Global Scientific JOURNALS
GSJ: Volume 10, Issue 1, January 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

Is Ransomware a challenge for Cybersecurity?

Abdul Rehman
Faculty of Science and Technology
Bournemouth University
Bournemouth, UK
S5320018@bournemouth.ac.uk

***Abstract*—Cybercriminals use Ransomware to encrypt your data and demand payment to decrypt it. This is still a growing threat for cybersecurity started with simple email attack. This paper discusses different types of techniques and versions used in ransomware attack and how you can save yourself and your organization by following Incident handling Guide.**

Keywords—ransomware, encryption, decryption, malware, email attack, cybersecurity, security,

I. Introduction

With the progress of technology, people are always linked to the internet and may utilize it for a diversity of functions, like education, work, recreation, and so on. The online platform is full of numerous forms of threats, and one of the most current is known as Ransomware [1], [2], in which Cyber Criminals attack users with malware that encrypts their data on their own computers or networks and forces them to pay money in exchange for the decryption key [4].

Billions of gadgets are at risk as a result of this major attack. To make a successful ransom demand, criminals use a variety of weaknesses and strategies. From £554,808 in 2020 to £1.34 million in 2021, the average cost of recovering a ransomware attack has more than doubled [3]. Each company in the United States lost an average of £1.70 million [4]. According to [4] survey, the primary industries hit by the attacks were retail and education, which accounted for almost 44% of the total. In 2020, 26% of victims will pay money to have their data returned, up to 32% in 2021.

Cybersecurity faces a significant difficulty in this area. The techniques, facts, and countermeasures for Ransomware attacks will be investigated by the authors while maintaining Confidentiality, Integrity and Availability [5]. Is ransomware still a big threat to cybersecurity?

II. Ransomware Threats and Techniques to Attack

A. History of Ransomware

The First ransomware attack happened in 1989 targeting Healthcare Industry encrypting all files on the C drive known as PC Cyborg virus. This was the birth of a new threat for cybersecurity [6]. Ransomware attack went viral in 2017 with WannaCry and Petya attack affecting 200,000 computers in more than 150 countries [6], [7].

B. Techniques used by Ransomwares

Infected Email – The Attackers commonly attach a malware with executable file pretending to be a credible source [28]. When recipient opens the infected file, the system will be infected by the malware, and the device will be locked by ransomware [25].

Exploit Kits – When any person deliberately or undeliberate click any advertisement, downloads a malicious software containing exploit kits [25], [27].

Social Engineering – It's easy to find information about an organisation or employee using social media. By compiling collected information into an email and pretending to be credible source. When they open the link or file shared in the email and eventually end up with the ransomware [26]. Finally, all of the companies connected device on that network will going to be the victim of Social Engineering attack [35].

By paying the Ransom demand – Unfortunately, most of the time people pay for the ransom demand by cyber criminals. Which only increase their moral to do it again to same organization or individual [32]. Additionally, all the payment are in crypto currency it's difficult to track the who is paying who and how much [31].

Not having any Cyber Incident Response team – By considering cyber security of any organisation then Incident Response Team is the basic requirement. Which, most of the time neglected by them and Cyber Criminals take advantage of this weakness of the company and get successful in the attack as there is no team to counter that threat [33].

By neglecting the rules – When Organisations ignore basic rules and regulatory bodies warnings to save some money on the IT Security. Ransomware attacks take advantage of this situation and exploit weaknesses and vulnerabilities in the system to gain illegal access and achieve them goals [34].

By using Basic Signature based Solution – Most of the time organisations using signature-based antivirus detection-based system. Which is not a good idea. Since, they are using already detected threats and hence vulnerable to new type of virus and malwares [29], [30].

C. Top Ransomware Families of 2021

Following are the infamous variants of Ransomware observed in year 2020 and 2021 that took advantage of COVID-19 [8].

