© Universiti Tun Hussein Onn Malaysia Publisher's Office

JSTARD

https://publisher.uthm.edu.my/jstard

Journal of Social Transformation and Regional Development

A Study of Ransomware Attacks: Evolution and Prevention

Aini Khalida Muslim[1*], Dzunnur Zaily Mohd Dzulkifli[2], Mohammed Hayder Nadhim[3], Roy Haizal Abdellah[4]

[1]Universiti Tun Hussein Onn Malaysia,
Parit Raja, Batu Pahat, Johor, 86400, Malaysia

[2]Universiti Tun Hussein Onn Malaysia,
Parit Raja, Batu Pahat, Johor, 86400, Malaysia

[3]Universiti Tun Hussein Onn Malaysia,
Parit Raja, Batu Pahat, Johor, 86400, Malaysia

[4]Universiti Tun Hussein Onn Malaysia,
Parit Raja, Batu Pahat, Johor, 86400, Malaysia

*Corresponding Author

DOI: https://doi.org/10.30880/jstard.2019.01.01.003
Received: March 2019; Accepted June 2019; Available online June 2019

Abstract: Ransomware is a combination of two words, ransomware and software. In other words, ransomware makes it really hard forusers to access all files and data in a computer because it hacks the data and do not allow the users to access the files unless theypay ransom to the hacker. Dr. Joseph Popp is the first person to develop ransomware. Ransomware is known as a global epidemic that attacks all types of organizations using computing infrastructure. Ransomware has undergone various evolutions. Preventive measuresare needed in order to avoid losses especially in business. The purpose of this study is to examine the evolution of ransomware and preventionsagainst it. In this study, the secondary data were collected by using telemetry data by Symantec to track ransomware attacks in certain countries. Samplescame from among top 5 countries that have been declared as the onesmostly infected by Crypto Ransomware and Locker Ransomware infections. The findings of the study confirm that ransomware prevention is really needed in order to avoid the countries from beingcontinuously attacked by Ransomware. The findings in this study can be used as a reference for future researchers who want to conduct further study especially on cybercrimes.

Keywords: Ransomware, Evolution, Characterization, Prevention Measures

1. Introduction

Ransomware can be considered as a serious threat when it comes to protection of information assets. The main targets are internet users. Ransomware hijacks user files, causes difficulties and then requests some funds through extortion for decryption purposes (Bhattacharya & Kumar, 2017). Ransomware can be categorized as malware which can affect the vulnerability of the user's system, allowing the system to be accessible individually and eventually encrypts all the files that have been targeted (Gonzalez & Hayajneh, 2018).

**Corresponding author: ainimuslimkhalida@gmail.com*

The world was initially unprepared to deal with the attacks as it was difficult for to become widespreadthen due to personal computers usage factor and the Internet was still in its infancy. In addition, encryption technology was still limited (Srinivasan, 2017). Ransomware creators and distributors are aware that they could earn a much higherransom when the main targetsare companies and organizations rather than individual users (Richardson & North, 2017). They achieve the goal of gaining more profits through computers at police departments, city halls, schools. Things become more critical when hospitalsare also targeted (Chhillar, 2017).

The affected countries are predictably to be among the top countries of where organizations and individuals have the most money. According to Symantec, the United States is in the top position affected by Ransomware, followed by Japan, United Kingdom, Italy and Germany (Everett, 2016). According to data obtained by McAfee, the victims of the attacks are mostly in North America (44%) and Europe (29%). The growth of the attack is still ongoing and as there isno chance for the culprits to be caught, ransomware becomes very popular (Morse & Ramsey, 2017). Ransomware is getting more dangerous nowadays during this era of digital economy due to the emergence of cryptographic currencies (Srinivasan, 2017). The famous biggest cyber-attacks in history are on Google China, Heart bleed, PlayStation Network and Yahoo. However, the first ransomware was discovered in 1989 and it targeted the health care industry then (Sharma & Verma, 2017). Criminals usually attack small businesses because big firms have more comprehensive networks and backups by technical and support department. These criminals find out that small businesses have huge potential to pay for ransom (Richardson & North, 2017). Some experts highlighted that some victims made the wise decision by not paying the ransom as paying it will become themmore popular targetsas their data will be continuously hacked and the demand for a higher ransom will be imposed (Savage, Coogan& Lau, 2015).

