Ransomware Attacks: - Impact, Symptoms, Working, Preventive Measures and Response

Anant Gangwar

Abstract*: Ransomware is the malware that breaches the protection of the system by using malicious codes. Modern ransomware families, encrypt certain file types on compromised systems. The attacks not only focused on a particular individual, but many organizations and institutions are also involved. New threats to the education sectors and similar organizations are centered here. Possible identification, prevention methods & responses to the rising ransomware attacks explained to combat them efficiently. The main ground of this research is to identify & understand the working of encrypting ransomware and understand the potential ways to counter them before attacking our systems & networks. Following the methodologies presented in this paper with careful analysis can effectively prevent and avert ransomware attacks.

Keywords: Anti-Ransomware, Prevention and Response, Ransomware, Ransom-Cloud, Threats to Education Sector, Cyber safety.

I. INTRODUCTION

During the pandemic, ransomware attacks have increased significantly. Recently there are many cases of companies, organizations, and authorities like NHAI, US Newspaper company, Mac hit by the ransomware attacks. New ransomware - Maze (attacked NHAI), WastedLocker (US Newspaper Company), Try2Cry (infects USB drives), Avaddon (using Excel Macro 4.0), ThiefQuest & EvilQuest (for Mac).

A. What is ransomware?

Ransomware is a malware that gets installed silently on a victim's computer or cloud then it performs a crypto virology attack that sceptically affects the system, and demands a ransom to decrypt it. Old type ransomware is not difficult for an experienced person to reverse & decrypt. More advanced malware encrypts the victim's data files, which could be on a system or the data of cloud & cloud email boxes (known as Ransom-Cloud), making them inaccessible, and demands a ransom mostly in bitcoins to decrypt them. [1] It causes the loss of important data, intellectual property theft, and defamation. With industries, it can cause a data breach or, the attacker may threaten to expose the most valuable data on publicly available websites. Ransom-Cloud works by sending an email that assures your cloud anti-spam service. When you click on the email to install the service, it will deliver a ransomware payload that encrypts all the emails and attachments.

There are mainly three types of ransomware:

- Scareware: You're likely to be bombarded with pop-ups claiming that the system got infected with malware, but your files are safe. E.g. AdwarePunisher, Total Secure 2009, and XP Antivirus 2009.
- Screen Locker: When you start up your computer, a full screen window appears displaying a message that your computer is locked by the FBI or US Department of Justice saying that an unlawful activity is detected on your computer. And ask for a fine. The FBI never does such screen locking. E.g. Police scam, FBI Money-Pak scam.
- Encrypting Ransomware: It seizes up your files and encrypts the data, asking ransom to decrypt. This one is very dangerous and commonly used by the attackers these days. When the attackers get control over your data & system, there's nothing that can help you restore your files unless you pay the ransom. And still, if you do pay up, there's no guarantee of getting your files decrypted. [2] E.g. Crypto-Locker, WannaCry, Bad Rabbit, Jigsaw, Petya, Locker-Goga.

II. HOW DOES A COMPUTER OR DATA GET ATTACKED BY RANSOMWARE?

Mostly its spread through phishing emails having malicious attachments or by downloading from drive links. Drive-by downloading happens when a user unknowingly hits an infected website and the malware gets installed. It has also spread through social media, web-based instant messaging applications, vulnerable web servers have been misused as an entry point to gain access to an organization's network. Out-dated technology infrastructure, Wi-Fi routers with default passwords, not checking the authenticity of the emails, unconfigured firewall are some of the reasons for your system to be infected. Other types of social engineering attacks like Spear phishing, Whaling, Smishing (SMS phishing), Vishing (voice phishing), Pharming (DNS based phishing - involves the alteration of a system's host files or domain name system), Content-Injection Phishing (inserting malicious code or misleading content into the real websites), Man-in-the-middle Phishing.

A. Impact

- Significant loss of confidential data.
- Interruption to the normal working of the systems.
- Financial costs in restoring data & ransom.
- Possible harm to organization reliability.

Revised Manuscript Received on July 20, 2020.

Anant Gangwar, Gurugram Police Cyber Security Summer Internship, Gurugram, Haryana, India. E-mail: gangwaranant@gmail.com

- Probably an entire cessation of organization progress.

