Research Article

iMedPub Journals
http://www.imedpub.com

Global Journal of Research and Review

2021
Vol. 8 No. 4: 79

The Impact of Ransomware, Patterns, Types of Attacks and Organizational Measures Applied to Mitigate Ransomware Attacks

María Luz Barreto Bermúdez[1*] and Nima Zahadat[2]

[1]Department of College of Public Affairs, University of Baltimore, Baltimore, United States
[2]Department of forensic Science, University of Baltimore, Baltimore, United States

Corresponding author:
María Luz Barreto Bermúdez, Department of College of Public Affairs, University of Baltimore, Baltimore, United States

maghami.fatemeh@yahoo.com

Citation: Bermúdez MLB, Zahadat N (2021) The Impact of Ransomware, Patterns, Types of Attacks and Organizational Measures Applied to Mitigate Ransomware Attacks. Glob J Res Rev Vol.8 No.4: 79.

Abstract

Malicious hackers (Black Hat Hackers) are targeting business and industrial environments with a wide of variety malware attacks such as: worms, viruses, Trojan Horses, and ransomware, which disrupt or shut down systems to obtain financial gains, power of knowledge, revenge, or any other purposes. Currently, one of the most significant attacks comes from ransomware in which the number of yearly submissions has significantly grown over the past few years as criminals look on security vulnerabilities opened due to the rise in remote working to obtain financial gains. Especially in this COVID-19 times, where the number of people working from home is rising more businesses have been left at risk from ransomware. Thereby, a high alert in preventing ransomware attacks is paramount to educate yourself; besides, adjustment of security policies in business organizations. Ransomware is not only created by cybercriminal for the encryption of the networks with malware that demands hundreds of thousands of millions of dollars in different payment methods such as bitcoin but also to threaten to leak stolen sensitive data if the perpetrators are not pleased with their ransoms. This article aims to provide an overall view about ransomware core concepts, the impact generated in current society, and the role social engineering tactic plays for ransomware attackers. Lastly, this paper will discuss the role of deterrence through security measures that will give the insight to assuring confidentiality, integrity, and availability to our data against ransomware attacks.

Keywords: Ransomware; Social engineering; Security policies; Payment methods; Bitcoin

Received: June 10, 2021; **Accepted:** June 24, 2021; **Published:** July 01, 2021

Introduction

Ransomware is a type of malware that comes from “ransom” which means payment and “ware” which means a type of malware attack. Thus, ransomware is malicious software that attacks infecting a computer and then asks for a ransom. In other words, the files are encrypted on the computer and the criminals demand a ransom for the private key to decrypt the files [1,2]. The ransomware program displays a message that demands payment to restore functionality. Ransomware can be defined as an extorsion in which paying a ransom could be the only option to recover access to files. In other words, this game involves two players, a criminal and a victim. Throughout recent years, the estimation on the amount of ransom received by the criminals range from $300 to over $1000 per victim (with fluctuations in bitcoin making valuation volatile) [3]. As far as we know, there are many ways of ransomware attacks as social engineering where the victims do not have more choice but to pay a ransom. One of the known operations made by those cybercriminals is the Cryptolocker which revenue reached approximately 12 million in 2014, and in which victims could only recover 50 % of their data [4]. A survey revealed that various industrial sectors in Europe and the United States had been greatly affected and about 40% of these victims paid to attackers. A new report generated by Virus Total (Open Source statistics service) demonstrated a new sample of approximately 1.3 million cyber ransomware attacks were submitted by February 16 2021, in the USA (https://www.virustotal.com/en/statistics). Cybercriminals that use ransomware utilize numbers of strategies to avoid detection, propagate, and attack users through social engineering techniques that come in different known ways of around thirty-six families of ransomware attacks among them are CrytpoWall 3.0 that made highlines around the world as a highly profitable ransomware family, causing an estimated $325 millons in damages, DirtyDecrypt, Cerber, CryptoLocker, CryptoWall, Crysis, CTB-Locker, GoldenEye, Torrent, Locker, BackDoor [5]. Alie, Python wall, Ransonware as software, Reveton, Tesla Crypt, wannacry, among others. Criminals encrypt their files or sensitive information in exchange for financial gain finding reliable and untraceable payment methods as Bitcoin, Premium method, among others [6]. Ransomware is one of the most difficult securities cyber threats to detect and prevent because they are difficult to track, that is why the federal government is particularly concerned about the impact of ransomware on the networks at state, local, tribal, territorial governments, municipalities, hospitals, and other critical infrastructure levels. Those ransomware attacks can delay assistance to the police station or fire's department's response to an emergency or even prevent a hospital from accessing lifesaving equipment. To combat this threat, the National Cyber Investigate Joint Task Force (NCIJTF) has convened experts to educate the public on many ways to prevent ransomware attacks, to improve law enforcement coordination and response. Many organizations as Cybersecurity and Infrastructure Security Agency (CISA) Essentials and CISA Insights are working to assist small and large entities in improving their security policies and protecting them effectively from different cyber incidents as ransomware attacks [7]. Due to the negative impact that ransomware is causing around the world, this article provides a better understanding of the strategies and known signatures utilized by ransomware attackers. This article depicts the latest efforts made by researchers to detect ransomware attacks and help to underscore the necessity to secure protocols in any organization, giving insightful recommendations to avoid being a victim.

