ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 3, Issue 7, DOI: 10.29027/IJIRASE.v3.i7.2020, 490-497, January 2020

Ransomware Attack and Remedial: A Survey

[1]L.A. Kong, [2]K.N., Yeo, [3]R.X., Ng, [4]S.H. Kok
Taylor's University, 47500 Subang Jaya, Selangor, Malaysia
[1]lousekong8@gmail.com
[2]yeokainee@gmail.com
[3]rueyxin.nrx@gmail.com
[4]koksimhoong@sd.taylors.edu.my

***Abstract* –Ransomware is a type of malware that deny user access to its own system and demands payment before the system is restored. According to Cybersecurity Ventures, ransomware harm expenses will reach $11.5 billion by 2019. That figure is up from 2015's $325 million and 2017's $5 billion. There are primary two types of ransomware attack; namely locky and crypto. Locky-ransomware locks the victim from accessing to its computer, while crypto-ransomware encrypts its victim's important files. Crypto-ransomware is considered to be more dangerous, as the effect is irreversible, even after removing crypto-ransomware from the system. This is because all encrypted files remain encrypted without the decryption key. The existing contributions that use to protect the system from ransomware are strengthening the security system, backup the data regularly, keep the system updated and so on. However, most of the method that mention above are the general way to prevent the system from ransomware. In this report, we will discuss in more detail about the latest ransomware attacks. We also look as the most common infection vector used by ransomware to infect its victim. Then we provide recommended remedial to deal with ransomware attack**

***Index Terms* – Crypto-currency, Cyber security, Encryption, Malware, Ransomware**

I. INTRODUCTION

A ransomware attack can be described as an effort to extort an organization by denying their access to its own database. Ransomware is considering as a type of malware that is a collection of all types of malware which including computer viruses and worms[1]. Ransomware often sneaked into the user's computer as computer worms or Trojan horses that exploit open security vulnerabilities. This type of attack will deny user access to their own system by encrypting the system on affected computers and then demands payment before the system are restored. Unlike other types of cyber-attacks, the victim of ransomware is usually be announce that an exploit has occurred in their computer and gives instructions on the way to recover from the attack. Payments are usually in virtual currency (e.g. Bitcoin) so that the identity of the cybercriminal will stay unknown[2].

There are multiple ways that can allow the attacker take access to a computer. Ransomware often appears and delivery through spear-style email. After the user has been locked out from the data or system, a ransom payment is requested by the cybercriminal. The cybercriminal allegedly provides the victim with an opportunity to regain access to the system or information after receiving payment [3]. There is other more aggressive ransomware which using the security vulnerabilities of computer to infect the computer without deceiving users. Ransomware can also be delivered on malicious website through drive-by-download attack. Some of the ransomware attacks were even sent by using social media messages.Ransomware: Recent Ransomware Attack Method and Way to Prevent it Based on U.S. Government interagency technical guidance, ransomware is a form of malicious software which used by cybercriminal to denies user access to their system and data for the purpose of extortion[3]. According to statistic from the U.S. government, the amount of ransomware assaults raised by 300% compare to the year before in 2016, which is more than 4,000 attacks identified per day. Ransomware is the worst kinds of infection among all the other cyberattacks as it not only encrypts network information, but ultimately all the information maybe lost even if the user pays the ransom [4]. Ransomware lifecycle is as shown in Figure 1 below, where it can enter its victim's system through various infection vectors.

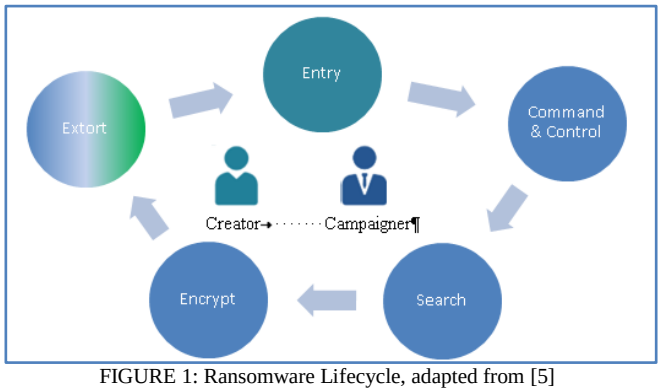

FIGURE 1: Ransomware Lifecycle, adapted from [5]