B. Symptoms

- If you find your system function slower than the usual speed, then do check if there's any Trojan running in the background spying your sensitive data or sending to a remote server. [3]
- Usually, Trojans are installed in the systems to steal sensitive data before encrypting the whole data of the victim with malware. After collecting the data, the Trojans then download malware from the remote server or run the pre-downloaded malware (crypto-ransomware) in the system of the victim.
- You are not able to open files. Errors like *corrupted files* or the *wrong extension* will start displaying.
- An alarming message with a countdown will be displayed on your desktop with the instructions for the ransom payment & file decryption.
- There will be files with the names like HOW TO DECRYPT FILES.TXT or DECRYPT INSTRUCTIONS.HTML. [4]

III. WORKING OF RANSOMWARE

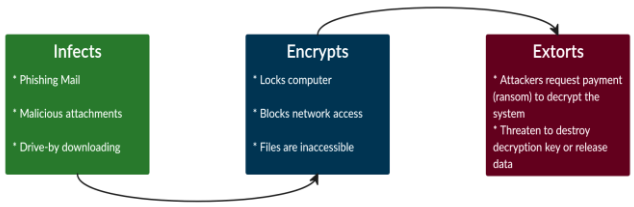


Fig 1. Flow of Infection (Source: CISA Ransomware)

1. Ransomware could be Single-threaded / Multi-threaded. (encrypts one/multiple document/s at a time)
2. It creates the encrypted copy of the files in the smaller chunks in a free available disk to prevent data recovery from the disk; it could encrypt the entire/partial document.
3. Renames the files and changes their extensions.
4. Elevates privileges to SYSTEM by exploiting available vulnerabilities in the older or newer versions of the system/services. And disable Windows Startup Repair.
5. Some ransomware moves the original files to the %temp% folder. A separate application TASKDL.EXE deletes the scrambled originals in the %temp% folder after all documents are encrypted. [5]
6. Deletes volume shadow copies via VSSADMIN.EXE, after the documents are encrypted.
7. Changes the desktop wallpaper.

A. Three-Round Protocol

Steps of three-round protocol of Encrypting Ransomware (between the attacker and the victim):

1. **Attacker → Victim:** The attacker creates a key pair and places the corresponding public key in the malware. The malware is delivered.
2. **Victim → Attacker:** The encrypting malicious software generates a symmetric key randomly and encrypts the files of the victim. The malicious software encrypts the symmetric key with the public key. It is also known as hybrid encryption. It zeroes the symmetric key and real data to prevent data recovery. It displays a warning message on the desktop of the victim, asymmetric cipher and instructions to transfer the money. The asymmetric ciphertext along with the ransom has to be transferred to the attacker by the victim.
3. **Attacker → Victim:** The attacker converts back the asymmetric ciphertext with his private key to the original text after receiving the ransom and sends the symmetric key to the victim. The victim then decrypts the encrypted files using that key.

B. Source Codes

- **WannaCry**– https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Ransomware.WannaCry
- **GonnaCry**– https://github.com/tarcisio-marinho/GonnaCry
- **CryptoLocker**– https://rb.gy/yyjdic
- **Locky**– https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Ransomware.Locky
- **WinLock**– https://github.com/mauri870/ransomware
- **Petya**– https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Ransomware.Petya
- **Jigsaw**– https://github.com/LeechxSys/Jigsawsource

C. Examples

1) WannaCry Ransomware (Biggest Ransomware Attack)

It was May 2017 global cyberattack by the WannaCry cryptoworm, which targeted machines running the Microsoft Windows operating system by exploiting the severe Windows SMB vulnerability, then encrypting data and demanding ransom in the Bitcoin cryptocurrency. Three files presented for analysis. The first file was a dropper, which was responsible for holding & delivering the ransomware via MS17-010/EternalBlue SMBv1.0 exploit. The remaining two files were ransomware segments containing encrypted plug-ins liable for encrypting the victim user's data. [6]

YARA signatures to detect the ransomware:

https://www.us-cert.gov/ncas/alerts/TA17-132A

2) Ryuk Ransomware

It was a worldwide attack which appeared in August 2018. A revised version and having similar properties as of Hermes Ransomware, named as Ryuk. This ransomware was focused and has compromised enterprises only. Its main characteristics - Multi-threaded and encrypts the data available on the mapped network drives. It used to append the Key Binary Large Object (also known as Key BLOB) at the tail of the encrypted document. In this ransomware, two trojans Emotet & TrickBot work together also known banking trojans as they can easily escape signature detections by Antiviruses. Emotet's work is to download the malware & other trojans. Files with exe, dll, or hrmlog extensions not encrypted by Ryuk. [7] TrickBot usually scrapes the confidential data & credentials from the system and sends them to the attacker remotely.

Then ransomware starts encrypting the files after being executed by Emotet. It has made 705.80 BTC, having a current value of $ 6.4 million (USD). But you can prevent it, the response to this kind of ransomware presented in section VII.

IV. WHY SHOULD THE EDUCATION SECTOR WORRY?

- Due to the coronavirus pandemic, every school/college is moving online. Most of the budget of the education institutions is deferred to their curriculum. A very less amount of budget is focused on IT security, training on best practices, and acquiring security tools.
- The technological infrastructure of most of the educational institutions are running on the old or outdated model.
- They usually store sensitive data of children, staff. The attackers misuse their data and threaten the schools for ransom.
- Their website, routers & other devices have default or weak passwords and poor security practices.
- Emotet & TrickBot trojans are increasingly used to attack the education sectors. According to recent reports, these trojans were the fifth-most prominent threat to the schools.
- Emotet & TrickBot usually work together in the attacks on organizations. Emotet downloads the malicious files, and TrickBot spreads the malware in the network parallelly.

