Asian Journal of Applied Science and Technology (AJAST)
(Peer Reviewed Quarterly International Journal) Volume 3, Issue 3, Pages 05-16, July -September 2019

A Survey on Different Types of Ransomware, its Detection, Recovery and Prevention

Gowthami & Libujashree R.

MVJ College of Engineering, Near ITPB, Whitefield, Bangalore-560 067, India.
Email: gowthami@mvjce.edu.in & libuja97@gmail.com

Article Received: 19 January 2019 Article Accepted: 01 May 2019 Article Published: 09 July 2019

ABSTRACT

For today's business owners and technology executives, cyber security is a top concern. In fact, a report from CBS Money Watch recently revealed that 80% of U.S. businesses were successfully hacked. Hackers are aware of the common vulnerabilities that organizations face, keeping security professionals on their toes constantly. There are three Cyber Security concerns business owners may face: Unprecedented attacks, data theft, cyber espionage. Clearly, there are many vulnerabilities in a new age of cyber security threats for both large and small businesses. Understanding the methodology of a hacker can help to mitigate the imminent threat of stolen data. You can prevent the massive damage resulting from large-scale data breaches by staying ahead of the game when it comes to cyber security. This paper describes a detailed survey on one of the malware known as ransomware which is a recent cyber threat.

Keywords: *Cyber security, unprecedented attack, data theft, cyber espionage, malware, ransomware.*

1. INTRODUCTION

A malware attack is a type of cyber attack in which malicious software performs activities on the victim's computer system, usually without knowledge of the victim. People today use words such as malware, spyware, and ransomware much more than the word "virus." (Bhojani et.all) [1]. We need to look at the word's original biological meaning to understand the virus. Biological viruses can make you sick; they inject their own code (DNA or RNA) as a replication tool into the host cell. This code makes the host cell ultimately burst, sending new viruses everywhere to generate many copies of the virus. Using similar means, computer viruses operate [2-4]. Computer viruses tend to be a smaller piece of code that can piggyback on other computer applications and files, unlike some malware programs that are fully executable in nature (Lakhotia et.all) [5]. Only when conditions are right, viruses replicate. So by a certain date and time they can be triggered, opening a specific program, etc.

1.1. An overview of most significant and common malware types

Adware:

Adware is the name given to programs that display ads on your computer, redirect your search requests to advertising websites, and collect marketing data about you. For example, adware typically collects the types of websites you visit so that advertisers can display custom ads. Many consider adware to be malicious adware which collects data without your consent. Another example of malicious adware is intrusive pop-up ads for supposed fixes for non-existent computer viruses or performance problems.

Spyware:

Spyware is a software that spies on you, as the name implies. Spyware, like adware, will often send your browsing activities to advertisers, designed to monitor and capture your web browsing and other activities. However, spyware includes features that are not found in adware. It can also capture sensitive information such as bank

accounts, passwords, or information on credit cards, for example. Although not all spyware is malicious, it is controversial because it is capable of violating privacy and has the potential for abuse.

Computer virus:

The main feature of a computer virus is malicious software to be reproduced by cybercriminals. Usually it does that by attacking and infecting the target system with existing files. Viruses have to perform their dirty work, so they target any type of file the system can perform. From the early days of computers, viruses have been around, at least in concept. In 1949, John von Neumann did the first academic work on the theory of computer self-replicating programs. The first examples of viruses actually appeared in the seventies. While their threat has declined in recent years and other forms of malware have moved into the spotlight, over the years, viruses have caused widespread destruction. They consume system resources besides stealing and corrupting data — often rendering the host system ineffective or even useless. Another common feature of viruses is that they are covered, which makes them difficult to detect. Viruses come uninvited, hide in secrecy, reproduce when executed by infecting other files and usually work in darkness.

Worms:

Worms are infectious like a virus, and they are designed by cyber criminals to replicate themselves. However, a worm replicates files that are already present on a computer without targeting and infecting them. Worms carry themselves in their own containers and often limit their activities within the application that moves them to what they can accomplish. To spread, they use a computer network, rely on the target computer to access security failures, and steal or delete data. Many worms are designed to spread only and do not try to change the systems through which they pass.

