files. It has become a very serious cyber threat nowadays. The basic idea of ransomware was presented in the form of a cryptovirus in 1995. However, it was considered as merely a conceptual topic since then for over a decade. In 2017, ransomware has become a reality, with several famous cases of ransomware having compromised important computer systems worldwide. The objectives of this project is to investigate the ransomware attack, how to secure the user data from being infected by the virus and to develop software that can detect and mitigate the ransomware virus. This project helps to secure users' data from being infected by the ransomware. At the same time, this software also has functionality to mitigate the suspicious process that have been assumed as a ransomware virus. The software will be tested to ensure that the attacks can be prevented by the software.**

I. INTRODUCTION

The internet plays a prominent role in carrying out daily activities in today's world. As the internet is growing rapidly, the attacks on the internet grow. These attacks have a purpose of either to steal information and misuse the stolen information or to simply disrupt the regular day to day activities [1]. A large company or even an individual that relies heavily on the network may or will face risks and require to establish strategies for mitigation. There are various types of malware that exist and each malware has a purpose. One such category of malware is Ransomwares. The first ever ransomware attack is dated in 1989. It was called AIDS Trojan-PC Cyborg. One probable reason of the ransomwares not being famous back then could be that Internet was not made available to the public in 1989. Ransomwares deny the user access to the system or files and demand ransom for the release of hostage system or files. This ransom is mostly in Bitcoins currency unless otherwise specified by the attackers. The recent cyber-attack in May 2017, which was carried by WannaCry malware, revealed that ransomwares have developed over the decade and it does not use the conventional methods of propagation anymore. The detailed summary of attacks is discussed in [2].

Countermeasures for ransomware have a similarity to current countermeasures for malware thus far. General anti-malware program is one example that use a black list that of known malware characteristics (i.e. signatures). Therefore, to distinguish the unique ransomware signatures, current solution is the ransomware activity will be observed and ransomware codes will be analyzed on the user's device by trust party. Such a trust party then distributes the analyzed ransomware information to users so that they can both block ransomware distribution roots and detect or prevent the execution of ransomware based on the distributed information [3].

Ransomware samples from victims normally received by such trust parties that will be sent by victims. This suggests that certain users are inevitably the victims of new or variant ransomware. Because of traditional antivirus software is unable to identify new types of malware fast enough, it is important to discover when ransomware is starting to trigger and it needs to be blocked before further damage to the system. A honeypot, which is a computer system implemented to identify resources that was used without consent, may be a potential solution. As no legitimate connections are expected by the honeypot system, an attack on the system would be considered if there are any interactions. An attack alert will be raised based on this information.

Without the assistance of a trust party, this project is about to conduct a technique to detect real-time ransomware to solve the problems. In order to prevent unauthorized programs from opening or modifying files on the device, the file operation mechanism of the operating system on the user's devise will be subjected to an access control policy.

A. Problem Statement

During ransomware attacks, valuable user files located on the device of a victim will be encrypted. The attacker will demand a ransom to unlock the encrypted file. A decryption key is required by the victim to recover the encrypted file. It has emerged in recent years as one of the most dangerous cyber threats, with widespread damage. For example, zero-day ransomware In 2017, WannaCry has caused world-wide catastrophe, from knocking U.K. National Health Service hospitals offline to shutting down a Honda Motor Company in Japan. In some other cases, back to October 25, 2017 Ukrainian transportation systems and Russian media companies were also being attack by ransomware. Other countries such as Germany and Japan was also being targeted by this virus.

Ransomware is a challenging threat that ciphers a user's files while hiding the decryption key until a ransom is paid by the victim [4]. This type of malware is a lucrative business for cybercriminals, generating millions of dollars annually. The spread of ransomware is increasing as traditional detection-based protection, such as antivirus and anti-malware, has proven ineffective at preventing attacks. Additionally, this form of malware is incorporating advanced encryption algorithms and expanding the number of file types it targets. Cybercriminals have found a lucrative market and no one is safe from being the next victim. Encrypting ransomware targets business small and large as well as the regular home user.

II. Literature Review

A detailed literature review was conducted. The review will start with two detection technique that currently being used. Then proceed with the classification of virus ransomware and finally in this chapter, the discussion about danger of ransomware and all the information that related to it will conduct. By having this literature review, it will help to clear the problems that have been occurring during the research before the development of this project being start.