This study analyzed the evolution of ransomware attacks ways to diagnose ransomware. This study will help new researchers by providing them with summaries of previously published research worksthat will aid them to identify research gaps. There are two questions of this study; "What is the evolution occurred for ransomware attacks?" and "How to deal with the rapidly growing ransomware attacks?" Those questions are answered by referring to further literature analysis about ransomware attacks from 2014-2018 and an analysis has been done to analyse the ransomware infections which leads to the needs of ransomware preventions.

2. Background of Study

2.1 Evolution of Ransomware

The evolution of ransomware has been greatly influenced by a range of developments in technology, economy security and culture since 1989 (Savage, Coogan, & Lau, 2015). The first ransomware was detected in 1989 and known as AIDS Trojan or PC Cyborg. This ransomware was developed by Dr. Joseph L. Popp (Richardson & North, 2017). The purpose of the creation PC Cyborg was to ask for ransom from users. Since there were not many users who have personal computers at that time, this ransomware was unsuccessful. Following the failure, cyber-attackers worked harder to develop a more malicious ransomware that can be better executed (Chhillar, 2017). Even though the first ransomware was rather useful, Adam L. Young and Moti Yung made an initiative to introduce the first prototype asymmetric ransomware in 1996 (Gorman & McDonald, 2012). As a result, these prototype ransomwares were found to have some logistical problems on their method of the payment which could risk the developers. Therefore, the developers decided to create a fake antivirus in order to prevent their identity from getting exposed.

The first modern ransomware known as GPCoder was introduced in 2015. This ransomware was spread via spam email attachments that falsely appeared as a job application (Richardson & North, 2017). Users who opened the attachment were required to pay for the ransom. Other than that, Locker ransomware attacked users' operating systems that forced the users to make payment via SMS text messages or call a premium-rate phone number. During this period, cybercriminals switched their targets from individual users to giant companies because they aimed to get huge ransom. In addition, Satoshi Nakamoto invented a payment system known as Bitcoin in order to improve the payment methods. Bitcoin has since become the new cyber currency payments (Nakamoto, 2008). Majority of the victims would pay the ransom by using bitcoin especially when infected by certain ransomware such as CryptoLocker, CryptoWall, Virloc and TorrentLocker.

The most famous piece of ransomware is known as CryptoLocker and it was developed by a hacker named Slavik (Richardson & North, 2017). The functions of CryptoLocker are to encrypt and later decrypt the user files. This ransomware gives user three days to pay the ransom and the payment can be made by using Bitcoin. KeRangerransomware and Xbot attack started to invade mobile devices and target Apple and Android users. This version of ransomware was dangerous to a giant company like Apple because it could adversely affect the company's productivity and sales. KeRanger takes only three days to activate the files and then encrypt more than 300 file types (Richardson & North, 2017). Therefore, Apple has to release an update in order to block the KeRangerransomware.

Since its first appearance, ransomware has consistently grow and evolve to inflict more damages in the cyberworld (Chhillar, 2017). Ransomware has shown a tremendous progress until today.

3. Theoretical Foundation

3.1 Types of Ransomware

Ransomware is known as the most popular Cybercrime in the world (Krunal, 2017). Generally speaking, ransomware is a category of malware that spreads like a worm and inhibits or limits users from accessing their system either by locking the systems screen or encrypting and locking users' files unless after ransom is paid (Deo and Farik, 2015). There are several types of ransomware and they have been categorized into three basic types. According to Yaqoob et al., (2017), the three basic types of ransomware are known as Crypto Ransomware, Locker Ransomware, and Hybrid Ransomware. The first type of ransomware is Crypto Ransomware. Another name for this ransomware is encrypting ransomware. This ransomware deals with complex algorithm and it blocks users from accessing specific files. Users need to pay ransom by using bitcoins in order to decrypt the data. There is another type of encrypting ransomware which is called WannaCryransomware. This ransomware is a modern ransomware which encrypts certain files types in the infected systems and forces users to pay ransom through certain online payment methods to get a decrypt key (Deo & Farik, 2016).