Trojan:

A Trojan is a malicious program that appears to be useful to misrepresent itself. Cybercrime offers trojans in the guise of routine software that persuades a victim to install it on their computer. The term derives from the wooden horse's ancient Greek story used to stealth invade Troy's city. Trojan horses on the computers are just as deadly. The payload can be anything but is usually a backdoor form that allows unauthorized access to the affected computer for attackers. Trojans also provide access to a user's personal information such as IP addresses, passwords, and banking details for cyber criminals. They are often used to install keyloggers that can easily capture account and password names or credit card data and disclose the data to the malware actor. Most ransomware attacks are performed using a Trojan horse by storing the harmful code within a seemingly harmless piece of data. Security experts believe that Trojans are among today's most dangerous types of malware, especially Trojans designed to steal users ' financial information. In fact, some insidious types of Trojans claim to remove any viruses from a computer but introduce viruses instead.

Phishing:

Phishing is a cybercrime in which someone posing as a legitimate institution to lure the victim into providing sensitive data, such as personal identifiable information, banking, credit card details and passwords, contacts a

target or targets by email, telephone or text message. Phishing is not technically a type of malware, but rather a method of delivery used by criminals to distribute many types of malware. Because of its significance, we listed it among malware types here to illustrate how it works. A phishing attack often lures an individual to click on a URL infected with malware that fools the victim into thinking that they are visiting their bank or other online service. Then the malicious site captures the ID and password of the victim, or other personal or financial information. Spear Phishing refers to an attack targeting a particular individual or group of individuals, such as a corporation's CFO, to gain access to sensitive financial information. The masses are targeted at regular "phishing."

Ransomware:

Ransomware is a type of malware that, typically by encryption, locks the data on a victim's computer. Before decrypting the ransomed data and returning the victim access, the cybercriminal behind the malware demands payment. The motive for attacks on ransomware is almost always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has taken place and instructions are given to make payment to restore the data to normal. In a virtual currency, such as Bitcoin, payment is often required so that the identity of the cybercriminal remains hidden (Brien at.all) [6-7].

2. COMMON TYPES OF RANSOMWARE

There are two main types of ransomware: Locker ransomware, which locks the computer or device, and Crypto ransomware, which prevents access to files or data, usually through encryption.

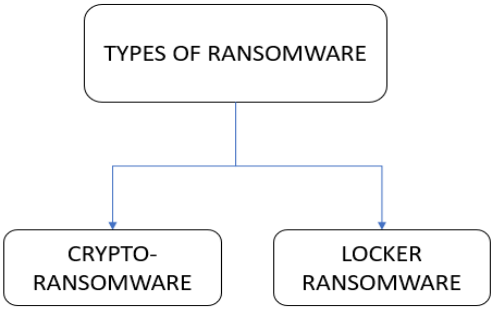

Fig 1: Types of Ransomware

2.1. Crypto-ransomware:

Crypto ransomware is as simple as armed against victims with strong encryption to deny them access to those files. The malware silently identifies and encrypts valuable files when the ransomware infiltrates the device of the victim. The ransomware only asks the user for a fee to access their files after successfully accessing the target files is restricted. The user loses access to encrypted files without the decryption key held by the attackers or, in some cases, a vendor decryption solution. Ransomware crypto often includes a time limit. Some crypto ransomware variants even provide a site for users to buy Bitcoins and articles explaining the currency.

2.2 Locker Ransomware:

This is also referred to as a computer locker. This ransomware does not encrypt the victim's files but denies the device access instead. This locks the user interface of the device and then demands a ransom from the victim. This ransomware is going to leave the victim with very few capabilities such as just allowing the victim to communicate with the attacker and pay the ransom.

