EAI Endorsed Transactions
on Energy Web

Research Article EAI.EU

A Three-Level Ransomware Detection and Prevention Mechanism

Amos Loh Yee Ren[1], Chong Tze Liang[1], Im Jun Hyug[1], Sarfraz Nawaz Brohi[1], NZ Jhanjhi[1,*]

[1] School of Computing & IT, Taylor's University, Malaysia.

Abstract

Ransomware encrypts victim's files or locks users out of the system. Victims will have to pay the attacker a ransom to decrypt and regain access to the user files. Petya targets individuals and companies through email attachments and download links. NotPetya has worm-like capabilities and exploits EternalBlue and EternalRomance vulnerabilities. Protection methods include vaccination, applying patches, et cetera. Challenges faced to combat ransomware include social engineering, outdated infrastructures, technological advancements, backup issues, and conflicts of standards. Three-Level Security (3LS) is a solution to ransomware that utilizes virtual machines along with browser extensions to perform a scan, on any files that the user wishes to download from the Internet. The downloaded files would be sent over a cloud server relay to a virtual machine by a browser extension. Any changes to the virtual machine after downloading the file would be observed, and if there were a malfunction in the virtual machine, the file would not be retrieved to the user's system.

Keywords: Malware, Petya, Ransomware, Security, Virtual Machine

Received on 16 September 2019, accepted on 29 December 2019, published on 14 January 2020

doi: 10.4108/eai.13-7-2018.162691

* Corresponding author. Email: noorzaman.jhanjhi@taylors.edu.my

1. Introduction

Malware is a common threat to many computer systems since the Internet has become widely used. Ransomware is a new form of malware which utilizes the benefits of cryptography to encrypt the file system table of an infected computer's hard drive and prevents Windows from booting, rendering the whole computer system of the user to be useless. The attacker will then ask for a 'ransom' from the victim if they wish to decrypt and regain access to the system. The two types of ransomware recently identified are described as below.

1.1. Petya

Petya, a trojan horse classified ransomware that, according to Symantec, was first discovered on 29th March 2016, spreads through emails with attachments or download links to the malware. It is disguised to look like any other innocent and legitimate program. Trojans are malicious codes (not viruses) as they do not reproduce by infecting other files, nor do they self-replicate like worms [1]. Once Petya enters the user's system, it immediately forces a restart if it is run by the user and given administrative access via Windows User Account Control (UAC). A fake CHKDSK utility screen is shown seemingly to repair the sector. The fake utility screen deceives the user into not turning off the system while it overwrites and encrypts the Master Boot Record (MBR) which is unknown to the user. Once completed, Petya restarts the system again and

displays a screen with a flashing ASCII art of skull and crossbones prompting the user to press any key. After any key is pressed, a ransom note is displayed. The victim is required to access through a separate computer which is not infected to pay the ransom.

1.2. NotPetya

In June 2017, a variant of Petya ransomware emerged. It was named as NotPetya by Kaspersky Systems to distinguish it from its original, due to its significantly different operating methods. This variant affects systems connected through a local network. It abuses the Windows exploits EternalBlue and EternalRomance, which is the same exploit used by WannaCry. The exploit utilizes the vulnerability in Server-Message-Block (SMB) version 1 and allows anyone on the Internet to attack SMB servers and run any code. SMB protocol enables applications on a computer to read and write to files and request services from server programs in a
computer network [2]. Upon execution of NotPetya, it immediately deletes its executable (.exe or .dll) and encrypts all the files within the system.

NotPetya also schedules a force restart to the system in an hour and can be seen through the Task Scheduler. Unlike the original Petya variant, NotPetya will try to spread itself similar to a worm. It utilizes Local Security Authority (LSA) dump tool which copies credentials from memory and uses the collected credentials with PsExec or Windows Management Instrumentation Command-line (WMIC) tool to remotely infect computers. PsExec allows executing processes on other systems, complete with full interactivity for console applications, without having to install client software manually [3]. The WMIC tool enables systems management from the command line [4]. NotPetya checks for security products based on process names and alters its behavior if some are found. For example, if Norton or Symantec Endpoint Protection (SEP) is detected, it does not try the EternalBlue exploit. When force restarted, like the original Petya, it displays the same fake CHKDSK utility which secretly encrypts the MBR and immediately displays the ransom message after completion and another reboot (without the flashing skull and crossbones). The research mainly contributes about ransomware and how Petya and NotPetya operates, along with the necessary measures to combat similar ransomware. Further, research proposed a solution and a method to deal with the ransomware or malware by using virtual machines. This paper is organized as follows:

Section II – Characteristics and findings
Section III – Protection mechanisms
Section IV – Challenges of combating ransomware
Section V – Solution: Three-Level Security (3LS)
Section VI – Conclusion
Section VII –Future Work

2. Characteristics and Findings

Since the emergence of ransomware, many characteristics and findings were identified through researches and investigations.