One of the primary and most common ransomware distribution channels is through huge spam campaigns that are malicious. This spam is spread using compromised computer networks, ranging from hundreds to millions of infected computers to send out large number of spam emails to the public. When a person opens the email or clicking the link that are provided in the email, malicious software might be install in the person's computer. Email was the dominant source of ransomware during 2016, with well-resourced botnets pumping out millions of spam messages every day. Although it remains a significant danger during 2017, in the first half of the year malicious email retailers encountered

ISSN(Online) : 2456-8910
International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE)
Volume 3, Issue 7, DOI: 10.29027/IJIRASE.v3.i7.2020, 490-497, January 2020

some disturbance, meaning that activity is behind 2016 rates[6]. Other than that, exploit kits also one of the common and popular tools that used by hacker until today. Exploit kits operate by taking advantage of software vulnerabilities to install malware. Exploit kit attackers compromise web servers from third parties and inject iframes into their web pages. The iframes are directing browsers to servers of the exploit kit. Attacker can redirect the user to the exploit kits in different ways like give a malicious links in spam emails or social posts, advertisements and redirected web traffic from traffic distribution services. There is also ransomware that use self-propagation like new versions of WannaCry and Petya used self-propagation to have a drastic impact. They were not the first ransomware families to use this method, and ZCryptor (W32.ZCrypt) had earlier used it to infect all removable disks with a copy of itself before starting to encrypt documents. A number of Android ransomware families also show worm-like conduct by distributing SMS messages to all contacts in the address book of a device [6].

Attackers were also seen targeting susceptible server software to obtain access to the network of an organization. Normally prominent websites are the prime target [7]. The gang behind the SamSam ransomware is using free instruments to identify and exploit vulnerabilities to spread their malware across the network. Furthermore, the ransomware family of LinuxEncoder targets Linux web servers. In website plugins or third-party software, the attackers exploit vulnerabilities to infect victims. Linux Encoder then encrypts website-related directories, rendering any website hosted on the desktop concerned[6].

II. TYPES OF RANSOMWARE

There are mainly two types of ransomware attacks in circulation today as shown in Figure 2 below:

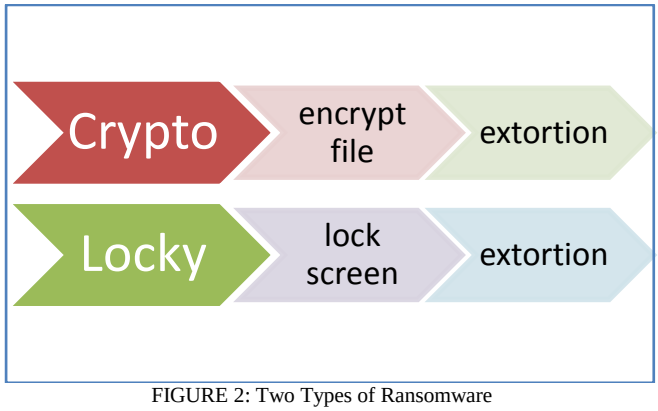

FIGURE 2: Two Types of Ransomware

1. Locky-Ransomware

Locky-ransomware rejects entry to the machine by shutting the devices and enabling individuals to communicate with the malware only. Besides that, locker ransomware typically keeps the documents on the desktop unmodified so that individuals can view the documents again after the malware has been withdrawn. Hence, IT organisations and sophisticated individuals have a stronger opportunity of restoring the machine from locker ransomware attacks than from other types of assault. This sort of ransomware often pretends as law enforcement officials and requests to impose penalties to individuals for suspected internet indiscretions or criminal operations[8].