A. Classification of detection technique

For this project, it is using two techniques to detect the virus of ransomware. There are Heuristic analysis and behaviour analysis [5].

B. Classification of virus ransomware

Observing what is the characteristics on how the malware operates is concept of detection using behavior analysis.

Ransomware is a malware family that used cryptography to hijacking user files and associated resources, then requests cryptocurrency in exchange for the locked data [6]. Some ransomware gets into the system utilizing social engineering, malicious advertisements, spamming, drive-by downloads, while others try to discover vulnerabilities to exploit it, using open ports or exploiting a backdoor to get inside [7].

Malware attempts to be hidden and undetectable while upon encrypting the victim valuable file, the system will inform the victim that they are actually being attack by ransomware [8].

Common steps of ransomware attacks:

- System shall be infected via phishing or any other methods.
- Files, documents, folders, and any valuable date will be encrypted and locked.
- Ransom amount will be displayed. In some of the cases, time limit will be also displayed. The ransom amount will be increased once the time is over thus making it more difficult to unlock the files.

According to [9], the chronological ransomware attack begins when the user downloads a suspicious connection from a suspicious website in an email attachment or accident drive. This leads to the next step, because the ransomware file is an executable file, which is the victim's ransomware file. While the ransomware is running, the malware attempts to create a Command & Control connection so that the attacker can access the victim's encryption key to negotiate with the victim.

In addition, author [10], explains that files with various extensions such as pdf, docx, xlss, pptx and jpg are searched for after ransomware. Encryption is then carried out by renaming the file, encrypting the file, and renaming the file again. Depending on the form of ransomware, these measures will reveal the majority of the encrypted file with a unique extension. First the file in the directory has been encrypted, a ransom note containing steps by step to pay the ransom is shown by the ransomware, using Bitcoin in The Onion Ring (TOR) protocol.

Moreover, Akbanov et al. [11] revealed that WannaCry communicates with the command and control server to download the installation program "Tor-browser" via embedded onion addresses via a secure channel on port 443 and the popular Tor ports 900, 9050.

Meanwhile, author [12] has established three Compromise Indicators or IoCs to understand the actions of ransomware. Based on the outcome of ransomware activity identification, these IoCs have been analysed. File changes in the file system are the first indicator to be detected. Ransomware alters the properties of files by encrypting the files, such as modifying the file extension and the file name. The randomness of files in the file system can be observed by a second indicator, which is file entropy.

Since ransomware encryption causes high entropy that activates the detection threshold, this is critical for detecting ransomware actions. Therefore, it is like an attack that the device

can detect. Canary files are the third predictor, which is a fake file implemented with actual files. If ransomware manages to encrypt the data, these files will set an alarm for a device, so early detection can be achieved.

C. Current Technique to Securing from virus ransomware

As advised by Microsoft, damage from a ransomware attack can be mitigated by testing a reliable backup system. It is not possible to upgrade Antivirus early enough to block a ransomware attack. To block the running of programs in common places and to managed domain, AppLocker application was suggested by Microsoft. This application. There is nevertheless, still a risk of writing new variants of malware in unregulated areas thus further investigation has evolved. Due to its morphing nature, it is difficult to detect ransomware because it has already managed to evaded spam filter or firewall.

Almashadani et al. [13] proved that behavioural analysis of crypto ransomware in network interactions, Locky is one of the extremely dangerous ransomware. An experiment from testbed have been implemented, and a set of informational network characteristics were extracted by utilizing two separate classifier working side by side and flow levels. The author assumed that most of ransomware try to get in touch with command and control servers before harmful payloads are achieved.

To show the existence of ransomware, there is no simple signature to search for. *.locky is the common extension used, however the malware is evolving and depanding on the variant, it could easily be *.nochance or *.encrypted. Network administrator need to constantly update the list of filename patterns because the detection would depend on updated list. Due to the difficulties for the network administrator to keep updating the list, therefore it was rejected as an acceptable method as a proof of an attack by searching for an extensions or a unique filename.

Machine learning based system was proposed another method, which whether there is an encryption, dataflow need to be analysed [2]. This method searched for threatening text associated with ransom note. However, only Android platform can use this solution.