2.1. Technical Analysis

An analysis was made by the Carbon Black Threat Research Team to uncover the secret behind the ransomware after its attack on Maersk, the world's largest container shipping company.

Table 1. Details of Analysed NotPetya

File Size	362,360
MD5	71b6a493388e7d0b40c83ce903bc6b04
SHA1	34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
SHA256	027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
Fuzzy	6144:y/Bt80VmNTBo/x95ZjAetGDN3VFNq7pC+9OqFoK30b3ni5rdQY/CdUOs2:y/X4N
Magic	PE32 executable for MS Windows (DLL) (console) Intel 80386 32-bit
Import Hash	52dd60b5f3c9e2f17c2e303e8c8d4eab

With this initial analysis, the research team thought that a new variant of Petya was created. Table 1 shows many similarities of NotPetya with Petya regarding functionality and encryption. However, upon further inspection, it seemed

to be an entirely new type of ransomware. Hence, the name "NotPetya" or "Schrodinger's Petya" was created.

2.2 Wiper Disguised as Ransomware

Based on the analysis of encryption routine in Petya attacks done by experts from Kaspersky Lab, theorized that NotPetya was designed to be a wiper under the disguise of ransomware. They discovered that "the ID shown in the ransom screen is just plain random data", where the attackers are unable to use the random data for identification to decrypt the victim's data even if the victim pays the ransom. NotPetya is even more malicious than other ransomware such as WannaCry, as it has no clear "kill switch" [5]. A kill switch is "a computer function for disabling software or a device remotely" [6]. To better understand ransomware, research on ransomware emergence and how it spreads was conducted.

2.3 Evolution of Ransomware

Reference [7], the first instance of the appearance of ransomware, AIDS Trojan (also known as the PC Cyborg) was in 1989. It was distributed via floppy disks which were labeled "AIDS Information – Introductory Diskettes" at the World Health Organization's International Aids Conference. It used a simple symmetric cryptography algorithm to encrypt file names. The first modern ransomware appeared in May 2005, the Trojan. Gpcoder (also known as GP Code and GPCoder). Majority of early ransomware was developed by Russian criminal organizations and spread by email attachments throughout Russia and its neighboring countries. Ransomware evolved through the subsequent years, following up to the latest Petya ransomware in 2016. Methods used to combat each ransomware must be documented, as it is vital for constructing new techniques to combat future ransomware.

2.4 Monitoring Ransomware

An investigation of common characteristics of ransomware attacks was done by Kharraz [8] to detail its interaction with the file system. A monitoring tool to capture input/output (I/O) requests was developed to describe how malicious process interacts with file systems. The I/O requests were monitored by defining callback routines to record any I/O activity on the files. A minifilter was deployed in a privileged kernel so that it would have access to almost all objects of the operating system. Through this finding, computer forensic investigators are provided with knowledge on how to monitor ransomware.

3. Protection Mechanisms

As many ransomware such as the recent Petya and WannaCry emerge, proper protection mechanisms must be implemented and used.

3.1 Vaccination from NotPetya

In the case of the Petya variant, NotPetya, there is no kill switch to the malware, but there is a vaccine. The creation of a read-only file called "perfc" in the C:\Windows folder prevents infection. This method is effective because the NotPetya checks and creates "perfc" which is an infection marker. If the infection marker exists, the NotPetya malware considers the system is already infected and does not encrypt.

3.2 Updates and Patches

Microsoft has released updated versions of Windows which prevent recent ransomware that takes advantage of Windows vulnerabilities. According to Microsoft, their latest Windows 10 operating system is resilient against Petya. The updated Windows 10 help mitigate SMB exploits like EternalBlue and EternalRomance [9].

3.3 Anti-Malware & Anti-Ransomware software

After the recent outbreak of different variants of ransomware, antivirus vendors have integrated ransomware prevention tools within their software and provide a separate specialized anti-ransomware tool to combat known ransomware such as Petya and its variants.