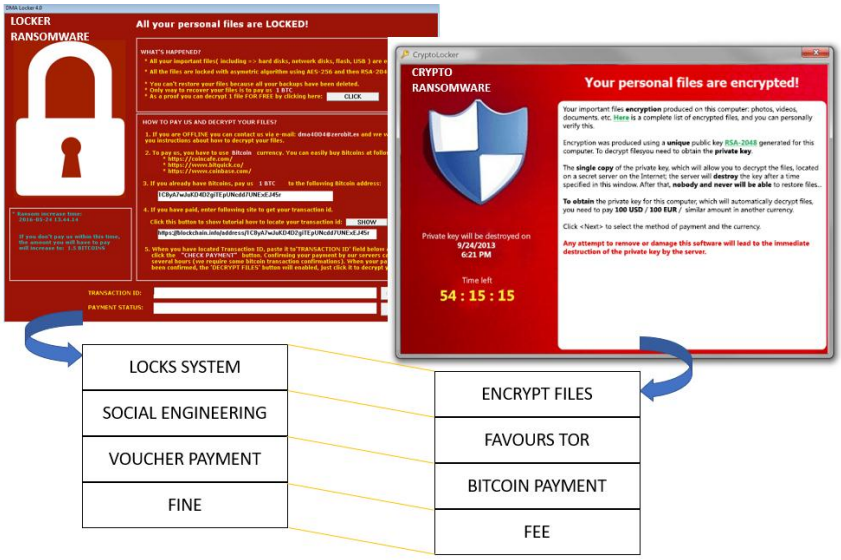

Fig 2: Comparison of locker ransomware and crypto ransomware

3. MOST ADVANCED RANSOMWARE FAMILY EXAMPLES

Ransomware encrypts data on a server, workstation, or mobile device and demands a ransom through a Bitcoin-like cryptocurrency. But not all ransomware is financially motivated— some are intended primarily to cause a network operational disruption. Below are the examples of real-life ransomware that are used on a regular basis— and are extremely hazardous [7].

Some of the common Ransomware families are

Bad Rabbit:

A strain of ransomware that has infected Russian and Eastern European organizations. Bad Rabbit is spread on compromised websites through a fake Adobe Flash update. When a machine is infected with ransomware, users are directed to a payment page requiring $285.05 bitcoin. With its advanced antivirus, Comodo has already beaten Bad Rabbit with multiple scanners and malware detection tools. Bad Rabbit is a kind of ransomware that claims to be a legitimate update of the Adobe Flash player. When the user visits a specific website, the availability of a new version of Adobe is interrupted by flashing. When the user clicks the bait it will be installed when it is installed. Bad Rabbit is a dangerous malware because it encrypts the hard disk of the computer as well as the files. It also prevents normal booting of Windows. The good news is that Comodo has a powerful antivirus that detects any kind of malware instantly. It uses multiple detectors and recognizers that recognize and block malicious files quickly before it even reaches the computer. Comodo provides instant ransomware protection.

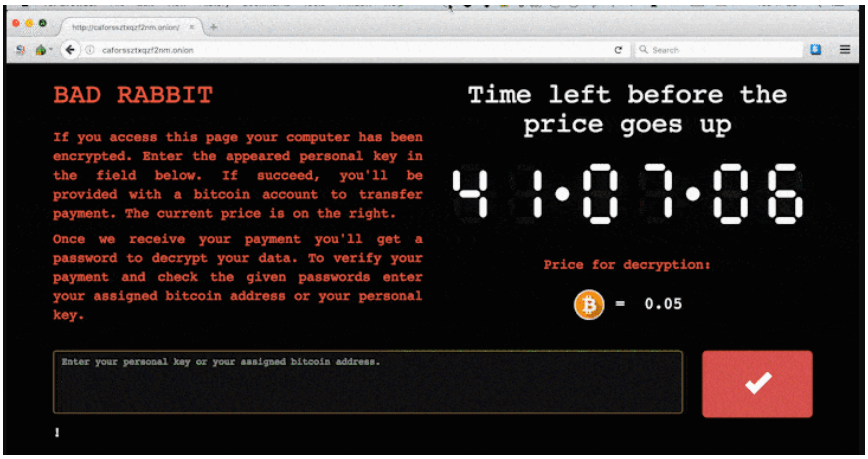

Fig 3: Bad Rabbit Ransomware

Crypto-Locker:

Ransomware has been around for the past two decades in some way or another, but with CryptoLocker it really came to prominence in 2013. The original botnet from CryptoLocker was shut down in May 2014, but not before nearly $3 million was extorted from victims by the hackers behind it. The CryptoLocker approach has since been widely copied by hackers, although the variants in operation today are not directly linked to the original. The word CryptoLocker has become almost synonymous with ransomware, just like Xerox and Kleenex in their respective worlds. Cryptolocker is one of the examples of ransomware being targeted by Comodo. Comodo has a unique feature that when it reaches the computer automatically protects the user from CryptoLocker. The changes made by CryptoLocker are reversed in real time and are removed by the removal tool for ransomware. Cryptolocker is known to encrypt the files of the user and requires a payment to open them later. Comodo creates a hard drive shadow version to protect the important files from CryptoLocker immediately. It tricks the malware that it has infected the files when in fact only the shadow version has been encrypted.