Ryuk – Ryuk was originally discovered in August 2018 as part of a campaign that targeted a number of businesses. Using a combination of AES-256 and RSA key encryption to cipher user data by exploiting Remote Code Execution to trick and gain access [16]. The file contents are encrypted using the symmetric key, while the symmetric key is encrypted with the asymmetric public key. The associated asymmetric private key is released after the ransom is paid, allowing the encrypted files to be decoded [9].

Maze (ChaCha) – Maze is a ChaCha variant and actively targeting victims since December 2019. Mostly infecting Microsoft Office files and using Brute Force Attack and exploit kit to gain access to a network and spared to all the available devices [10], [17], [18].

Defray777 – Defray777 was first discovered in 2017 and also known as RansomEXX and Target777. Windows variant cipher all of the system files but Linux variant encrypt only directories using command line argument [8] The main target of Defray777 was Virtualized hosts running ESXi servers [11]. Defray777 uses these vulnerabilities CVE-2019-5544, CVE-2020-3992 to bypass Windows OS security and encrypt Virtual Machine Disk directly on hypervisor [19].

WastedLocker – Evil Corp is behind WastedLocker Ransomware attack, this is the identical association accountable for Dridex and BitPaymer attacks [12]. The main target audience of WastedLocker are those with £7.4 million assets or more [8]. Each file encrypted using new created AES key using a CBC mode. These are also encrypted using public RSA key. The Final output is stored as a base64 output in the ransom note [13]. WastedLocker uses these vulnerabilities CVE-2019-0752, CVE-2018-8174 to run JavaScript code and then run wscript.exe in windows to download and run real malware [20].

REvil – REvil ransomware also known as Sodinokibi targeted mainly professional and legal services related to media and communication, retail, energy sector and wholesale in US, Canada, Hong Kong and Australia. It also uses RDP vulnerability and phishing to gain access and initiate DNS request to multiple domains [8]. REvil uses zero-day vulnerabilities such as CVE-2021-30116, CVE-2018-8453 to deploy ransomware of clients using Kaseya products that helps for monitoring and managing infrastructure [21], [22].

NetWalker – NetWalker which is also referred as MailTo use weak RDP credential, or exposed VPN to spared via phishing email targeting government, healthcare, transportation, manufacturing, and energy sectors in the US, Saudi Arabia, Germany, New Zealand, Pakistan, India, UK, Colombia and South Africa [8], [14]. NetWalker uses these vulnerabilities CVE-2019-11510, CVE-2019-18935 to commonly target RDP servers, web application and VPN servers to gain unauthorized access of a network and attack them with ransom [23].

DoppelPaymer – DoppelPaymer first discovered in April 2019 using AES-256-CBC encryption. This group was able to compromise 60 organizations using CVE-2019-19781 vulnerability affecting Citrix ADC [15]. DoppelPaymer uses this vulnerability CVE-2019-19781 to drop payload to extort ransom. Usually, servers were unpatched against this type of vulnerability [24].

III. Solution techniques

Incident Handling Guide – Following is the process of incident handling guide as outlined by National Institute of Standards and Technology (NIST) [36], [37].

Developing and rehearsing an incident handling guide – Mainly, an incident handling guide is built to put an organization to act quickly and effectively in time of stress and threat of digital assets and integrity of data. This Guideline is also designed in compliance with NIST Incident Response Process consisting of following major stages such as Preparation, Detection and Analysis, Containment, Recovery, Paying a ransom and Post-Incident Activity [38].