3.4 Least Privilege Principle

Least privilege is the concept and practice of restricting access rights to only those resources required to perform routine, legitimate activities [10]. NotPetya often spreads through a system due to lack of configuration and management of access control of the users. The root of the cause of ransomware is due to the accidentally allowed admin privileges which enable NotPetya to create malicious files and encrypt the victim's data.

3.5 Prudence, Self-awareness, and Logic

All the security and prevention in the world would not be able to save users from ransomware if they are careless. The users must take responsibility in educating themselves to be aware of obvious malware threats to prevent an outbreak of an epidemic computer virus situation.

4. Challenges of Combating Ransomware

Although many protection mechanisms can be used to prevent people from getting infected, many still fall victim to ransomware such as Petya and NotPetya.

4.1 Social Engineering

Social engineering is a technique used by cybercriminals to lure unsuspecting users into sending their confidential data, infecting their computers with malware or opening links to infected sites [11]. Many businesses fall prey to Petya and NotPetya as it spreads in the form of emails disguised as job application resumes with attachment or a download link. The two ransomware take advantage of regular business sustainability factors such as employment. Social engineering makes it easy for targeted people to be tricked as it utilizes what users usually do and make it seem natural. For example, gamers who intend to get a "free" paid game, are prone to download software from suspicious websites and execute it.

4.2 Outdated Infrastructure

Many ransomware exploits vulnerabilities in computers running outdated operating systems. Many companies and government bodies are hugely affected by this as most of the systems are not updated due to stability and security issues when upgrading. Businesses hit by the NotPetya attack were affected using the same vulnerability as WannaCry because their systems had still not been updated [6]. The cost of upgrading and retraining of staff is often deemed not worth the effort to stay up to date as it interrupts their business processes. However, the reluctance to upgrade caused most of them to be vulnerable.

4.3 Technological Advancement

Ransomware such as NotPetya use complex and established encryption algorithms to encrypt the compromised system's files. NotPetya encrypts the victim's data with a dynamically generated, 128-bit key and creates a unique ID of the victim [12]. The encryption algorithm used is Advanced Encryption Standard (AES) 128-bit, which is not feasible to be cracked via brute force as it would take a billion of years and too many resources.

4.4 Backup Issues

Ransomware holds victim's data as the hostage, with some people opting to pay the ransom to restore their compromised system. The ransomware issue escalates due to many not having a proper and regular backup. According to a data storage provider, Backblaze and their backup awareness survey, 91% of Americans do not back up their computers daily, and 21% of Americans have never backed up all the data on their computers. Although the survey focuses on Americans, the same is applicable to people elsewhere.

4.5 Conflicts of Standard

Many software developed particularly for medical purposes are marketed as "built to last," which conflicts to "update often." Certification and testing have been done extensively for built to last software. However, it is only for that version. As such, software which is classified as built to last, are not planned and regularly updated causing it to be vulnerable to ransomware that exploits vulnerabilities. While, software that undergoes updates and changes often require to be retested and recertified for compatibility safety, security and other criteria.

5. Solution: Three-level Security (3LS)

Due to ransomware continuously emerging and evolving, a new solution is derived to reduce, detect and eliminate these types of malware. The solution suggests a three-level security mechanism which utilizes a browser extension, Virtual machine (VM), and anti-malware/anti-ransomware solutions within the VM.

The first level of security is achieved through a browser extension which can detect any malicious websites accessed that attempts an unauthorized download of files. Once identified at the browser extension level, it immediately prevents any access and blocks the malicious process or site. The browser extension uses two layers of malware detection mechanism which are Signature-based Detection mechanism and Anomaly-based Detection mechanism. The first layer uses the Signature-based Detection mechanism with a hybrid approach, where the browser extension will be able to either use the syntax or structural properties of the program or leverage the runtime information to determine its maliciousness. Should the malware remain undetected and penetrates the first layer, the second layer within the browser extension kicks in as it utilizes Anomaly-based Detection due to its specialty in detecting a new type of malware. A key advantage of anomaly-based detection is its ability to detect zero-day attacks [13]. Also, the browser extension acts as a download manager which ensures any files downloaded via the browser is saved to a VM through cloud computing. The second level of security mechanism is tied closely to the browser extension which makes use of the VM to create a contained environment. Virtual Machine Manager can provide an additional security layer to the system and can act as a security tool during updates [14]. The third level of security is the usage of anti-malware/anti-ransomware solutions which scans the downloaded files within the VM, eliminating any potential threats that bypassed the initial two levels.