Fig 4: Crypto-Locker

Wanna Cry:

The WannaCry ransomware attack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency, was a May 2017 global cyberattack. It propagated through EternalBlue, an exploit developed for older Windows systems by the U.S. National Security Agency (NSA), released a few months before the attack by The Shadow Brokers. While Microsoft had previously released patches to close the exploit, much of the spread of WannaCry came from organizations that had not applied these or used older Windows systems that had gone past their end-of-life. WannaCry also made use of backdoor installation on infected systems.

Fig 5: Wanna Cry Ransomware

LeChiffre:

Le Chiffre,' which comes from the French noun 'chiffrement' meaning' encryption,' is the main villain in Casino Royale novel by James Bond who kidnaps Bond's love interest in luring him into a trap and stealing his money. Unlike other variants, on the compromised system, hackers must run LeChiffre manually. Cyber criminals scan networks automatically in search of poorly secured remote desktops, logging in remotely and running a virus instance manually. If you have Comodo Advanced Endpoint Protection, LeChiffre will never infect your personal or business network. To install more malware and viruses on computers, LeChiffre is used to attack vulnerable networks. Comodo has multiple security layers that prevent this ransomware from protecting your network. If one of the devices connected to the network becomes vulnerable to malware, the information will be transmitted remotely to immediately block the malware on other devices.

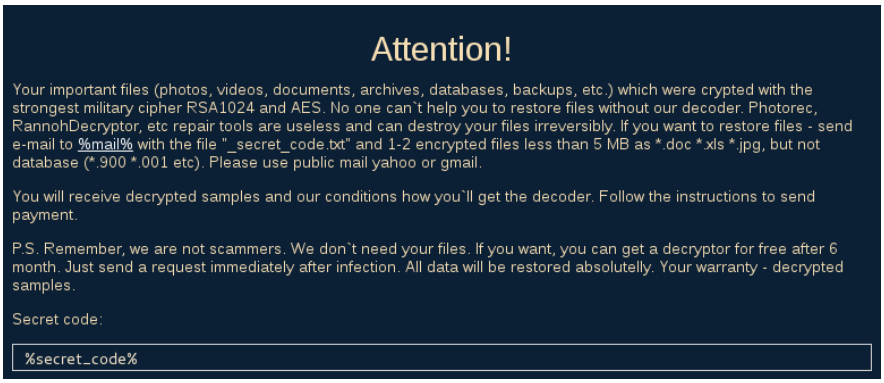

Fig 6: LeChiffre Ransomware

Jigsaw:

Jigsaw encrypts files and deletes them gradually until a ransom is paid. After the first hour, the ransomware deletes a single file, then deletes more and more per hour until the 72-hour mark is deleted. Jigsaw is another of those examples of ransomware that Comodo Advanced Endpoint Protection has already rendered useless. Jigsaw can encrypt and remove files. It first encrypts the files and deletes them if the user does not pay the ransom after an hour. Comodo has the ability to protect your files and reverse the malware's damage. You never have to worry about losing your files with Comodo Advanced Endpoint Security because it provides real-time protection against ransomware for your personal data.

Fig 7: Jigsaw Ransomware

Petya:

Petya encrypts entire computer systems, unlike some other types of ransomware. The master boot record is overwritten by Petya, which makes the operating system unbootable. Is another of those dangerous examples of ransomware which by overwriting the original data can destroy the operating system. Petya infects the computer system as a whole. Your computer system is safe, however, with Comodo Advanced Endpoint Protection.

Fig 8: Petya

ZCryptor:

ZCryptor is a self-propagating strain of malware that displays worm-like behavior, encrypts files, and also infects external drives and flash drives so it can be distributed to other computers. Comodo has the best defense against ZCryptor -a self-replicating malware that infects the USB drive and the computer. ZCryptor is spread through software installers that are spam or deceptive. Comodo Advanced Endpoint Security can detect any malicious files hidden in an infected program immediately. Comodo has the best defense against ZCryptor -a self-replicating malware that infects the USB drive and the computer. ZCryptor is spread through software installers that are spam or deceptive. Comodo Advanced Endpoint Security can detect any malicious files hidden in an infected program immediately.

Fig 9: ZCryptor Ransomware

4.ENCOUNTERING RANSOMWARE

There are two common ways ransomware can be found:

- Via files or links delivered via emails, instant messages or other networks
- Other threats, such as trojan downloaders or exploit kits, downloaded to your device (Gonzalez et.all) [8].