A. Incident Handling: Detection

It really depends on the situation that how an enterprise detects an attack. Most of the time, it's employee of the organization that detects a ransomware in the first place.
First step would be to identify all of the infected systems and isolate them with the unaffected systems to help reduce more damage to the business.
Authors have discovered some of the following situations to help business deal with ransomware attacks.
Situation one – A user try to open a file on a shared network and found out it is encrypted. In this case, when a user accesses a file on a shared device noticed the file is encrypted. At this point, it is important to find the access of the user account as it can still encrypting other files on the network. So, identify the permission of the user account on the network and try to revoke the permission and isolating the system which is spreading the ransomware. Because, the ransom notice is not displayed yet as the attack is still in progress.
Situation two – A user accessed a file stored in a local storage and it is encrypted by the ransomware. But it does not mean that all of the files on the local computer are encrypted. To counter this type of situation. Do not reboot or restart your device. Just shut down your system immediately or disconnect it from network. Additionally, hibernate the system as occasionally ransomware saves encrypted keys in the memory. So, IT experts can use it to save your encrypted data.
Situation three – When suddenly user received a ransom message on their device, providing the contact and payment details. This is an illustration of successfully ransomware attack.
Situation four – Enormous misuse of data (file sharing traffic) alert. In this case, if organization enabled file manipulation alert in the rules, then they can receive the notification about abnormal usage across the network or device comparing with normal daily usage.

B. Incident Handling: Analysis

First Step – Identifying specific family of the ransomware. This is very important to counter any ransomware attack. Finding the variant of the malware used is important as our lateral movements may be helping attackers depending on the code of the ransomware. Normally, contact IT support or experts to guide you in this step.
Second Step – Using Root Cause Analysis (RCA). If you skip a basic RCA to the network or device and recovered the system from ransomware attack then the attack can repeat

itself. When, you missed the root cause of the incident which can be a host in you network still affected which initiated the attack in the first place. For instant, the most common access points for the ransomware attack are browser exploitation, email or other vulnerabilities [39], [40].

Email access point – A deep search should be conducted in the mailboxes of the employees to search for any unopened mails containing the malware and should be purged from the mailboxes to prevent future attack.

C. Incident Handling: Containment

This stage of the incident handling is very critical. Authors identify that after finding system affected by ransomware attack, it should be isolated from the rest of the network including WIFI connection as well. Failure to do so can increase potential risk of future encryption of the devices connected to the same network. If not properly planned it can cost organization two to three times longer to disinfect and recover from the incident.

By running endpoint detection and response (EDR) – With the use of Endpoint detection and response (EDR) solution attacks can be detected two or three days earlier than normal basic antivirus solution [41].

By terminating access – If determination of the source of the attack is taking more time than as a last option the access to the shared network should be terminated. Try not to change permissions of the files as it can be time consuming process. Meanwhile, ransomware can keep doing its work.

D. Incident Handling: Eradication

This stage involves removing ransomware from the infected devices by using trusted settings stored in a secure location. It can be a lengthy process depending on the scope of the attack and affected devices. Moreover, infected devices or first infected device can be detected by using root cause analysis to stop future attacks.

E. Incident Handling: Recovery

Recovery stage should begin after the completion of containment and identification stage. There are several considerations that an organization should consider while doing recovery of a network or a device.

By patching vulnerabilities – If the attack used a vulnerability, then it needs to be patched. So, it cannot be exploited again. If patching is not possible then ensure security controls are made to minimize the risk.

By restoring data from backups – Backups should be used to recover from the attack. Nonetheless, the most important part is to check and verify that a secure backup is being used to restore. In a silent attack the malware can remain undetected for weeks and can be backed up as a part of backup process and it can again affect the systems. Additionally, hard disk, optical disks and cloud solutions can be used to backup data in multiple places.

By breaking the encryption – Sometimes week encryption can be reversed by the expert. Which can save organization money to pay the ransom. While some variant cannot be reversed. Thus, an expert should be consulted to check the version and variant of ransom to check if the decryption key can be found [42].

F. Incident Handling: Paying a ransom

Finally, some organizations can decide to pay the ransom demand to get the data that is not possible to recovery by other means. Some of the things should be considered before paying any ransomware. For instant, business continuity goals, costs, legal implications and not receiving any decryption key even after paying the ransom demand.

Supporting criminal's business model – if the ransom demand is fulfilled it can increase the motivation of any cybercriminal or even increase the price for the next attack [43].