Kharraz, Amin, et al. [3] proposed that monitoring the Master File Table (MFT) for activity, and used decoy resources a method of detecting activity. First, looking for a commercial solution to the problem, Varonis in their DatAdvantage product use User Behaviour Analytics (UBA) to determine baseline normal activity [3]. Later, when abnormal activity occurs, such as thousands of file modifies in a short time, this can trigger an email then alerting the administrator and user that unusual access has occurred. Another commercial product is HitmanPro which detects unusual system behaviour, rather than typical static anti-virus signatures. A HitmanPro feature to share detected activity with VirusTotal gives the opportunity to learn more about the attacks.

To detect changes, method such as to use the File Server Resource Manager (FSRM) feature built into Window Server 2012 can also be implemented. As an early warning against poisonous emission, the canary resources name was suggested from the coal miner's tradition bringing down canary mines. File Screening is an access control function which can be used to block unauthorised file writing.

Koecher [14] highlighted that EventSentry product able to track Windows Security logs over the past 3 years, and when user activity passes a threshold, the user action will be triggered. This is a product for aggregating log files by Security Information Management (SIM). Server shutdown can be invoked or an email could be send to informed about the action. This product is available as full featured commercial product, however the free EventSentry Light provides the functionality to undertake necessary monitoring and action [14]. Having determined there were multiple approaches to detect ransomware, further investigation was required to establish which solution would best meet the requirements to invoke an action on the discovery of an intrusion

Table 1 shows the comparison based on previous research for securing from ransomware virus.

Table 1 Technique to securing from ransomware virus

Year	Authors	Title	Method Used
2006	Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda E	Cutting the Gordian knot: A Look Under the Hood of Ransomware Attacks	Use User Bahaviour
2015	Andronio, N., Zanero, S. & Maggi, F.	Heldroid: Dissecting and Detecting Mobile Ransomware.	Data flow will be analyzed in order to determine whether an encryption is taking place
2017	EventSentry Blog	Defeating Ransomware with EventSentry & Auditing	When a threshold is crossed by user activity, it will trigger an action

III. METHODOLOGY

Methodology is a set of procedure or methods used to complete the project. Agile Model was chosen because this method is more flexibility compared to other method, see Figure 1. Agile model allows the user to provide a unique functionality

for future release, the tasks are split into time boxes (small time frames).

Figure 1 Agile Model

IV. PROTOTYPE DEVELOPMENT

The prototyping and product development process involved all devices and software. Each stage that involved was designed to make sure project achieves the target objectives. The main objective in developing this software is to detect the ransomware virus and mitigate the virus if it is pass the threshold level.

A. The Development of Prototype

Visual Studio are needed in order to develop the software. All the coding for developing software will create and run on the visual studio only. The software will filter the viruses based on the default heuristic and behaviour. If the scan file meets the rules that have been set in the heuristic and behaviour, the software will automatically detect that the file has the virus.

If the software detects the new threat, the process of detection will go through to specific coding to filter the entire process. This because the existing heuristic does not have this kind set of behaviour.

Figure 2 Rules Based on Heuristic and Behaviour

Figure 2 shows the coding of heuristic and behaviour process. The software will filter the viruses based on the default heuristic and behaviour. If the scan file meets the rules that have been set in the heuristic and behaviour, the software will automatically detect that the file has the virus.

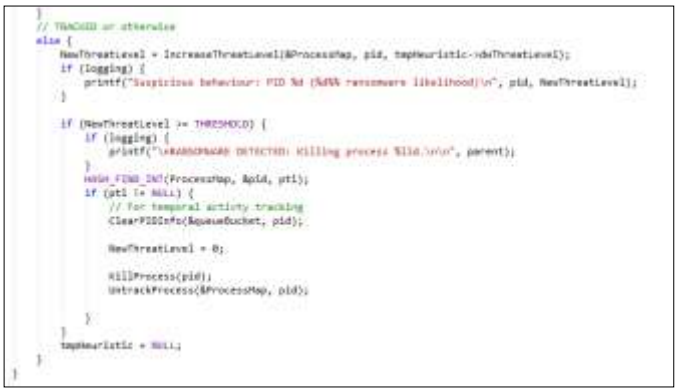

Figure 3 New threat level coding

Figure 3 shows the coding for new threat level. If the software detects the new threat, the process of detection will go through this coding to filter the entire process. This because the existing heuristic does not have this kind set of behaviour.

B. Functionality of Software

This software has their own functionality that makes it different to others software. This software has two function that is to detect and mitigate the ransomware virus. For the detection function, the software will automatically detect any kind of process with extension .exe that seem suspicious. It will calculate the threat level based on the heuristic and behaviour that already have been set in the coding. If the likelihood of the process up 100% and above, this software will automatically detect the process as a ransomware virus and kill the process immediately.