The second type of ransomware is Locker Ransomware. Locker ransomware is a type of malware that locks the target out of the operating systems and prevents access to the target desktop, applications and files (Shah & Farik, 2017). This ransomware is different from Crypto ransomware as it spams messages to users with malicious attachment. The locker ransomware attacks will occur when users are surfing the internet such as watching movies. The ransomware then displays a malicious message in user computer. The criminal then will demand for a ransom. The most popular example for Locker ransomware is Winlocker. The third type of ransomware is Hybrid ransomware. This ransomware is the most aggressive ransomware as it uses all possible means to maximize profits. According to Yaqoob et al., (2017), Hybrid ransomware that attacks and causes encryption and locks mechanisms, is more dangerous because it will cause data and device functionality to be compromised. Indeed, Hybrid ransomware attacks can be more violent to users as they can possibly target Internet of Things (IoT) devices and systems and also cause physical damages to users until the ransom is paid.

Other than that, there are other types of ransomware that are also dangerous because they use government officers' identity and they are called Reveton or Police Ransomware. According to Pathak & Nanded (2016), criminals will impersonate themselves as local police by showing a notification page to inform victims that they have been caught doing an illegal or malicious activity online that require them to pay fine as a punishment.

3.2 Ransomware Phases

Ransomware has been emerged and declared as a potentially devastating class of cybercrime. Ransomware attacks occur when attackers download malicious software which prevents users from accessing computer system until ransom is paid. Ransomware mainly attacks businesses and industries have grown dramatically in recent years. There are five phases of ransomware attack (Quinkert, Holz, Hossain, Ferrara, &Lerman, 2018).

The first ransomware phase is exploitation. In the first phase, files that contain ransomware are usually deleted from computer. This exploitation is executed through exploit kit and phishing email. Its distribution spread through phishing schemes involving email attachments or downloads. The second ransomware phase is delivery and execution. This is the phase where the ransomware executing files arrive in the computer systems of the victims (Zhanhui et al., 2017) and start the attacking process. This phase only takes a couple of minutes to complete. This process will encrypt key servers in order to retrieve the loss data. Third ransomware phase is damaging of backup files. The ransomware will search for f for important files in the system such as JPG, Doc, and PDF. It will also seek and damage folders including the hidden ones where the backup files are stored (Zhanhui et al., 2017). The purpose of damaging the files is to prevent computer users from performing backup restoration.

The fourth ransomware phase is encrypting of files. Criminals will move and rename the target files. After that, they will encrypt and rename the files after a successful encryption (Tk, 2017). When the backup files cannot be opened by users, criminals will perform secure key exchange. This key will give command to users and control the server. The last ransomware phase is notifying users and demanding for money. Criminals will notify users about the payment the latter have to make after the ransomware has deleted the backup files. The demand for payment will be prompted with the payment instructions to clear the ransomware (Zhanhui et al., 2017). After locking the files or system, criminals will demand for payment which is usually high. Usually, the ransom value to unlock the infected files will be raised if the payment is not made within the stipulated time.

3.3 Ransomware Attack Channel

Ransomware uses different channels to attack its victims or businesses. The common attack methods are exploit kit, malicious email attachments and malicious email links. When victims visit a website, exploit kits are executed and malicious codes are activated in the system (Surati & Prajapati, 2017). Thus, victims will get a spam email and a notification that their computer has been locked. Malicious email attachments can occur when a recipient opens an attachment thinking the email is sent from a trusted source (Surati & Prajapati, 2017). Victims will open the files and unknowingly download the ransomware. Then the system will be infected and the files inside the system will be held. Criminals will extort for ransom. If attacks are made via email links such as URLs, these emails are sent from someone or some organizations which victims believe to be a trusted source (Surati & Prajapati, 2017). After victims clicked the URL, malicious files will be downloaded from the web. Then, criminals will send ransom notification after holding back the files.

Thus, ransomware attack can be transmitted via emails, software, download activity and exploit kit. Phishing is one of the most popular and common methods to deliver malware to victims' machines (Singh, 2017). Criminals or attackers will design a legitimate email and send them to victims. This attack if successful is considered as a huge achievement to criminals because malware is delivered via spear phishing that enables criminals to gather various information about individuals or companies. They will use the information to threaten victims that their private information will shared with the public. Victims also have a high chance of getting a ransomware attack from drive by download. Drive by download is a malicious program that automatically downloads viruses without users' knowledge (Singh, 2017). Criminals always look for vulnerability in software or network. This is because they want to find out weaknesses in the software that will provide opportunities for them to exploit and gain full access for the whole network.