Materials and Methods

As already mentioned, ransomware is a type of malicious software or malware that encrypts data on a computer and demands for the key to decrypt that data. In most of the cases, victims are given a set of time, typically 72 hours, to pay a ransom which is generally around $100 to $1000 for individuals, and much more from organizations and firms [8]. There are some patterns of ransomware attacks such as gaining an administrative privilege by simply asking for it or using any social engineering tactics. For instance, some of those cybercriminals try to get access to ask the user to install software or adding any patches on their installation or requesting fake updates or antivirus updates. In most of the cases, ransomware perpetrators ask for app-level permissions to perform their tasks. It is important to know that ransomware lies in two platforms Android and Windows. The first one uses a zombie machine or network commonly named bonet, which is a sort of backdoor channel open for the attacker to get access to the infected system. These botnets are used by hackers to control systems and lunch a Distributed Denial of Service (DDoS) attacks so the ransomware attacker can steal passwords and banking account details. Thereby, all the permission of the victim's devices and administrative access of the attacker are gathered and sent to Command-and-Control Server (C and Cs), which contains all the stolen information obtained from zombies using encrypted Transport Layer Security mechanism to secure their stolen data [9]. On the windows platform, ransomware attacks the victim through malicious websites, email attachments, any malicious web-link or request one of several payment methods. Subsequently, when the system is infected with this ransomware, it contacts C and C server as the android application mechanism, where the C and C server generates the symmetric key and then, starts the encryption of data using asymmetric encryption (RSA) preventing that the key cannot be used for decryption. This asymmetric algorithm uses two different keys, one public key for encryption of data and one private key for decryption [10]. At that same time, all the backups, restore points and volume shadow copies are deleted by this ransomware. Among the main types of ransomware are the crypto ransomware which obtains a private key from C and C to encrypt all the victims' files Cs with a public key RSA generated randomly by the C and Cs and after that the crypto sends threatening messages asking for a ransom through a Bitcoin payment to exchange the key to decrypt their data [11]. On the other hand, we have the locker ransomware which works differently compared to crypto, it resets the device PIN using all types of social engineering tactics (explained below) to restrict user access to device and system functionalities and then asks for a ransom. Therefore, a locker of ransomware is considered more detrimental than crypto ransomware causing inactivation of systems by Denial of Service (DoS) until the victim pays for a ransom [12]. Typical signatures or characteristics of all ransomware families attack is schemed by device locking, data encryption, data deletion, data stealing, and sending threatening messages [13]. **Table 1** portrays a list of notable features of some ransomware families are mentioned from columns 2 to 11.