3LS also acts as indirect protection from staged malware. "When the network virtualization isolates virtual networks used by VMs, it also isolates faults and attack impacts in a network" [15]. Most recent well-known malware uses some downloader or dropper as their initial program to execute on the victim's computer [14]. Hence, by using the download manager in the form of a browser extension proposed in this solution, not only can it stop ransomware from intruding the

main computer, but it can also reduce the number of people using questionable downloaders. The main protection is achieved using a virtual machine where the ransomware is tricked into an enclosed virtual space and attempts to manifest. Not only does this isolate the ransomware successfully, it also tricks the sender into thinking the system has been compromised, hence there would not be a second wave of ransomware. The proposed solution is unique as every download will be sent to separate and individual virtual spaces to ensure that one infected download will not spread to others that are safe. However, due to the limitation of current technology, only four downloads are allowed per instance. Once the file has been sent to the VM, there will be another Signature-based Detection mechanism inside with a dynamic approach. Since this Signature-based Detection mechanism has a different database, it may find malware that those on the previous level may have missed. The two-layer detection mechanism ensures the highest possible safety levels for users. Once the scan is complete and no issue is found, the user will be given an option to retrieve the file from the VM.

Most antivirus software is most vulnerable when they are updating, as the software will be inactive during the time of update. All antivirus software must be updated at a very high frequency to provide up-to-date protection of a computer system [14,16,17]. In [18] prevention of ransomware using a pre-encryption detection algorithm has been suggested. 3LS will be able to alleviate the issue by updating itself only when the user is not using it. Unlike antivirus software, 3LS utilizes the VM to contain the infection of malware. The proposed security mechanism allows the user to drag and place any file they deem suspicious into the VM and run it from there. If the file is malicious, the threat will be contained inside the VM without harming the host system. The remote execution is useful for users when they want to check the files received. The drawback for this function is that the number of downloads the user can do per instance will drop in accordance to how many VMs are concurrently used due to the limitations of the machine. Fig. 1 shows an illustration of 3LS, where a user laptop or personal computer accesses the browser extension, it is connected through cloud computing. The cloud allows resource sharing which enables VMs to be created locally within the user's system or externally in a cloud server based on the number of files downloaded. Fig. 2 and 3 show the browser extension mockup, where the browser extension has detected ransomware. The browser extension allows the user to identify, block and delete the threat before the threat is downloaded. If the threat manages to bypass the detection, the anti-malware within the system will detect and automatically quarantine it. The user is given a choice to choose to trust the file or delete the threat.

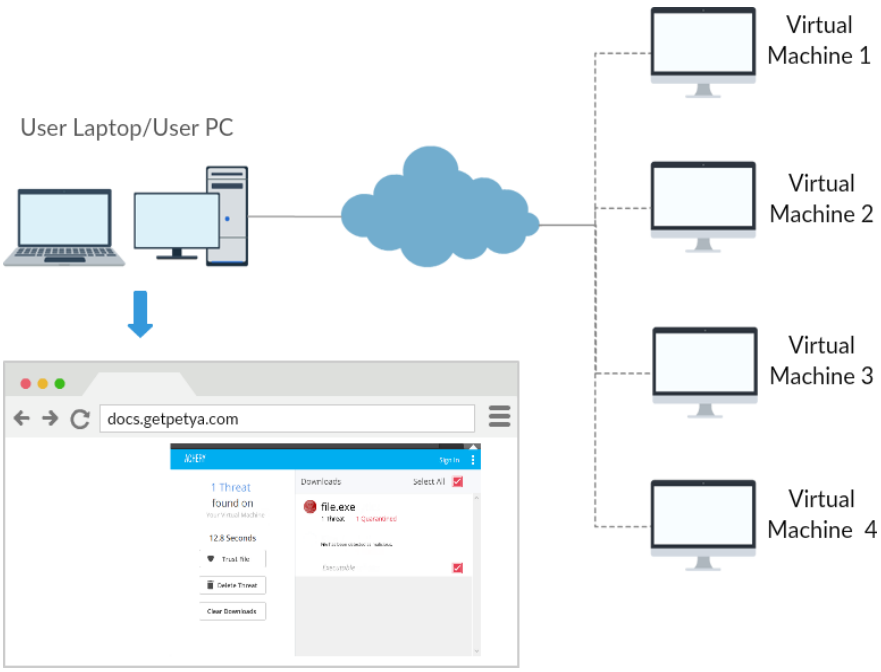

Fig. 1. Illustration of Three-Level Security (3LS)