Locker ransomware exists for a multitude of applications with distinct kinds of operating systems such as Microsoft Windows, Linux, OS X, Android etc. Some of the samples discovered in other research paper and throughout the web search were Lockdroid, SimpLocker, etc., and are ransomware[9]. For example, this locker ransomware can develop more and more by joining Internet of Thngs (IoT), assuming an intelligent car that does some of its activity likes opening and locking doors. If it is corrupted, it may be out of reach and the individual must settle the ransom to open it. In the light of the latest rise in wearable electronics and the IoT, millions of linked machines could possibly be in danger from such a ransomware. This is a possible issue zone.

2. Crypto-Ransomware

Crypto-ransomware encrypts precious information on devices without alerting the customer or administrator — then the documents are useless. A crypto program runs secretly on a computer system to encrypt as many records as necessary without excessively impacting the operating system. Most individuals will proceed to use the machine until a notification of extort is submitted demanding compensation, without knowing that the ransomware is working. In addition, many people perceive it as a sophisticated assault that is difficult to prevent because of its stealthy design and catastrophic consequences. There are many pathways leading to an infection of ransomware. Some of them include Traffic Distribution System, Malvertising, SPAM mail, Downloaders and botnets, and Social Engineering.

After the setup, a crypto-ransomware search and encrypts records silently. It is intended to remain under the radar until all the files that can be of value to the user can be found and encrypted[8]. By the moment you receive the malware signal informing you that your information is encrypted, the harm is already achieved where people are responsible for paying the ransom money.

III. RANSOMWAREFAMILIES

1. WannaCry

WannaCry is a cryptoworm ransomware which targets the machines that running the old version Microsoft Windows operating system by encrypting the information

and requesting Bitcoin cryptocurrency ransom payments form the victims. On May-June 2017, the WannaCry Ransomware cyber-attack has occurred in wide range which affected more than 300,000 systems in over 150 countries. This attack has result in the lost up to $1 billion in one-week time[10]. All the machines that are targeted by WannaCry are the machines that using the older version of Microsoft Windows operating systems. This malicious software contains a URL and the victim's system will gets infected with phishing messages. Besides that, WannaCry spreads through SMB (Server Message Block protocol) operating ports 445 and 139, which is used by Windows computers to interact over a network with file systems. Once WannaCry is successfully installed, the ransomware will scan for the system in the device in order to find is there have any backdoors that are available in the machine. The two main technics that use by WannaCry are DoublePulsar and EternalBlue to exploits the SMB [11]. Microsoft has reacted to the gravity of the situation since the assault by issuing safety updates to older versions of Windows that are usually unsupported.

Based on the news there were a real incident which happen in Taiwan,where a company that name Taiwan Semiconductor Manufacturing Company (TSMC) has to temporarily shut down some of its chip-fabrication factories due to the WannaCry has spread to 10,000 machines which us the most advanced facilities in TSMC [12]. There has no report of anyone that getting back their file after did the payment to WannaCry hacker.

2. Ryuk

The Ryuk ransomware virus is a new form of ransomware that was first released in August 2018 and has since been used by unidentified performers online in a targeted attack system. The evolution of the attack took shape to imitate some of the methodologies used by the SAMSAM group (Iran) to locate vulnerable companies through recognition and phishing to achieve a foothold in their assault as the first stage. The Ryuk performers then intensify the incursion by loading the ransomware on the company's servers and thus totally shutting it down from the daily business. There are two way that Ryuk can obtain access to inner networks. The first method is using phishing to infect EMOTET systems and then pivoting laterally to obtain access. The other method is using Shodan and other instruments to locate open RDP sessions and exploit sensitive systems online to escalate the attack. The second phase of the attack in both attack vectors is to use the acquired access to reconnect the org to find devices (servers) for Ryuk infection. The Ryuk infection will then encrypt all information, delete copies of shadows, and leave a message that the systems have been encrypted and where bitcoins can be sent.

Bitcoin transfers from impacted organizations have accumulated about $2,680,077.93 in the malware campaign form the past few years. The average demand for cash per assault is based on the tolerances of the organizations and judged by the performers to assess what they can afford. The Ryuk ransomware has a low data recovery-success rate after the ransom payment is made and the incidents will be much longer than other kinds of ransomware due to demanded elevated ransom quantities and the decryption tool's labor-intensive nature [13].