DF	Notable features					Payment method			DF	DF
5	Summary	Data deletion	Data stealing	Data encryption	Device locking	Bitcoin	Premium	Untrace-able	Type	Platform
(Trojan .Ransomcrypt.A) (2016)	Strong grip over remote desktop Protocol based servers									
MM Locker (2016)	Behaves similar to the locked ransomware	-	-	√	-	√	-	-	Trojan	Windows
8Lock8 (2016)	Encrypts your data and then appends the 8lock extension to encrypted files.	-	-	√	-	√	-	√	Trojan	Windows

Shade/ Trolde sh	Create using development kit that encrypts	-	-	√	-	-	-	√	Viruses	Windows
Zyklon Locker (2016)	It is variant of GNL locker.	-	-	√	-	-	-	√	Trojan	Windows
MIRCOP (2016)	Highest ransom amount seen 48.48-bit-coin (around	5	5	5	5	5	5	5	5	5
$28,730.70)		√	√	-	√	-	-	Trojan	Windows	5
Android. Lock droid.E (2016)	Sends illegal videos on third-party app stores, the app snaps a picture of the	5	5	5	5	5	5	5	5	5
	victim using the device's camera and includes the image as part of the	-	-		-	-	-	√		

Table 1: List of Ransomware families with their notable features, payments methods, type, and platform [9].

According to investigations one of the best techniques used by ransomware attackers is the social engineering tactic which is based on deceiving users or persuading people to perform certain actions by using physical or digital access to an organization's system information to encrypt the data and consequently, asking for a ransom. Recent researchers such as Peltier, Abraham, and Chengalur-Smit [14,15]. concluded that social engineering can be categorised into two groups humanbased social engineering attack and technology-based social engineering attack. In other words, the first group human based social engineering attacks uses person to person sometimes third-party authorization such as: dumpster diving, shoulder surfing, creating a sense of urgency using psychological tricks, lies, bribes, and even extorsion, impersonation. The second group technology based social engineering attack is characterized by using digital technology as basis for email phishing, online scam, pop up advertisements by installing software, and other threats to accomplish cybercrimes (**Figure 1**).

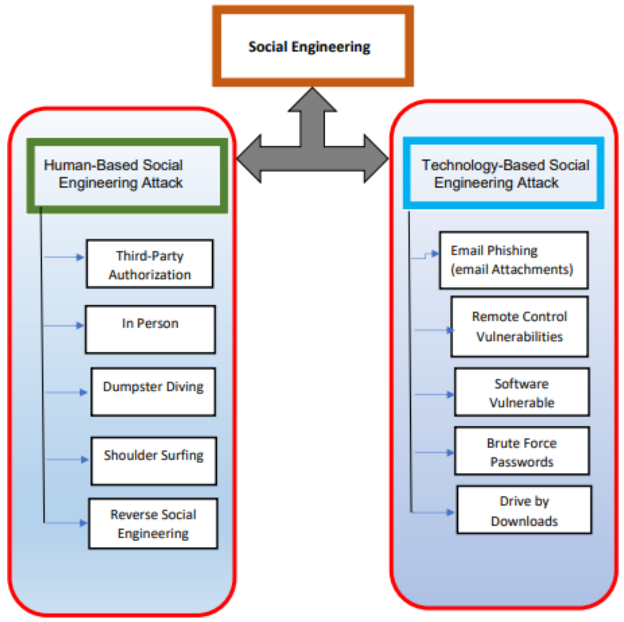
Social Engineering
Human-Based Social Engineering Attack
Third-Party Authorization
In Person
Dumpster Diving
Shoulder Surfing
Reverse Social Engineering
Technology-Based Social Engineering Attack
Email Phishing (email Attachments)
Remote Control Vulnerabilities
Software Vulnerable
Brute Force Passwords
Drive by Downloads

Figure 1: This scheme shows the two ways of social engineering tactics applied by ransomware attackers.

Henceforth, this article's also passage aims the variety of attack techniques that social engineering tactics computer technologies use as a to tool to infect systems with ransomware (**Table 2**).

Email Phishing: When the cybercriminals send a spam email that contains a malicious file or link, which deploys malware when it is clicked. That is what commonly is known as email spams that use social engineering themes to trick users into installing ransomware under the following known themes such as: Mail delivery notification, energy bills, job Third-Party Authorization In Person Dumpster Diving Shoulder Surfing Reverse Social Engineering Email Phishing (email Attachments) Remote Control Vulnerabilities Software Vulnerable Brute Force Passwords Drive by Downloads 7 seeker resume, tax returns and invoices, police traffic offense notifications.

Remote Desktop Control vulnerabilities: Network protocol that allows individuals to control the resources and data of computers over the internet.