4. Methodology

In order to analyze ransomware attacks, qualitative research has been selected as the method for the analysis. The data for this study collected for this research is secondary data. Secondary data can be collected via field research. Secondary data for social science include information from organizations and analyzed government departments as well as data that are originally collected for other research purposes. Data analysis was done by using telemetry by Symantec to track the ransomware attacks in certain countries. The samples were obtained from 5 countries that have been identified as countries which has are mostly infected by ransomware. According to Symantec (2016), the top five countries infected by Crypto Ransomware are United States, Japan, United Kingdom, Italy and Australia. Meanwhile, the countries mostly infected by Locker Ransomware are United States, Germany, United Kingdom, Russia and Canada.

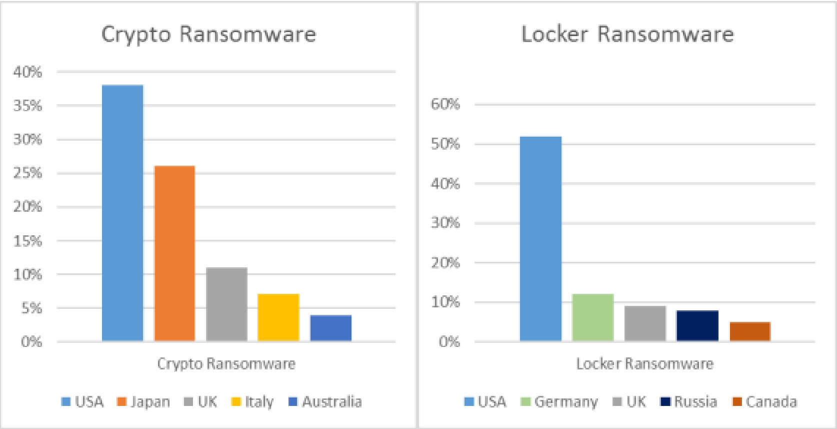

Fig. 1 - Top countries infected by Crypto ransomware and Locker Ransomware
Source: (Symantec, 2016)

Based on Figure 1, it can be said that United States is the country that has been mostly affected by Crypto and Locker Ransomware. The findings in the study confirm that the ransomware prevention is really needed in order to avoid the countries from being continuously attacked by Ransomware. The ransomware prevention will be discussed in further in the discussion part.

5. Discussion

The popularity of ransomware has been increasing. This can be witnessed from the large number of ransomware attacks on of high profile organizations over the last few years. For an example, Sony recently delayed the release of the movie “The Interview’ as the company was experiencing large scale ransomware attacks. This attacks operated by locking victims’ computer access or by encrypting, overwriting or in the worst case deleting their files. Despite the availability of systems that can detect malware, a which specifically tracks ransomware attacks is still unavailable. The following section will explain more about Ransomware prevention and ransomware removal tools.

All important data must be saved and backed up as these will minimize threats from ransomwares will be minimized and easily to be handled. Back up is a process where additional data copies are made so that the data can be restored in the future (Brewer, 2017). Attackers will usually try to steal data and threaten data owners and extort money from in order for the owners to get back those data. However, the threatscan be minimized by performingdata backup. Data backup makes data owner not having to worry of having to pay the hackers as they already have the duplicated data. Important and up-to-date data need to be backed up regularly. Other than that, backup system itself has a high potential of becoming the target of ransomware attacks because the system is very much needed to prevent infection and restore data (Gazet, 2010). Owners are also encouraged to use cloud backup system or any system that will only be connected to the network while backup process is being carried out as some attackers may try to encrypt the backups locally. Owners need to create multiple data backups and restore encrypted data to minimize the risk of ransomware attacks.

The most common way to spread ransomware is through phishing attacks. The owner must be careful by avoiding from clicking on undisclosed and suspicious links or opening attachments in spam emails. Ransomware is capable of attacking computers using multiple channels such as infected user emails, attachments in infected emails, and bad links. It may alsouse social engineering tactics such as phishing or instant messaging (Allen, 2017). Criminals have also used different tactics by using fake advertisements in order to attract people to click on them and unconsciously spread ransomware. Using ad blockers, turning off Java and Java Script will help data owners to avoid those malicious advertisements. Operating systems and security software must also be kept up to date from time to time. Thismeasure is essential in order to ensure the system is secured by the latest security updates and ensure the safety of network in an organization. The updated system and latest security software will help to minimize the risk of ransomware infections. Scaife (2016) issued a suggestion it is important to monitor file changes and track indicators of ransomware activities by using the initial warning system. Other than that, computers that have been infected by any suspicious infection should be switched off immediately. Ransomware is spreads once systemsare infected via network connection, shared storage system and shared credentials (Collier, 2017). Computer system must be kept unconnected to the network as soon as possible in order to prevent spread of ransomware infections to the whole systems in organizations. The suspectedinfected systems must be checked and repaired by authorized personnel before they can be connected to the network and restart their normal operation.