Paying criminals does not mean recovery – paying a ransom does not mean they will be providing you the relevant information for recovery as they can vanish after receiving the payment.

FBI recommendation for paying ransom – FBI does not support paying any ransom demand after ransomware attack. As, paying the ransom does not guarantee that they will going to provide a decryption key to recover data [44].

G. Incident Handling: Post-Incident Activity

Post-incident activity is the last stage in the incident handling guideline. Organizations should hold a meet or get to gather to discuss kind of "lessons learned" from the analysis that help the organization improve safety and minimize potential impact.

Furthermore, if any new technology or technique can be used in future to improve security and analyses the situation in the future. This is a general guideline for most of the organizations. Please contact your incident response team or service provide if you need further assistant to prevent ransomware attack.

IV. Conclusion

As authors discussed the ransomware attack is kind of a challenge to the cyber-security. Since, organizations losing millions of pounds per attack. Ransomware attacks can be minimized or stopped by following Incident Handling Guide provided in this research paper to secure your organization.

References

[1] NCSC.GOV.UK, 'Mitigating malware and ransomware attacks', 2021. [online]. Available: https://www.ncsc.gov.uk/pdfs/guidance/mitigating-malware-and-ransomware-attacks.pdf. [Accessed: 02- Nov- 2021].

[2] KASPERSKY, 'Ransomware – definition, prevention and removal', 2021. [online]. Available: https://www.kaspersky.com/resource-center/threats/ransomware. [Accessed: 02- Nov- 2021].

[3] SOPHOS, 'Ransomware Recovery Cost Reaches Nearly $2 Million, More Than Doubling in a Year, Sophos Survey Shows', 2021. [online]. Available: https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-

more-than-doubling-in-a-year.aspx. [Accessed: 02- Nov- 2021].

[4] SOPHOS, 'The State of Ransomware 2021', 2021. [online]. Available: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf. [Accessed: 02- Nov- 2021].

[5] FORTINET, 'CIA Triad', 2021. [online]. Available: https://www.fortinet.com/resources/cyberglossary/cia-triad. [Accessed: 02- Nov- 2021].

[6] A. Lakhani, 'Analyzing the History of Ransomware Across Industries', 2021. [online]. Available: https://www.fortinet.com/blog/industry-trends/analyzing-the-history-of-ransomware-across-industries. [Accessed: 02- Nov- 2021].

[7] A. Kharpal, 'Hackers who infected 200,000 machines have only made $50,000 worth of bitcoin', 2017. Available: https://www.cnbc.com/2017/05/15/wannacry-ransomware-hackers-have-only-made-50000-worth-of-bitcoin.html. [Accessed: 02- Nov- 2021].

[8] PALOALTO, 'Palo Alto Networks | Unit 42 | Ransomware Threat Report, 2021', 2021. [online]. Available: https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html. [Accessed: 02- Nov- 2021].

[9] M. Elias, 'New Ryuk Ransomware Sample Targets Webservers - McAfee', 2021. [online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/new-ryuk-ransomware-sample%E2%80%AFtargets-webservers/. [Accessed: 02- Nov- 2021].

[10] kaspersky, 'What is maze ransomware? Definition and explanation', 2021. [online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-maze-ransomware. Accessed:

[11] vmware, 'Deconstructing Defray777 Ransomware', 2021. [online]. Available: https://blogs.vmware.com/networkvirtualization/2021/03/deconstructing-defray777.html/. [Accessed: 03- Nov- 2021].

[12] P. Arntz, 'Threat spotlight: WastedLocker, customized ransomware', 2020. [online]. Available: https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/. [03- Nov- 2021].

[13] N. Pantazopoulos, S. Antenucci, M. Sandee, 'WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group', 2020. [online]. Available: https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/. [Accessed: 03- Nov- 2021].

[14] cybereason, 'Cybereason vs. NetWalker Ransomware', 2021. [online]. Available: https://www.cybereason.com/blog/cybereason-vs.-netwalker-ransomware. [Accessed: 03- Nov- 2021].