3. LockerGoga

LockerGoga is the latest form of ransomware which is targeted and more destructive. Interestingly, both ransomware and wiper capacities appear to be available. Later variants of LockerGoga forcefully log victims off the infected device, often resulting in victims being unable to see the ransom message and file recovery guidelines. This is a very distinct approach to typical ransomware, which only encrypts some files on a computer. LockerGoga is a newly made headlines ransomware owing to its disruptive impacts on the networks of industrial and manufacturing companies. The latest victims include Norwegian aluminium manufacturer Norsk Hydro, French consultancy company Altran, and U.S. chemical firms Hexion and MPM Holdings. The ransomware does not target or infect ICS systems, but its weakening impacts on the networks of company and manufacturing linked to these industrial systems lead to expensive downtime manufacturing[14].

It caused manufacturing networks to be temporarily shut down, forcing businesses to turn to manual activities and processes. The economic effect is estimated to be between US$ 35 million and $41 million for one of the biggest objectives, Norsk Hydro. Operator placement was most probably needed, with malicious threat actors observed from LockerGoga shifting the payload around the network using SMB. The actors also used Active Directory management services in some incidents to distribute the payload in the network. The method that it uses to launch the attack are unconfirmed which it may using a phishing email campaign with specially designed Microsoft Word files or macro / OLE content RTF attachments [15]

4. Sam Sam

SamSam is specialized in focused assaults on ransomware, breaking into networks and encrypting various computer across an organization before issuing a demand for high-value ransom [16]. During a past wave of SamSam assaults in 2016 and 2017, people notice that the attacks were made on objectives through susceptible JBoss host servers. Recently, SamSam will use either vulnerabilities in remote desktop protocols (RDP), Java-based web servers, or file transfer protocol (FTP) servers in order to gain access to the victim's network or even brute force against weak passwords to get an original foothold [17].

SamSam has assaulted a broad variety of U.S. based sectors which mostly critical infrastructure such as hospitals, healthcare firms, and municipalities. Organizations that provide vital tasks need to swiftly resume activities and are more probable to pay bigger ransoms. Last year, the SamSam attack crippled Atlanta City for days and costing taxpayers nearly $17 million. By pursuing the cash and monitoring the Bitcoin payment wallets with the assistance of Neutrino (a company specializing in monitoring cryptocurrency flows), Sophos scientists estimated that the SamSam attacker had netted more than $5.9 million since version 1 which is late 2015 and started to be used in January 2016. They also estimate that, the attacker is raising an average of $300,000 per month in the future [18].

5. Petya/NotPetya

Petya is a ransomware encryption family that first found in 2016 [19]. The malware targets systems that are using Microsoft Windows by infecting the master boot record to execute a payload that encrypts the file system table of a hard drive and prevents the booting of Windows. It then requires the user to create a Bitcoin payment to regain access to the scheme. This malware was not intended for financial benefit as a ransomware assault. Instead, it was intended to be damaging as a wiper that pretending to be ransomware. It wipes the computer directly and destroys all documents of the targeted system called wiper malware.

The first infections of Petya started to spread throughout Europe, especially in Ukraine, where the threat was experienced by more than 12,500 machines. In 64 other nations, including Belgium, Brazil, Germany, Russia, India, and the United States, infections were then noted. It has influenced many critical systems, organizations, airports, banks, and departments of government which has cost the organization $1.2 billion in revenue [20]. There are not possible to have a decryption key as it generates a random ID for each computer. Even if the victims pay the ransom, their files that have been encrypted will never be recovered. The virus may have spread to a Ukrainian tax accounting scheme called MeDoc through a malicious software update. MeDoc was infringed and the virus spread through updates [21].

6. Cryptolocker

Cryptolocker is a Trojan ransomware targeted at Microsoft Windows and circulated since the end of 2013. It is usually propagated as an extension to an apparently harmless e-mail notification that a lawful business happens to have sent.