There are several anti- ransomware tools available in the market to handle and mitigate the risk of ransomware attacks on personal computers or an organizations’ network system. The first one is Trend Micro Lock Screen Ransomware Tools. It is designed to track and subsequently remove lock-screen ransomware. This ransomware is a type of malware that obstructs users from operating on their computer or network systems. Similar to modus operandi other common ransomware , users are forced to pay certain amount of money in order to get access to their files again. The software operates in two situations; the first one is when computers’ normal mode is blocked even though they can still access those files in safe mode. The second one is when lock screen ransomware blocks both normal and safe mode. In this situation, the tools will clean and remove the infected files followed by a reboot. The second anti-ransomware is Avast Anti- Ransomware Tools which is designed to detect and fight against malware and ransomware threats. Not all ransomware threats are similar and work in the same way. Avastdecryptors are free of charge and detect viruses at the same time. It provides a decryption wizard and ask users for two copies of files. The files are then separated into two; which are with password and without password protection.

BitDefender Anti- Ransomware Tools is also considered as an important tool to provide a full protection against attacks from CTB- Locker, Locky, Petya and Tesla Crypt Ransomware. Once the software has been loaded to a computer, it will detect any infection as it starts and stops the ransomware before it spreads to other files in the computer. The splash screen in the software is clean and infected section will stop executable from running to certain locations and turn on protection from boot. The software does not act to replace any existing anti- virus software, but instead work together with it. The last one is Kaspersky Anti- Ransomware Tools. It has been designed for small and medium size enterprises (SME). It comes with tools that can prevent ransomware from attacking computers and frosting the entire system network. The tools operate and monitor network activities regularly by detecting any suspicious behaviour and patterns. The tools are also suitable for businesses as they are free of charge for commercial uses and simple to operate and provide a good level of protection to the network system.

6. Conclusion

There are several challenges during the process of overcoming ransomware infections (Singh Rajput, 2017). Many ransomware attack cases involved resetting of Internet of Things (IoT) devices which did not work because the device had been attacked earlier and the owner had no choice but to to pay for ransom. Therefore, the solution to this problem is first by detecting the device, making inspections before the devices are attacked. Previous ransomware attack occured when the devices were unable to upload extensions or certain files that have a specific name as an identifier. Additionally, uniformed operating systems, communications, networks, data and sensors in IoT devices are also considered as big challenges especially when security and design are combined. Applying full security to IoT devices needs IoT systems for not being infected with ransomware throughout the application lifecycle. In addition, the IoT devices perform function, monitor, control and rearrange by only working within the network.

It would not be surprising if ransomware would change for the next few years. If ransomware is not monitored seriously, ransomware will not be just a malware which has capabilities of disabling entire infrastructure of businesses but has the potential to disable an entire city or possibly a country until the demanded ransom is paid. Cyber criminals are likely to use strategies such as hacking industrial control systems (ICS) and other critical infrastructure and aim at disabling ecosystems and not just the network. Among the few targets that cyber criminals may be targeting are payment systems such as E-bay. In 2016, a transit attack took place where ransomware targeted a service provider's kiosk.

Ransomware already has an attack record against hospitals and transport providers. Attackers are able to target larger targets in the future such as industrial robots that have been widely used in the manufacturing or infrastructure sectors that connect smart cities. Extensions via online are seen to be bound as the online system is very sensitive and easy to attack including smart devices or critical infrastructure. Cyber criminals are capable of creating, launching, and making huge profits from this cybercrime threat to continue in the future.

Acknowledgement (Acknowledgement)

We would like to express deep our appreciation to Dr Siti Aisyah Salim, our lecturer for Strategic Information Management MPA 10503 course who hasassisted us during the completion of this manuscript. The appreciation is extended to the university that provides us with the opportunities to enter the International Conference on Technology Management, Business and Entrepreneurship 2018 (ICTMBE 2018).