[15] Acronis, 'Threat analysis: DoppelPaymer ransomware', 2021. [online]. Available: https://www.acronis.com/en-gb/articles/doppelpaymer-ransomware/. [Accessed: 03- Nov- 2021].

[16] BD, 'Bulletins and patches', 2020. [online]. Available: https://cybersecurity.bd.com/bulletins-and-patches/ryuk-ransomware. [Accessed: 03- Nov- 2021].

[17] S. Boulevard, 'Maze Ransomware Exploiting Exploit Kits', 2019. [online]. Available: https://securityboulevard.com/2019/11/maze-ransomware-exploiting-exploit-kits/. [Accessed: 04- Nov- 2021].

[18] G. Belding, 'Maze ransomware', 2020. [online]. Available: https://resources.infosecinstitute.com/topic/maze-ransomware/. [Accessed: 04- Nov- 2021].

[19] P. Paganini, 'Ransomware operators exploit VMWare ESXi flaws to encrypt disks of VMs', 2021. [online]. Available: https://securityaffairs.co/wordpress/114124/malware/ransomware-attack-vmware-esxi.html. [Accessed: 04- Nov- 2021].

[20] BITDEFENDER, 'RIG Exploit Kit delivers WastedLoader malware', 2021. [online]. Available: https://www.bitdefender.com/files/News/CaseStudies/study/397/Bitdefender-PR-Whitepaper-RIG-creat5362-en-EN.pdf. [Accessed: 04- Nov- 2021].

[21] A. jain, 'Kaseya REvil Ransomware Attack (CVE-2021-30116) – Automatically Discover and Prioritize Using Qualys VMDR®', 2021. [online]. Available: https://blog.qualys.com/product-tech/2021/07/08/kaseya-revil-ransomware-attack-cve-2021-30116-automatically-discover-and-prioritize-using-qualys-vmdr. [Accessed: 04- Nov- 2021].

[22] WEZEN, 'NEW ATTACK – REvil Ransomware', 2020. [online]. Available: https://www.wezengroup.com/new-attack-revil-ransomware/. [Accessed: 04- Nov- 2021].

[23] S. Carpenter, 'Netwalker Ransomware: What You Need to Know', 2020. [online]. Available:

https://expanse.co/blog/netwalker-ransomware-what-you-need-to-know/. [Accessed: 04- Nov- 2021].

[24] S. Gatlan, 'DoppelPaymer Hacked Bretagne Télécom Using the Citrix ADC Flaw', 2020. [online]. Available: https://www.bleepingcomputer.com/news/security/doppelpaymer-hacked-bretagne-t-l-com-using-the-citrix-adc-flaw/. [Accessed: 04- Nov- 2021].

[25] PALOALTO, 'Ransomware: Common Attack Methods', 2021. [online]. Available: https://www.paloaltonetworks.com/cyberpedia/ransomware-common-attack-methods. [Accessed: 04- Nov- 2021].

[26] P. Gallegos, J. Bravo-Torres, V. Larios-Rosillo, P. Vintimilla Tapia, I. Yuquilima, and J. Jara, 'Social engineering as an attack vector for ransomware,' pp. 1-6, 2017, doi: 10.1109/CHILECON.2017.8229528. [Accessed: 04- Nov- 2021].

[27] K. Donegan, '3 ransomware distribution methods popular with attackers', 2021. [online]. Available: https://searchsecurity.techtarget.com/feature/3-ransomware-distribution-methods-popular-with-attackers. [Accessed: 04- Nov- 2021].

[28] L. James, 'Phishing Exposed. Rockland, MA: Elsevier Science,' pp.2-3, 2014, [Accessed: 04- Nov- 2021].

[29] SOPHOS, 'What are Signatures and How Does Signature-Based Detection Work?', 2020. [online]. Available: https://home.sophos.com/en-us/security-news/2020/what-is-a-signature. [Accessed: 05- Nov- 2021].