4.1. Delivered by files:

Users most commonly contact ransomware through files or links distributed in email messages:

- The email message contains links to online saved' documents.' In fact, the documents are executable programs (the crypto-ransomware itself)
- The emails have files attached to the device that download crypto-ransomware.
- Microsoft Word document (file name ends with.doc or.docx)
- Microsoft XSL document(.xsl or.xslx)• XML document(.xml or.xslx)
- Zipped folder containing a JavaScript file(.zip file containing a.js file)
- Multiple file extensions (e.g., < INVOICE#132435>.PDF.js)

4.1.1. Tricking the recipients

Receiving the email itself does not trigger an infection; it would still be necessary to download or open the attached or linked file. Attackers often use social engineering tricks to craft email messages to attract recipients to open links or attached files. For example, they use legitimate companies ' name and branding, or texts that are intriguing or legally sounding.

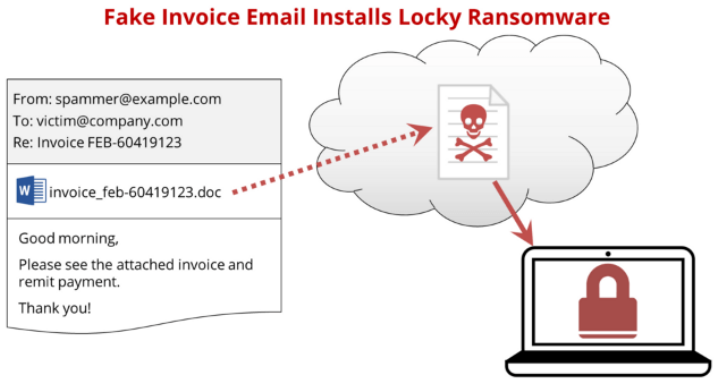

Fig 10: Ransomware via mail

4.1.2. Opening the attachments

If the opened file is JavaScript, a remote website or server will attempt to download and install the crypto-ransomware itself. If the attached file is a document from Microsoft Word or Excel, it embeds harmful code as a macro in the file. Even if this file is opened by the user, the macro can only run if there is one of the following conditions:

- Macros are already enabled in Word or Excel
- Macros are disabled by default in Microsoft Office. When the file is opened, if they are enabled, the macro code will run immediately. If macros are not enabled, a notification prompt will be displayed in the file asking

the user to activate them. If the user clicks ' Enable Content,' macros will be enabled and the embedded code will run right away.

4.2. Delivered by Exploit Kits:

Exploit kits can also deliver ransomware, which are toolkits that website attackers plant on. There are numerous exploit kits currently supplying wild ransomware such as Neutrino, Angler and Nuclear. These kits test the device of each website visitor for flaws or vulnerabilities that they may exploit. The exploit kit can immediately download and run crypto-ransomware on the device if a vulnerability is detected and exploited.

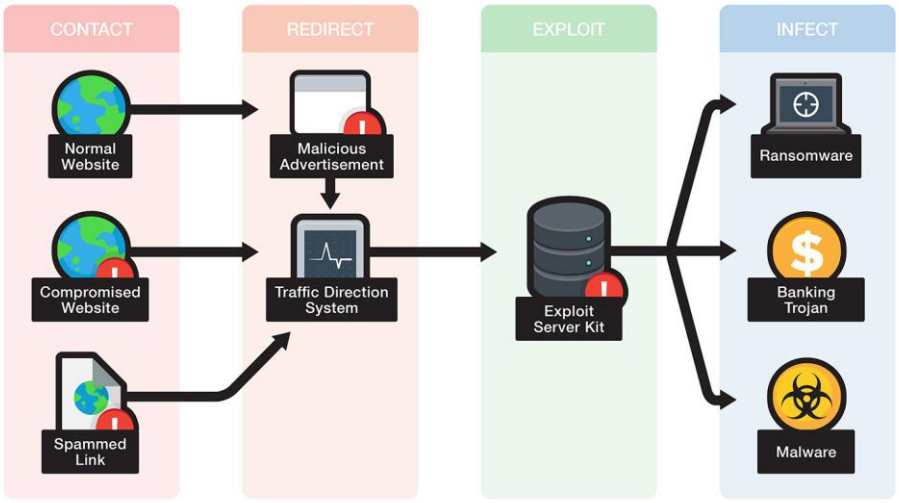

Fig 11: Exploit Kits

5. WHETHER TO PAY OR NOT?

Ransomware works on the assumption that the user is uncomfortable enough to lose access to the files that they are willing to pay the requested sum. Security researchers and law enforcement agencies generally strongly advise victims not to pay the ransom. However, the crypto-ransomware infections were so disruptive in some reported cases that the affected organizations and users opted to pay the ransom to get back access to the data or device (Everett et.all) [9].