In addition, Tor network is usually used for anonymity, 2048-bit encoding protocol for extortion and Bitcoin for billing techniques. Though due to the symmetrical buttons that are positioned on C&C computers, its existence could not be sustained, it paved the door for fresh ransomware development with its origin software. CryptoWall is the most popular, with over half of the total number of ransomware available by 2015 [22].

For example, an executable file with the filename and icon disguised as a PDF file contains a ZIP file attached to the email message [23]. The sender has named his / her document with a ".pdf" (Windows covers the.exe) with Window's concealed links function, and the unintended person is tampered in believing that the connection is a safe, trustworthy, PDF file. If a file is found supporting this expansion, then a public key is used to encrypt the document and track the document in the registry of Windows. It then prompts the individual his or her documents were encrypted and needs to submit hundreds of bucks to the malware creator to get back and open the documents.

7. Cryptowall

CryptoWall is a class of ransomware file encryption that first emerged at the beginning of 2014. The use of unbreakable AES encryption, distinctive method for CHM infection, and strong C2 operation over the Tor private network is noteworthy. The miscreants operating the CryptoWall procedure also provide a private one-use decryption facility to demonstrate that they retain the keys needed to restore the hijacked documents.

One fresh "function" was presented by CrytpoWall 4.0, published in late 2015: it encrypts the filenames of the documents it encrypts to make it more difficult for the recipient to understand what has been encrypted. The ransomware is distributed through a multitude of techniques, including email attachments that are meant to arrive from financial institutions, packages that utilize vulnerabilities in user software when visiting fake web pages, and web pages that show false advertisements.

8. TeslaCrypt

TeslaCrypt is one of the latest kinds of on-scene ransomware. It utilizes an AES algorithm to encrypt documents like other types of ransomware. It is typically distributed to specific vulnerabilities of Adobe through the Angler exploit package. TeslaCrypt installs itself in the Microsoft temp folder once weakness is accessed [24].

It uses Angler to exploit Adobe Flash (CVE-2015-0311) and downloads TeslaCrypt as a payload once it has been effectively utilized. Angler is utilized from the altered page via an inserted iframe. It redirects to a heavily obfuscated landing page, includes anti-vm methods, and monitors the existence of anti-virus software or malware assessment instruments such as fiddler etc. It includes de-obfuscation script on the same internet site for each obfuscation code.

Once all terms have been fulfilled, Flash application will be downloaded by decrypted URLs which will then retrieve the ransomware payload from the temp folder. It also decodes the stored payload using Xtea algorithm. We also saw attacks associated to Silverlight and Internet Explorer in addition to the Flash vulnerability. Angler does not use the file less payload method but incorporates the ransomware payload into the device.

IV. INFECTION VECTOR

1. User download the malware unknowingly

[25] mentioned that user might download or run malware document on their computer without their attention. [26] stated that malware document might be downloaded from the drive by download or when they click on malicious link. Drive-by-download has a meaning of malware that pushes malicious code on a client system and execute it without user's concern. There are plenty of messages that used to divert attention of the user, so he/she can click on the link, unknowingly download the malware to the computer system, such as the popping screens, animated pop-ups etc. It is normal if the user has no idea about the code being run at the background [27]. For example, when an individual accidentally click on certain link, which causes some file to be downloaded and the file will initiate its program once it was being executed.

2. People/User does not patch its system

Most user and enterprises do not enable auto update in their workstation. Some of the individual lack of the knowledge of importance of keeping their device patches. As well as some enterprise, they do not auto update the patches, this is because before the enterprise push that patch to every single workstation. They chose to test the workability of the patches for 2 weeks to 2 months. This had result in most of the enterprise had always behind the patches updates. A software without patches stay highly vulnerable to attackers. Attackers are more likely to start attack user which their system security has not patch to the latest version of patches.

3. E-mail as an infection vector

One of the primary delivery platforms is huge spam campaign for ransomware. This spam is spread across hundreds to millions of affected pcs with botnets-an affected computer network. Many of these botnets can send spam on a massive scale every day, most of which apply easy social engineering techniques to lure recipients into destroying their devices[5].