[30] C. Point, 'Signature-based security solutions can leave networks defenseless for months', 2020. [online]. Available: https://blog.checkpoint.com/2016/09/27/signature-based-security-solutions-can-leave-networks-defenseless-for-months/. [Accessed: 05- Nov- 2021].

[31] L. Jeffery, V. Ramachandran, 'Why ransomware attacks are on the rise — and what can be done to stop them', 2021. [online]. Available: https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them. [Accessed: 05- Nov- 2021].

[32] cybereason, 'Three Reasons Why You Should Never Pay Ransomware Attackers', 2021. [online]. Available: https://www.cybereason.com/blog/three-reasons-why-you-should-never-pay-ransomware-attackers. [Accessed: 05- Nov- 2021].

[33] K. Towndrow, 'Cyber Security Incident Response – Ransomware Attack', 2021. [online]. Available: https://first-response.co.uk/cyber-incident-response-ransomware-attack/. [Accessed: 05- Nov- 2021].

[34] D. Jose, 'Cybersecurity spending must rise - Data breaches cost money: companies must invest to counter cyber attacks', 2021. [online]. Available: https://www.gbm.hsbc.com/insights/global-research/cybersecurity-spending-must-rise. [Accessed: 05- Nov- 2021].

[35] D. Jackson, 'Social Engineering Attacks: A Path to Ransomware', 2020. [online]. Available: https://www.netstandard.com/social-engineering-attacks-a-path-to-ransomware. [Accessed: 05- Nov- 2021].

[36] D. Ellis, 'What is an incident response plan for cyber security? Learn how to manage a data breach with the 6 phases in the incident response plan', 2021. [online]. Available: https://www.securitymetrics.com/blog/6-phases-incident-response-plan. [Accessed: 05- Nov- 2021].

[37] J. Cawthra, M. Ekstrom, L. Lusty, J. Sexton, J. Sweetnam, 'Data Integrity Detecting and Responding to Ransomware and Other Destructive Events', 2020. [online]. Available: https://www.nccoe.nist.gov/sites/default/files/legacy-files/di-detect-respond-nist-sp1800-26-draft.pdf. [Accessed: 05- Nov- 2021].

[38] P. Cichonski, T. Millar, T. Grance, K. Scarfone, 'Computer Security Incident Handling Guide; Recommendations of the National Institute of Standards and Technology', 2012, doi:10.6028/NIST.SP.800-61r2. [Accessed: 05- Nov- 2021].

[39] C. Harrell, 'Malware Root Cause Analysis – Don't Be a Bone Head', 2014. [online]. Available: https://its.ny.gov/sites/default/files/documents/corey-harrell.pdf. [Accessed: 06- Nov- 2021].

[40] Infocyte, 'Root Cause Analysis: Finding Patient Zero During a Cyber Security Incident', 2021. [online]. Available: https://www.infocyte.com/blog/2019/02/21/root-cause-analysis-finding-patient-zero-during-cybersecurity-incident-response-investigations/. [Accessed: 06- Nov- 2021].

[41] D. Finger, 'Endpoint Detection and Response is a Key Weapon in the Battle Against Ransomware', 2021. [online]. Available: https://www.csoonline.com/article/3619556/end

point-detection-and-response-is-a-key-weapon-in-the-battle-against-ransomware.html/. [Accessed: 06- Nov- 2021].

[42] L. Laporte, 'Is it possible to reverse ransomware encryption?', 2017. [online]. Available: https://techguylabs.com/episodes/1363/it-possible-reverse-ransomware-encryption/. [Accessed: 06- Nov- 2021].

[43] B. Nieuwesteeg, 'We must take down the criminal ransomware business model', 2021. [online]. Available: https://www.eur.nl/en/news/we-must-take-down-criminal-ransomware-business-model/. [Accessed: 06- Nov- 2021].

[44] FBI, 'SCAMS AND SAFETY', 2021. [online]. Available: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware/. [Accessed: 06- Nov- 2021].