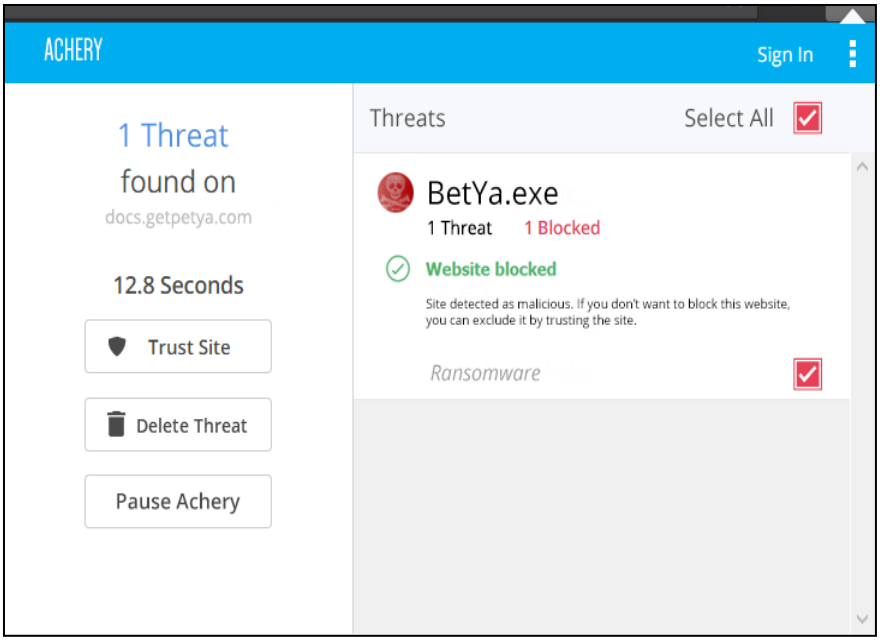

Fig. 2. Browser Extension Mockup (While Browsing)

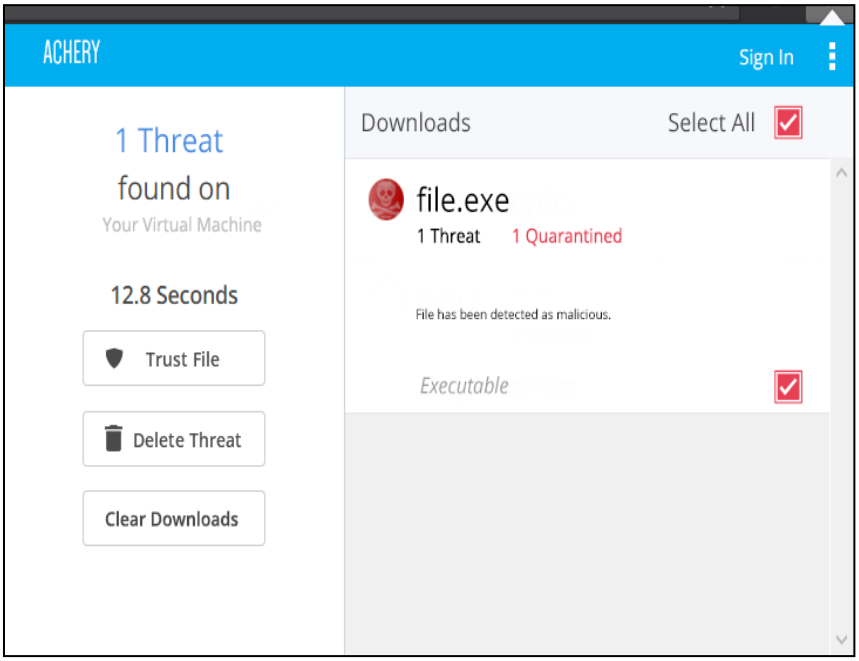

Fig. 3. Browser Extension Mockup (After Downloading)

6. Conclusion

This research covers the concept of Petya and NotPetya, with the Petya ransomware encrypting only the MBR, and its variant NotPetya encrypting both files and MBR. NotPetya emerged with worm-like capabilities and exploiting existing vulnerabilities. While initially classified as ransomware, NotPetya was later identified as a wiper that disguised as ransomware because of how NotPetya corrupted the victim's data instead of encrypting them.