6. RESPOND & RECOVERY

6.1. Response:

If the worst thing happens and crypto-ransomware infects your device, you can take a few steps to contain the damage:

- Immediately disconnect the device or devices affected from the local network and/or the Internet. This does not spread the infection to other connected devices.
- Scan for similar flaws and additional threats all connected devices and/or cloud storage. Not only should the same threat check other connected devices and storage media for infection, but also any other threats that might have been installed on the side.

• Identify the specific responsible ransomware if possible. Knowing the specific family involved makes online searching for remedial options information easier[10].

6.2. Recovery:

The following measures can be taken in order to recover the original data:

• Format and reinstall the device if possible. This is usually the most expedient way to remove an infection with ransomware. There are removal tools available for specific ransomware families in a small number of cases (see Family-specific removal tools below), which you may consider as an alternative. Recover clean backup data. If available and clean, by restoring data from backup files, the encrypted data can be recovered. In cases where no decryption is possible, this is the method recommended to avoid paying the operators responsible for crypto-ransomware by law enforcement authorities and security experts.

• Reassess the security of any installed software. Assure that any installed software (including the operating system) is up-to-date with the latest security patches to prevent recurrence.

• Report the incident to the local law enforcement authority concerned. Each country handles electronic crime incidents differently, but most national law enforcement agencies generally urge affected individuals or businesses to report incidents and avoid paying any demanded ransom[10].

7. PREVENTION

To avoid becoming a victim of crypto-ransomware, the following precautions can be taken:

• Save all necessary files regularly and store them in a location that is not connected to the computer or network. This means you always have unaffected backups available even if your computer is affected.

• Apply to all installed operating systems and applications all critical and important security patches. This prevents scenarios where the attack vector is not just attachments to email files, but exploits attacks on vulnerability.

• Enable all the security features of your antivirus solution and keep it up-to-date with the latest database signature.

• Do not open emails sent by an unknown sender, particularly if they contain an attachment or a link.

• Activate "Show hidden files, folders and drives" and disable "Hide known file types extension." This helps you to spot multi-file extension files.

• The settings in Office 2016 should block macros from running in documents from the Internet at all. In response to the resurgence of macro malware, this new feature has been added.

REFERENCES

[1] Nirav Bhojani, “Malware Analysis”, ResearchGate, October 2014.

[2] C. Miles, A. Lakhotia, C. LeDoux, A. Newsom, and V. Notani, “Virus battle: State of-the-art malware analysis for better cyber threat intelligence,” in Resilient Control Systems (ISRCS), 2014 7th International Symposium on. IEEE, 2014, pp. 1–6.

[3] P. Black and J. Opacki, "Anti-analysis trends in banking malware," in Malicious and Unwanted Software (MALWARE), 2016 11th International Conference on. IEEE, 2016, pp. 1–7.

[4] D. Plohmann, K. Yakdan, M. Klatt, J. Bader, and E. Gerhards-Padilla, "A comprehensive measurement study of domain generating malware," in USENIX Security Symposium. USENIX, 2016, pp. 263–278.

[5] Arun Lakhotia, Paul Black, "Mining Malware Secrets", IEEE, 2017, pp. 11-18.

[6] D. O'Brien, "Ransomware 2017", Internet Security Threat Report, Symantec, July 2017.

[7] K. Savage, P. Coogan, and H. Lau, "The Evolution of Ransomware", Security Response, Symantec, June 2015.

[8] Daniel Gonzalez, Thaier Hayajneh, "Detection and Prevention of Ransomware", IEEE, 2017, pp. 472-478.

[9] C. Everett, "Ransomware: To pay or not to pay?," Computer Fraud & Security, vol.

4, pp. 8-12, April 2016.

[10] McAfee Labs, "Understanding ransomware and strategies to defeat it" White Paper,

2016.