References

Ali, A. (2017). Ransomware: a Research and a Personal Case Study of Dealing With This Nasty Malware. Issues in Informing Science & Information Technology, 14, 87–99. https://doi.org/10.1080/13880290490480167

A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, ―Cutting the gordian knot: A look under the hood of ransomware attacks", In: M. Almgren, V. Gulisano, F. Maggi (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science, Springer, Cham, Vol.9148, pp. 3-24, 2015.

Allen, J. (2017). Surviving ransomware. American Journal of Family Law, 31(2), 65-68. Retrieved from https://www.ncbi.nlm.nih.gov/labs/journals/am-j-fam-law/

Archana, V., &Vinothini, S. (2014). A Study on RansomwareCryptowall. International Journal of Advanced Research in Computer and Communication Engineering, 3(11), 17–23. https://doi.org/10.17148/ijarcce

Aziz, S. M. (2016). Ransomware in High-Risk Environments IT-792 , Independent Research Project December 2016 Advisor

Bertino, E., & Islam, N. (2017). Botnets and internet of things security. Computer, (2), 76-79.

Bhattacharya, S., and C. R.S. Kumar. 2017. "Ransomware: The CryptoVirus Subverting Cloud Security." 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, ICAMMAET 2017 2017–Janua: 1–6.

Brewer, R. (2017). Ransomware attacks: detection, prevention, and cure. Netowrk Security, 9, 5-9. http://dx.doi.org.ezproxy.utica.edu/10.1016/S1353-4858(16)30086-1

Chhillar, Pankaj. 2017. "Ransomware-Worldwide Cyber Attacker." 2(5): 324–29.

Collier, R. (2017). NHS ransomware attack spreads worldwide. CMAJ, 189(22), 786-787. https://doi.org/10.1503/cmaj.1095434

Dell Secure Works (2012) Anatomy of an Advanced Persistent Threat (APT).

Deo, S., &Farik, M. (2015). Information Security-Recent Attacks In Fiji. International Journal of Scientific & Technology Research, 4(8), 218-220.

Everett, Cath. 2016. “Ransomware: To Pay or Not to Pay?” Computer Fraud and Security 2016(4): 8–12.

Ehrenfeld J.M. Wannacry, cybersecurity and health information technology: A time to act. Journal of Medical Systems. Springer, 2017 Jul 1;41 (7):104.

Feguson, P. (2000) Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. Ferguson 2000 Network.

G. O’ Gorman and G. McDonald. Ransomware: A growing menace. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf,2012

Gazet, A. (2010). Comparative analysis of various ransomwarevirii. Journal in Computer Virology, 6(1), pp. 77-90. Giri, B. N., Jyoti, N., & AVERT, M. (2006). The emergence of ransomware. AVAR, Auckland.

Gonzalez, Daniel, and ThaierHayajneh. 2018. “Detection and Prevention of Crypto-Ransomware.” 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017 2018–Janua: 472–78.

Hampton, N., Baig, Z., &Zeadally, S. (2018). Ransomware behavioural analysis on windows platforms. Journal of information security and applications, 40, 44-51.

Harnedy, R. (2016). 3 better ways to use backup to recover from ransomeware. Retrieved from Barkly: https://blog.barkly.com/3-better-ways-to-use-backup-to-recover-from-ransomware

Jakobsson M, Ramzan Z. Crimeware: understanding new attacks and defences. Addison-Wesley Professional; 2008 Apr 6.

Kovacs E. Maersk Reinstalled 50,000 Computers After NotPetya Attack. Security Net-work, 28 January, 2018.Kelion, L. (2013). Cryptolockerransomware has' infected about 250,000 PCs'. BBC News techology.

Krunal, G. (2017). Survey on Ransomware: A New Era of Cyber Attack. International Journal of Computer Applications, 168(3), 975–8887. Retrieved from https://pdfs.semanticscholar.org/71df/288033380d3023f09d49b7b55a77677d27a2.pdf

Landoll, D. J. (2012). The security risk assessment handbook: A complete guide for performing security risk assessments (2nd ed.). [Kindle version]. Retrieved from Amazon.com

Lelii, S. (2017). WannaCryransomware attacks shows value of data backups. Retrieved fromhttp://searchdatabackup.techtarget.com/news/450418934/WannaCry-ransomware-attack-shows-value-ofdata-backups

Liu, Y., Sun, Y., Ryoo, J., Rizvi, S., &Vasilakos, A. V. (2015). A survey of security and privacy challenges in cloud computing: solutions and future directions. Journal of Computing Science and Engineering, 9(3), 119-133.