Software vulnerable: Cybercriminals usually take advantage of security weaknesses in software programs to gain control of victim's systems and deploy ransomware. For instance, on the Android app, there are some special features not only for encrypting files or locking devices but employing capabilities to spread to all contacts within the device's address book by sending social engineering SMS messages. For instance, Android. Lockdroid. E is illegal software that plays pirated videos and as soon as it displays videos on that software, it takes a snap of the victim using the device's camera and then, the cybercriminal asks for a ransom.

Brute Force passwords: This technique consists in acquiring login credentials for spreading ransomware through an exhaustive number of successive guesses of passwords to break the cipher of the encrypted data keys [16].

Drive-by-Downloads: Many legitimate websites contain malicious code injected in their host to compromise sensitive information by cross-site scripting attacks where most of the time victims cannot spot on their own (**Table 2**) [17].

Ransomware	Malicious Emails/ spam campaigns	Self-propagation	SMS messages	Software or third-party app Store	Exploiting server vulnerabilitie	Brute force password	Drive by download	Other ways
MM Locker	√	-	-	-	-	-	-	√
8Lock8	√	-	-	-	-	-	-	√
Zyklon Locker	√	-	-	-	-	-	-	
Mircop	√	-	-	-	-	-	-	
Apocalypse	-	-	-	-	-	√	-	√
Ransom32	√	√			-	-		
Cryptowall	√	-	-	-	-	-	-	-

Table 2: Ransomware attacking methodology [9].

Ransomware is a cybercrime business where the payment systems are accessible to make an easy path for the victims to pay. Cybercriminals always keep improving their source of payment by discovering new ways to causes difficulty in tracing the identification of the payments' receipts. Among the most known methods of payments are:

a. Bitcoin:

Bitcoin is one of the most used payment methods, characterized by its untraceable nature.

b. Premium Method:

Cybercriminals ask to the victim to send SMS to a particular number to decrypt files. Uses social engineering tactics and requires the least amount of technical background. When it is propagated in a large scale the revenue could be significant [9].

c. Other Untraceable Methods:

Some ransomwares instead of asking for bitcoin payments, they ask for iTunes gift cards worth of 200 USD. Other ransomware payments include Paypal, Ukash cards, Money Pak, Paysafecard [9].

Results

A report generated by The United States of Department of Justice demonstrates that 4000 ransomware attacks occur daily [18]. Likewise, in the healthcare industry, it has been revealed that approximately 88 % percentage of cybercrimes is generated by a ransomware attack as reported by Cyber Security provider Solutions [19]. Thereby, some preventative measures of ransomware attacks are recommended by the United States Office for Civil Rights (OCR), Federal Bureau of Investigation (FBI), and Federal Trade Commission (FTC) such as: There are some solutions for nontechnical personnel such as: making sure that all the employees can receive specialized ransomware training such as: never open an email attachment unless it is a trusted sender source. In general, we need to take into considerations to block email messages with the following extensions: *.exe, *.zip, *.rar, *.7z, *.js, *.wsf, *.docm, *.xlsm, *.pptm, *.rtf, *.msi, *.bat, *.com, *.cmd, *.hta, *.scr, *.pif, *.reg, *.vbs, *.cpl, and *.jar from suspicious sources [20]. Furthermore, users are advised to immediately delete any suspicious activity on monitors, scan the computer system regularly and Run USBs only if they are from trustable sources. Likewise, being alerted of a significant increase of the renamed files on your network could be a symptom that you are being stroked by a ransomware attack. Another important measure to restore and recover data is making a weekly backup and storing data offline. Maintaining backups offline and unavailable from their networks will reinforce the security against ransomware attackers [21]. On the technical solutions side, avoid staying logged as an administrator any longer than needed. Inadequate IT support or lack of security protocols open backdoors to cybercriminals. For instance, a bad placement of anti-virus or anti malware programs can prove an easy prey by ransomware attackers. In addition, it is required to encrypt sensitive data through protection with strong passwords*. In recent years, ransomware attackers are breaching health privacy information, becoming a big threat to the Health Insurance Portability and Accountability Act (HIPAA), which is a health database act 9 that actively encrypted and indecipherable health data can block attempts by ransomware attack if they are properly followed by the organization's members. To reinforce this breach of HIPPA act, the Civil Rights (OCR's) Ransomware Fact Sheet has been created to provide guidance against ransomware attacks and establish adequate notification of breaches, in case of attacks [21]. Likewise, ensuring basic technical procedures will help to avoid ransomware attacks such as: enabling automated patches for operating systems and web browsers, using complex and strong passwords, pop-up blockers, assuring that the firewalls are duly configured, keeping operating systems updates and maintaining the latest versions of the software, adjusting protection to browsers, and using web-filtering and gateway filter technologies. Likewise, installing spam filtering and email filtering services are essential to prevent infected systems; for instance, a good email filter used is Symantec Email Security Cloud to avoid being targeted by hackers as well as stop malicious emails [22]. According to Sophos Threat Report, the gap between highly skilled ransomware operators who target wealthy organizations and the script kiddie attackers who are looking for capturing smaller pretty companies has broadened significantly in the last few years (https://mytechdecisions.com/networksecurity/sophos-threat-report-whatthree-cybersecurity-trends-to-look-forin-2021/). The United States government provides resources to protect against the threat of ransomware; for instance, signing up for the OCR's Security Listenerv to receive ransomware updates and guidance [23]. Due to the complexity of detection ransomware attacks, various researchers strongly suggest monitoring those attacks with other sophisticated techniques such as Machine Learning Algorithms and Artificial Intelligence (AI) systems. Machine Learning (ML) approaches models to recognize ransomware's behavioral pattern rather than a specific signature in their attack. As far as it is known, a signature can be changed easily for each period of time, but the attack pattern is more difficult to change [12]. However, choosing the right Machine Learning (ML) algorithm to match with the right data and provide accuracy in its prediction is a dilemma at this time. Indeed, sometimes it is highly recommended to pay the ransom to avoid significant financial loss and to preserve critical business operations [24].