4. Macros as an infection vector

Ransomware can also be spread via Office Word document which contains a macro. Users are encouraged to enable the macro function to see more information. However, if the user enabled this function, the macro will get extra payload that bypasses the old security tools by downloading the encrypted data and decrypted it on the infected computer. Distributing malware via macros is a very traditional method, and probably one that has been unpopular for years.

5. Malvertising

Next attack vector why people are still vulnerable to ransomware is because of malvertising. For example, potential victims who access legitimate sites that display advertisements provided by third-party ad networks. If malicious code is integrated in one of the advertisements in that site, unpatched vulnerabilities in user's browser will be exploited to download ransomware. This kind of attack, however, is less likely to be effective. This is due to the reason it depends on the unpatched vulnerability in user's browse, but it has an advantage of no action needed to be taken on the victim's side if they are susceptible to the attack

6. Exploit kits

Exploit kit is a useful program that used by attackers to initiate exploit against vulnerable program. They function as repositories, rendering it simple to leverage this weakness for customers who do not have much technical understanding.

V. REMEDIAL STEPS

1. Endpoint Protection

a. Keep current with patching

The exploitation of the endpoints will be minimized if a operating system and application system is fully patched. The organization should have a procedure to guarantee that the system is well managed and regularly patched.

There are many kind of new ransomware variant recently, system upgrading should be done on time It is worth reiterating as a security risk study from HP in 2016 discovered that 44% of effective ransomware attack were created by software that had not been patched for two to four years. The privilege escalation is often feasible through the exploitation of known but unpatched vulnerabilities. One real life example is, the 2017 WannaCry ransomware, it took the advantage of unpatched Microsoft Window vulnerability.

b. SPAM filtering

Endpoint-level SPAM filtering is also workable and having different filtering solutions on the endpoints can help increase the chances of detecting spam and malicious email bypassing perimeter defences. This is crucial because some ransomware variants like Locky are usually spread through malicious email attachments.

c. Disable Support for Macros

Macro-enabled Word documents and PDFs are a problem because they are easy to write in order to generate arbitrary code to run on a machine. This Macro script is the first component of a string of infections that consists in the deployment of ransomware on machines. Macros in pdf and.docx files enable the execution of harmful code run easily in the system.

2. Backups
a. Backup using 3-2-1 backup method

One of the ways to prevent user from ransomware attack is using the 3-2-1 backup strategy. A 3-2-1 backup strategy is to have 3 copies of every critical file, two of which are on two different media or different physical device while another one is stored at an air-gapped from network Air-gapping isolate your business' data so that there is no other way to access it. This form a 'gap' in between your data and your backed-up data, which helps in prevent the data in falling to hacker's hand. If there's an attack attacking your organization, at least the air-gapped backup data is still safe

b. Educate employee

Organization should educate employees handle each email carefully. The best practice is to treat every single email as a potential malicious email unless it has proof to prove its not. Then, employee should know how to check the source of every email. Check if there is any simple or obvious grammar mistake in the content. Practice and learn to hover over links to observe the URL.

3. Network Defence
a. DNS Sinkhole

The DNS sinkhole is designed to prevent the host name of the specified URL from being resolved. It was used to pass error messages to specific URLs. It is used to provide incorrect DNS resolution and direct users to different resources instead of accessing malicious content.

b. Network Intrusion Detection System (NIDS)

NIDS is a tool that monitors network packet to look for possible malicious activities. This tool is normally situated outside the network that allows in-depth analysis to be carried out without causing lag to the network. Many researcher are using machine learning algorithm in IDS for detection of unknown ransomware [28].

4. Incident Response:
a. Setting-Up an Incident Response Plan.

The development of incident response plan (IRP) is important to ensure the efficient use of backup solutions. This includes provide training to the employee to identify the type of ransomware attack and also the tasks and duties for each employee during a ransomware attack.

b. Testing Your Ransomware Protections.