Figure 4 Software Functionality

Figure 4 shows the functionality in this software. This software will automatically attach to the C drive. If users have additional drive or such as E drive, user can choose **/a** to add at the drive to make it can monitor by the software. Command **/d** is used to detach any drive that have been attach to the software. User also can know which drive have been connected to the software by using command line **/l**. By using command line **/s**, user can turn on or off the showing logging output on the screen. If user do not want the software kill the process, user can use **/p**. In addition, **/v** and **/x** can display a verbose output on the screen.

V. TESTING AND RESULT

Software development testing in a project is compulsory in order to check whether the actual results match the expected results. After the system implementation, testing will be done to make sure that the application is functioning. This testing also to ensure all the objectives have been achieved.

To perform this attack, Vmware are needed as a platform to run the testing. Several type of viruses such as GandCrab, WannaCry are needed in order to perform the testing. In addition, the internet connection also need to be disable because the internet connection might affect the whole network on the physical devices.

i. Testing Without Detection Software

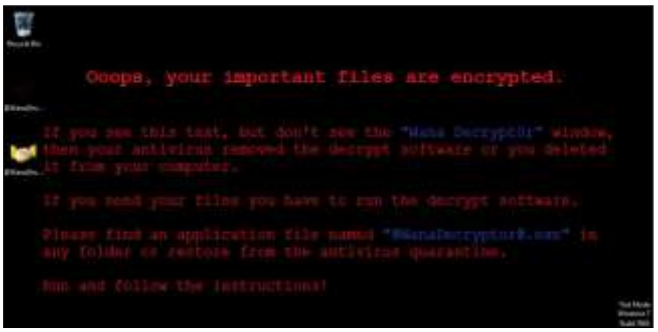

Figure 5 shows the result that windows have been infected by the ransomware virus.

ii. Testing with Detection Software

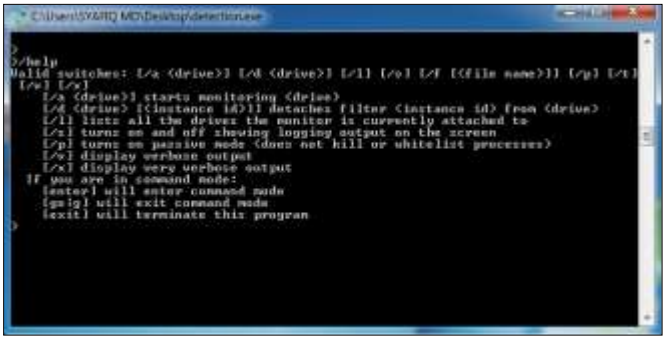

Figure 6 Main interface of detection software

Figure 6 shows the main menu on the detection software. The software will automatically attach to the C drive. To test the software, run the ransomware on the windows 7 to see how the software works.

Figure 7 shows the process of detection and mitigation when the virus run in the windows. The software will calculate the suspicious process to determine whether the process meet the heuristic that have been state in the minispy filter. When the process has been achieved 100% and above, the software will detect it as a ransomware and will kill the process immediately.

Figure 7 The process of detection and mitigation

Figure 8 Duplicate of Ransomware Files

It will generate duplicate files with WNCRY extension. User can still use the original file because the virus did not encrypt the actual file. The virus only duplicates the file and encrypt itself. This is because the software has kill the process before it can encrypt the actual file. In addition, user can manually delete the .WNCRY file and does not have any effect to the other file.

Table 2 shows the result of the testing from three kind of virus ransomware.

Table 2 Result of testing

Type of virus	Expected Result	Actual Result	Status (Success /Fail)
WannaCr y	The software can detect and mitigate the process	The software detected the software and mitigate the process of ransomware. But it do duplicate file .WNCRY to folder.	Success
GandCrab	The software can detect and mitigate the process	The software detected the javascript program and mitigate the process immediately.	Success
Petya	The software can detect and mitigate the process	The software cannot handle the advance encryption that has been used in this virus	Fail

VI. CONCLUSION

This project has been accomplished the entire objective. The first objective, which is to study the attack of the ransomware and how to securing the user data from being infected by the virus. To achieve the first objectives for this project, articles and journals that are related to the ransomware virus attack that are happened between these days, the detection and mitigation concept and everything that is in touch with how to detect and reduce the virus.