In our solution, we proposed a method to deal with the ransomware or malware by using virtual machines. The aim is to isolate potential malicious files into the virtual machine and quarantine them instead of letting malwares, the host system. While our solution managed to isolate any malicious files before they can cause severe damage, there

are some limitations. With the current technology, it is difficult for a computer to run more than a few virtual machines at the same time. Thus, the user can only have four downloads per instance as each file are put into separate, dedicated virtual machines to prevent one file from infecting the others.

7. Future Work

In the future, we hope to increase the number of virtual machines one computer can handle with technological advancement. In our research, we firmly believe that virtual machines can prove to be a valuable protection mechanism against malware, and this is a step in the right direction to combating malware.

References

[1] I. Khan, "An introduction to computer viruses: problems and solutions", Library Hi Tech News, vol. 29, no. 7, pp. 8-12, 2012.

[2] "Server Message Block Overview", Microsoft, 2013. [Online]. Available: https://technet.microsoft.com/en-us/library/hh831795(v=ws.11).aspx. [Accessed: 12- Nov- 2017]

[3] "PsExec - Windows Sysinternals", Microsoft, 2016. [Online]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/psexec. [Accessed: 12- Nov- 2017]

[4] "WMIC - Take Command-line Control over WMI", Microsoft, 2017. [Online]. Available: https://msdn.microsoft.com/en-us/library/bb742610.aspx. [Accessed: 13- Nov- 2017]

[5] S. Shackelford, "'NotPetya' ransomware attack shows corporate social responsibility should include cybersecurity", The Conversation, 2017. [Online]. Available: http://theconversation.com/notpetya-ransomware-attack-shows-corporate-social-responsibility-should-include-cybersecurity-79810. [Accessed: 13- Nov- 2017]

[6] "kill switch | Definition of kill switch in English by Oxford Dictionaries", Oxford Dictionaries | English, 2017. [Online]. Available: https://en.oxforddictionaries.com/definition/kill_switch. [Accessed: 13- Nov- 2017]

[7] R. Richardson and M. North, "Ransomware: Evolution, Mitigation and Prevention", International Management Review, vol. 13, no. 1, pp. 10-21, 2017.

[8] A. Kharraz, "Techniques and Solutions for Addressing Ransomware Attacks", Ph.D, Northeastern University, 2017.

[9] "Windows 10 platform resilience against the Petya ransomware attack", Microsoft Secure. 2017 [Online]. Available: https://blogs.technet.microsoft.com/mmpc/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/. [Accessed: 14- Nov- 2017]

[10] M. Miller, "What Is Least Privilege & Why Do You Need It?", Beyond Trust. 2017 [Online]. Available: https://www.beyondtrust.com/blog/what-is-least-privilege/. [Accessed: 14- Nov- 2017]

[11] "Social Engineering - Definition", Kaspersky. [Online]. Available: https://usa.kaspersky.com/resource-center/definitions/social-engineering. [Accessed: 14- Nov- 2017]

[12] "Petya Ransomware | US-CERT", US-CERT, 2017. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA17-181A. [Accessed: 15- Nov- 2017]

[13] N. Weaver, V. Paxon, S. Staniford, and R. Cunningham. A taxonomy of computer worms. In Proceedings of the 2003 ACM Workshop on Rapid Malcode, pages 11–18, 2003.

[14] B. Min, V. Varadharajan, U. Tupakula and M. Hitchens, "Antivirus security: naked during updates", Software: Practice and Experience, vol. 44, no. 10, pp. 1201-1222, 2013.

[15] H. Liao, C. Richard Lin, Y. Lin and K. Tung, "Intrusion detection system: A comprehensive review", Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16-24, 2013.

[16] SH Kok, Azween Abdullah, NZ Jhanjhi and Mahadevan Supramaniam,(2019). Ransomware, Threat and Detection Techniques: A Review, IJCSNS International Journal of Computer Science and Network Security, 19 (2), pp. 136-146

[17] SH Kok, Azween Abdullah, NZ Jhanjhi, Mahadevan Supramaniam, “A Review of Intrusion Detection System Using Machine Learning Approach”, in International Journal of Engineering and Research, Jan 2019.

[18] SH Kok, Azween Abdullah, NZ Jhanjhi, Mahadevan Supramaniam, “Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm”, in Computers MDPI, vol.8, no.4, pp.79 Nov. 2019.