It is essential to check your company's ransomware security every 1 week to prevent ransomware attack. One of the greatest approaches for avoiding ransomware attacks consists of regularly testing to avoid or rebound from them. This helps to define single error spots or other problems, so you can solve them before ransomware hits. In addition, ransomware is equally harmful for the internet of things, smart homes, cellular networks, and other networks including wireless sensor networks, E-health IoT based applications as well [29-34]. Furthermore, ransomware makes easy target cyber security application as well as to the smart phone applications [35-37], including Android and IOS based applications.

VI. CONCLUSION

In our opinion, we believe that ransomware is a permanent danger to computer networks. The economic retribution is so big for the attacker that other malware forms will decline as the new normal ransomware. The computer industry is now responsible for sounding the alert and thus increasing our defences. In addition, ransomware assaults have become a global impact, primarily aiming at gaining money through unlawful means. The assault began with e-mails and extended through spamming and phishing. Ransomware encrypts documents and show notifications of objectives, requiring deposit prior to unlocking the information. The request for ransom generally takes the shape of a virtual currency, bitcoin, as it is hard to decipher. Due to the profitability of the illegal law, the types of ransomware began to boost. There is, however, an increasing attempt to reduce the distribution of this malware. A strong knowledge of the conduct of ransomware helps people and companies clean up their vulnerabilities in this type of assault.

REFERENCES

[1] S. Cobb, "Ransomware : an enterprise perspective," 2018.https://www.welivesecurity.com/2018/10/29/ransomware-enterprise-new-white-paper/ Accessed on April 2019

[2] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Ransomware , Threat and Detection Techniques : A Review," *Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 2, pp. 136–146, 2019.

[3] S. M. Burwell, "Ransomware attak is a breach, How to protect your networks from Ransomware," 2016.https://www.bakerdonelson.com/Ransomware-Attack-is-a-Breach--Unless-You-Can-Prove-Otherwise-07-14-2016, Accessed on May 2019.

[4] L. Pascu, "Ransomware attacks increase 300% in 2016," 2017. [Online]. Available: https://businessinsights.bitdefender.com/ransomware-attacks-increase-300-in-2016.

[5] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Prevention of crypto-ransomware using a pre-encryption detection algorithm," *Computers*, vol. 8, no. 4, pp. 1–15, 2019.

[6] J. Danahy, "Internet Security Threat Report: Ransomware 2017," 2017.

[7] S. Kok, A. Abdullah, M. Supramaniam, T. R. Pillai, and I. A. T. Hashem, "A Comparison of Various Machine Learning Algorithms in a Distributed Denial of Service Intrusion," *Int. J. Eng. Res. Technol.*, vol. 12, no. 1, pp. 1–7, 2019.

[8] K. Savage, P. Coogan, and H. Lau, "The Evolution of Ransomware," 2015.

[9] D. A. Herati, A. M. Bojamma, and M. P. I. Gandhi, "Countermeasures to Ransomware Threats," *Bangalore Inf. Secur. Res. Conf.*, no. April, pp. 0–7, 2018.

[10] S. Askarifar, N. A. Abd Rahman, and H. Osman, "A review of latest wannacry ransomware: Actions and preventions," *J. Eng. Sci. Technol.*, vol. 13, no. Special Issue on ICCSIT 2018, pp. 24–33, 2018.

[11] A. Koujalagi, S. Patil, and P. Akkimaradi, "The Wannacry Ransomware: A Mega Cyber Attack And Their Consequences On The Modern India Article in," *Int. J. Inf. Technol.*, no. May, 2018.

[12] M. Kumar, "TSMC Chip Maker Blames WannaCry Malware for Production Halt," 2018. [Online]. Available: https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html.

[13] "Ryuk Ransomware Recovery, Payment & Decryption Statistics," *Coveware*, 2019. [Online]. Available: https://www.coveware.com/ryuk-ransomware.

[14] "LockerGoga," 2019.https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-22nd-2019-lockergoga/ Accessed on Nov 2019.

[15] O. Kolesnikov, H. Parashar, and S. Threat, "Detecting LockerGoga Targeted IT / OT Cyber Sabotage / Ransomware Attacks," 2019.

[16] "SamSam: Targeted Ransomware Attacks," *Symantec*, 2018. [Online]. Available: https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks.