The second objective is to develop the software that can be detect and mitigate the ransomware virus. Detection and Mitigation of Virus Ransomware project has been developed by using Visual Studio only. Besides that, to develop this project, agile model has been used. By using agile model, it can help to manage work more efficiently and do the work more effectively. Lastly, to test the software to ensure the attacks can be prevented by the software. For this objective, several viruses have been chosen based on their behaviour. The result shows the third objective has been achieved when the software can mitigate the process of viruses.

As a conclusion, this project has been achieved the entire objective. An impact from a ransomware attacks can be very devastating to a small organization and business owners. It also gives an impact towards people. Detection is one of the first important step to make sure our system safe from being infected. By using this technique, we can save our data from being lock by virus ransomware.

VII. RECOMMENDATION

Each software usually has its own weaknesses. From the weaknesses, some enhancement is needed to improve the software. As for recommendation and improvement of the software in a future, this suggestion may help this project to make it more efficient to user use it. This project can improve by adding more features such as the prevention of viruses. Besides that, by implementing autorun features, it can facilitate users to use the software.

In addition, an option for the quarantine process such as to keep or delete the viruses need to be implemented. From this, user can make their own decision for each quarantine viruses.

Lastly, this work can be extended by combining more techniques to prevent ransomware and make user data more resistance to ransomware.

REFERENCES

[1] Y. Yanfang, L. Tao, D.A. Adjeroh, S. S. Iyengar, A Survey on Malware Detection using Data Mining Technique, ACM Computing Survey, 2017.

[2] Andronio, N., Zanero, S., & Maggi, F. (2015). HelDroid: Dissecting and Detecting Mobile Ransomware. Research in Attacks, Intrusions, and Defenses Lecture Notes in Computer Science, 382-404. doi:10.1007/978-3-319-26362-5_18

[3] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). FCutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. Detection of Intrusions and Malware, and Vulnerability Assessment. Lecture Notes in Computer Science, 3-24. doi:10.1007/978-3-319-20550-2_

[4] D. Nieuwenhuizen, A Behavioral – Based Approach to Ransomware Detection, MWR Labs Whitepaper, 2017

[5] Deka, D., Sarma, N., & Panicker, N. J. (2016). Malware detection vectors and analysis techniques: A brief survey. 2016 International Conference on Accessibility to Digital World (ICADW). doi:10.1109/icadw.2016.7942517

[6] Al-rimy B, Maarof M, Shaid S. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers and Security.2018; 74:144-166.

[7] Popli N, Girdhar A. Behavioural Analysis of Recent Ransomware and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware. In Verma, Nishchal K, Ghosh, A. K. (eds) Computational Intelligence: Theories, Applications, and Future Directions - Volume II ICCI-2017. Springer, Singapore. 2018;799(4):65–80.

[8] K. Cabaj, M. Gregorczyk, W. Mazurczyk, Software-Defined Networking Based Crypto Ransomware Detection using HTTP Traffic Characteristics, Computers and Electrical Engineering, vol. 66, pp. 353 -368, 2018

[9] M. Safwan Rosli1 Abdullah. R S, Yassin. W, Faizal M.A and Wan Mohd Zaki ,W.F.H "Ransomware Behavior Attack Construction via Graph Theory Approach" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 2, 2020

[10] G. Hull, H. John, and B, Arief, "Ransomware deployment methods and analysis: views from a predictive model and human responses," Crime Science 2019, 8(1), p. 2.

[11] Akbanov M, Vassilakis VG, Logothetis MD. WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention, and Propagation Mechanisms. Journal of Telecommunications & Information Technology. 2019 Mar 1(1).

[12] Chew, and V. Kumar, "Behaviour Based Ransomware Detection," Proceedings of 34th International Conference, vol. 58, pp. 127-136, March 2019.

[13] Almashhadani A, Kaiiali M, Sezer S, O'Kane P. A MultiClassifier Network-Based Crypto-Ransomware Detection System: A Case Study of Locky Ransomware. IEEE Access. 2019; 7:47053-47067.

[14] Ingmar Koecher, "Auto Administrator: Chapter 3". EventSentry Blog, June 2, 2017. [Online]. Available: https://www.eventsentry.com/blog/2017/06. [Accessed November 24, 2020]