M. Labs, Understanding Ransomware and Strategies to Defeat it, Technical Report 1, Dec. 2016.

Marengereke, T. M., &Sornalakshmi, K. (2015). Cloud Based SecuritySolutionFor Android Smartphones. International Conference on Circuit, Power and Computing Technologies [ICCPCT].

Morse, Edward, and Ian Ramsey. 2017. “Navigating the Perils of Ransomware: EBSCOhost.” Business Lawyer 72(1): 287–94. https://web.b.ebscohost.com/ehost/detail/detail?vid=0&sid=99da73bd-cfca-4c55-b5a9-18a03ed2e3c1%40pdc-v-sessmgr01&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3D%3D#AN=120778278&db=bth.Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nassi, B., Shamir, A., &Elovici, Y. (2017). Oops!... I think I scanned a malware. arXiv preprint arXiv:1703.07751.N. Khoa, T. Dat, M. Wanli, S. Dharmendra, \An approach to detect network attacks applied for network forensics," in 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD'14),pp. 655{660, 2014.

O'Gorman, G., & McDonald, G. (2012). Ransomware: A growing menace. Symantec Corporation.

Pathak, P. B. (2016). Combating Cybercrime : A Growing Trend Malvertising and Ransomware, 4(Iii), 297–299.

Pathak, P. B., &Nanded, Y. M. (2016). A Dangerous Trend of Cybercrime: Ransomware Growing Challenge. International Journal of Advanced Research in Computer Engineering & Technology, 5(2), 371–373. Retrieved from http://ijarcet.org/wp-content/uploads/IJARCET-VOL-5-ISSUE-2-371-373.pdf

Quinkert, F., Holz, T., Hossain, K. S. M., Ferrara, E., &Lerman, K. (2018). RAPTOR: Ransomware Attack PredicTOR. arXiv preprint arXiv:1803.01598.

Richardson, R., & North, M. (2017). Ransomware : Evolution , Mitigation and Prevention, 13(1), 10–21.

Richet, J. L. (2016). Extortion on the internet: the rise of crypto-ransomware. Harvard.

Savage, K., Coogan, P., & Lau, H. (2015). The evolution of ransomware. Symantec, Mountain View.

Scaife R. A. 2016. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. IEEE 36th International Conference on Distributed Computing Systems. (2016)

Shah, N., &Farik, M. (2017). Ransomware - Threats Vulnerabilities And Recommendations. International Journal of Scientific & Technology Research, Vol 06, Iss 06, Pp 307-309 (2017) VO - 06, 6(6), 307–309.

Sharma, G. K., &Verma, K. K. (2017). Ransomeware attack in cyber security : A case study, (10), 103–106.

Singh, -Abhaypratap. (2017). Ransomeware : A high profile attack Abhaypratapsingh. International Research Journal of Engineering and Technology(IRJET), 4(2), 1854–1859. Retrieved from https://irjet.net/archives/V4/i2/IRJET-V4I2365.pdf

Srinivasan, C. R. 2017. “Hobby Hackers to Billion-Dollar Industry: The Evolution of Ransomware.” Computer Fraud and Security 2017(11): 7–9. http://dx.doi.org/10.1016/S1361-3723(17)30081-7

Surati, S. B., &Prajapati, G. I. (2017). A Review on Ransomware Detection &amp; Prevention. International Journal of Research and Scientific Innovation Issue IX, IV(Ix), 2321–2705. Retrieved from http://www.rsisinternational.org/IJRSI/Issue46/86-91.pdf

Symantec. (2016). Ransomeware and Business 2016. Retrieved November 28, 2017, from Symantec Website:https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

Symantec Corporation (April, 2016). Internet Security Threat Report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Tk, A. (2017). Discussion On Ransomware ,WannacryRansomware and Cloud Storage Services Against Ransom Malware Attacks, 2(6), 310–314.

Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., &Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless communications, 24(3), 10-16.

Zhanhui, L., Azlina, N., & Rahman, A. (2017). A Review on Ransomware Trend of Attacks and Prevention, 12(16), 6201–6210.