(*) Features of strong passwords:

Minimum length of six-ten characters

Must contain at least three of the following: Lowercasealpha, uppercasealpha, digitalandspecial character.

Alpha, number, and special characters must be mixed up.

Discussion

This article states that ransomware malware has become one of the most dangerous threats across the world. Although, the ransomware was discovered thirty years in the cyberspace, it has not been treated with the proper security standards for many organizations. As a result of this lack of security protocols, ransomware attacks trigger financial loss and cessation of organization's functionalities with more severity compared to a few years ago. Additionally, the rise in attack numbers has been reflected tremendously since we are being affected by this pandemic COVID-19 where all the work is being performed remotely. This whole article depicts basic core concepts of the highest vector of the cyberthreat ransomware, identifying its symptoms and the ransomware families. Combating the several security threats of this attack requires a deep understanding of these techniques and strategies adopted by this malicious malware over the network. New research efforts have been developing new algorithms applied in Machine Learning and Artificial Intelligence to achieve early detection of ransomware attacks but unfortunately without much success yet. Indeed, sometimes it is recommendable to pay for a ransom rather than being locked or to cease organizational operations to mitigate financial loss. Cybersecurity communities and law enforcement are making efforts to hunt these ransomwares attackers in their early stages of attacks.

Conclusion

Although this ransomware malware has been created and disseminated thirty years ago, it does not alleviate ransomware attacks predicting an expectation of a financial loss of approximately 20 billions of dollars by the end of 2021 and the global damages related to cybercrime will reach $6 trillion. (https://www.natlawreview.com/article/r ansomware-attacks-predicted-tooccur-every-11-seconds-2021-cost-20- billion). There is such a concern that many organizations are still using basic security protections against those threats. According to the CrowdStrike report (November 2020), approximately 56 % in a survey of 2200 organizations in 2020 have been infected by ransomware attacks with an average ransom in the USA of 1.3 million dollars and the estimation of the whole world easily can reach more than billions of dollars and the threats become worse with the COVID-19 situation (https://mytechdecisions.com/complian ce/crowdstrike-ransomware-nationstate-attacks-dominate-securitythreats/). For that reason, the purpose of this article is mainly to identify symptoms of ransomware attacks, the known ransomware families of attacks and to encourage individuals and businesses to follow the proper recommendations mentioned earlier to avoid becoming a victim. In other words, every company should be actively involved in the security protocols given by law enforcement or any certified cybersecurity company which needs to be followed by everyone from the simple employee (user) to the IT technical support to mitigate ransomware attacks by executing basic security practices; for simple users, this means handling the phishing menace by labelling emails that come in from external sources or making offline backups; for IT personnel, this means patching software and protect data by encryption. However, this might not be the solution to stop advanced skilled ransomware attackers due to the complexity to trace their dynamic attacks over the network as even sophisticated ML techniques used by cyber threat experts cannot unveil ransomware detections, but it will help to reduce the threats in terms of real time of the ransomware attack execution and stop most of the entry level ransomware attackers that are widening the number of the small companies' victims.