[17] C. Boyd, "SamSam ransomware: what you need to know," *Malwarebytes*, 2018. [Online]. Available: https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/.

[18] "SamSam: The (Almost) Six Million Dollar Ransomware," *Sophos*, 2018.

[19] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[20] CERT-MU, "the Petya," 2017.http://cert-mu.govmu.org/English/Documents/White%20Papers/PETYA%20CYBER%20ATTACK%20-%20CERTMU%20WHITEPAPER.pdf Accessed on March 2019.

[21] PNP, "NotPetya Ransomware," 2017.https://mg.pnp.gov.ph/index.php/11-administrative/64-csb17-02-notpetya-ransomwareAccessed on March 2019.

[22] B. Celiktas, "THE RANSOMWARE DETECTION AND PREVENTION TOOL DESIGN BY USING USING SIGNATURE AND ANOMALY BASED DETECTION METHODS Barış ÇELİKTAŞ Department of Applied Informatics Applied Informatics Programme MAY 2018," no. May, 2018.

[23] H.-T. S. NQ, "CryptoLocker Ransomware. What is it?," 2019. [Online]. Available: http://www.hitechsolutions.com.au/Cryptolocker Ransomware.pdf.

[24] J. Wyke and A. Ajjan, "The Current State of Ransomware," no. December, p. 59, 2015.

[25] A. Ali, R. Murth, and F. Kohun, "Recovering From the Nightmare of Ransomware - How Savvy Users Get Hit With Viruses and Malware: a Personal Case Study," *Issues Inf. Syst.*, vol. 17, no. 4, pp. 58–69, 2016.

[26] J. Glassberg, "Defending Against the Ransom Ware Threat," *PowerGrid International*, 2016. [Online]. Available: https://www.power-grid.com/2016/08/22/defending-against-the-ransom-war-threat/#gref.

[27] J. Zhang, C. Seifert, J. W, and W. Lee, "ARROW: GenerAting SignatuRes to Detect DRive-By DOWnloads," *Proceedings of the 20th international conference on World wide web*, 2011. .

[28] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "A Review of Intrusion Detection System using Machine Learning Approach," *Int. J. Eng. Res. Technol.*, vol. 12, no. 1, pp. 9–16, 2019.

[29] Z.A. Almusaylim and N. Zaman, "A review on smart home present state and challenges: linked to context-awareness internet of things (IoT) Wireless Networks", 25 (6), 3193-3204.

[30] A. Almusaylim, Z., Jhanjhi, N. Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. Wireless PersCommun (2019). https://doi.org/10.1007/s11277-019-06872-3

[31] M. Almulhim, and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications", 2018 20th International Conference on Advanced Communication Technology (ICACT), 481-487.

[32] M. Almulhim, N. Islam and N. Zaman, "A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications", International Journal of Computer Science and Network Security 19 (1), 107-120.

[33] K. Hussain, S.J. Hussain, NZ. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET", International Conference on Computer and Information Sciences (ICCIS), 1-4, 2019.

[34] K Hussain, NZ Jhanjhi, H Mati-ur-Rahman, J Hussain, MH Islam, Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes, Journal of King Saud University-Computer and Information Sciences

[35] S. Jawad Hussain, Usman Ahmed, H. Waqas, S. Mir, NZ. Jhanjhi, and M. Humayun, "IMIAD: Intelligent Malware Identification for Android Platform," IEEE 2019 International Conference on Computer and Information Sciences (ICCIS), Al Jouf, Saudi Arabia, 2019

[36] Adeyemo Victor Elijah, Azween Abdullah, NZ JhanJhi, Mahadevan Supramaniam and Balogun Abdullateef O, "Ensemble and Deep-Learning Methods for Two-Class and Multi-Attack Anomaly Intrusion Detection: An Empirical Study" International Journal of Advanced Computer Science and Applications (IJACSA), 10(9), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100969

[37] Humayun, M., Niazi, M., Jhanjhi, N. et al. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arab J Sci Eng (2020). https://doi.org/10.1007/s13369-019-04319-2