Acknowledgments

We would like to thank my brother Dante Daniel Barreto Bermudez who has been such emotional support for me, and for all the academic support received by my professors from the Cyber Forensics Master Program from The University of Baltimore.

References

1. Mansfield-Devine S (2016) Ransomware: Taking business hostage. Netw Secur 2016(10): 8-17.
2. Kalaimannan E, John Sk, DuBose T Pinto A (2017) "Influences on ransomware's evolution and predictions for the future challenges". J Cyber Security Tech 1(1): 23-31.
3. Liao K, Zhao Z, Doupe´A Ahn Gail-Joon (2016) Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin. In: Electronic Crime Research. APWG Symposium IEEE.
4. CyberEdge (2018) Fifth-Annual Cyberthreat Defense Report.

5. Ransomware What it is & What to do About it.

6. Amin Kharraz, Sajjad Arshad, Collin Mulliner (2016) “UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware”. 25th USENIX Security Symposium.

7. The cyber threat alliance. “Lucrative Ransomware Attacks: Analysis of Cryptowall Version3 Threat”.

8. J. Hernandez-Castro, A. Cartwright and E. Cartwright. An economic analysis of ransomware and its welfare consequences. (2020). Royal Soc Open Sci 7(3): 190023.

9. Aurangzeb S, Aleem M, Iqbal MA, Islam MA (2017) “Ransomware: A Survey and Trends”. Journal of Information Assurance and Security 12.

10. Barbulescu M, Stratulat A, TraistaPopescu V, Simion E (2016) “RSA Weak Public Keys available on the Internet”. (2016) In International Conference for Information Technology and Communications.

11. Monika, Zavarsky P, Lindskog D (2016) “Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization”. Procedia Comput Sci 94: 465- 472.

12. Yaqoob I, Ahmed E, Rehman MH, Ahmed AIA, Al-garadi MA, et al. (2017) The rise of ransomware and emerging security challenges in the Internet of Things. Comput Netw 129: 444-458.

13. Andronio N (2015) “Heldroid: Fast and Efficient Linguistic-Based Ransomware Detection”.

14. Peltier TR (2016) Social engineering: Concepts and solutions. Information Security and Risk Management. 15(5): 13-21.

15. Abraham S, Chengalur-Smith I (2010) An overview of social engineering malware: Trends, tactics, and implications. Technol Soc 32(3): 183-196.

16. Raza M, Iqbal M, Sharif M, Haider W (2012) “A survey of Password Attacks and Comparative analysis on methods for secure Authentication”. World Appl Sci J 19(4): 439-444.

17. Azad A, Murthy R, Kohun F (2016) "Recovering from The Nightmare of Ransomware–How Savvy Users Get Hit with Viruses and Malware: A Personal Case Study". Issues in Information Systems 17(4): 58-69.

18. The United States Department of Justice How to protect your networks from ransomware.

19. NT Security (2016) Solutionary SERT Q2 report: 88 percent of all ransomware is detected in healthcare industry.

20. Sittig DF, Singh H (2016) “A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks”. Appl Clin Inform (2): 624-632.

21. Pope J, JD (2016) “Ransomware: Minimizing the Risks’’. (2016). Innov Clin Neurosci 13(12): 37-40.

22. U.S. Department of Health and Human Services. Sign up for the OCR Privacy & Security listserv.

23. Symantec (2016) “An ISTR Special Report: Ransomware and Businesses”. (2016).

24. Cartwright E, Castro JH, Cartwright A (2019) “To pay or not: game theoretic models of ransomware. J Cybersecur 5(1): 1-12.