V. PREVENTION

- Educating yourself & your employees the new techniques cybercriminals use and discussing the preventive measures organizing the security awareness pieces of training. And giving them basic cybersecurity training. [8]
- Install the Antivirus & Anti-Malware software in the systems for the prevention from newly emerging threats.
- Systems and routers should have proper firewall settings.
- Filter the emails properly to prevent phishing emails from untrusted sources. [9]
- Examine all the emails in the Inbox & Sent box to detect threats and filter malicious or .exe files. To control the spreading of malicious emails. [10]
- Always check the headers, format & design, grammatical mistakes and the authenticity of the mail before following what's instructed in it.
- Hover over the URL attached in the email to see the actual URL behind the attached one. [11]
- To check websites, assure the green lock symbol & "https" at the beginning of the URL Box.
- Using whitelisting switches will be safeguard at the network level and, whitelisting software will block the execution of untrusted applications.
- Backup the data on the trusted cloud service or any separate device/drive rather than create a backup on the same system or any other system connected to the network.
- Systems must have updated Firmware and Antivirus, Anti-Malware installed with the latest patches. Other IoT devices must have updated firmware and better security configurations.
- Keep testing the security of your internet-facing applications, systems & devices and the internal systems by hiring penetration testers. [12]
- Analyze the response of employees to social engineering attacks. Most of such attacks are delivered via emails that spoofs a known enterprise or brand.
- Keep Ryuk, Emotet, TrickBot Emergency Kit. [13]
- Apply proper limits on the permissions of the normal users & employees on installing and running the applications and software from untrusted sources.
- Avoid unknown USBs & devices.
- Avoid enabling macros from email attachments. Opening the attachment and enabling macros will execute the embedded malware on the machine.

VI. ANTI-RANSOMWARE

The architecture merges security with data protection capabilities to protect, detect & recover data from ransomware and malware attacks.

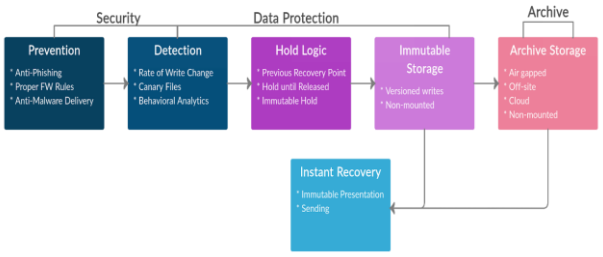


Fig 2. Architecture of Anti-Ransomware [14]

- **Prevention:** Prevents attacks either by isolating web and email attachments or by collapsing those attachments before delivery.
- **Detection:** Canary files & behavioral analytics applied for detection of the ransomware that prevents the system from being attacked.
- **Hold Logic:** When anti-ransomware detects the ransomware, a hold gets placed on a recovery point. That hold includes conversion to a full image & stores the recovery point on some stable storage device or an air-gapped location.
- **Immutable Storage:** This storage provides the ability to do versioned writes where each writer can no longer be changed once written. Each versioned write could be in an image or file format that was protected. It is a duplicate of the target, a secondary set of storage that has a different control plane & interface than the data protection targets. So, if standard targets get attacked, the immutable storage tier can be a recovery source.
- **Archive Storage:** It is the traditionally isolated archive of a data protection architecture. The goal of the archive is to provide a way to recover the business when all else fails.
- **Instant Recovery:** It is a manual process, but gives fast recovery. The gap between detection and recovery is as close to zero as possible.

VII. RESPONDING TO RANSOMWARE ATTACKS

1. If your system is running slower than usual speed, then:
   - Immediately disconnect the system from the connected network.
   - Delete the Trojan and affected files or application.
   - Do a full security check on the system & network while taking necessary precautions.
   - Doing this can prevent the system from being affected by any malware or pre-planned ransomware and will keep your data secure.
2. If attacked:
   - Check the encrypted files by uploading it on sites like https://www.nomoreransom.org, https://id-ransomware.malwarehunterteam.com to identify the type of ransomware.
   - If the ransomware was identifiable, then it would display the name of ransomware and possible solution to decrypt your files.
   - NoMoreRansom project is an initiative to help victims retrieve their encrypted data without having to pay the attackers. [15]
3. If these sites couldn't help you:
   - Then immediately isolate or power-off affected devices.
   - Change all the account passwords & network keys.
   - Take the help of experts.
   - Follow the preventive measures.
   - Contact law enforcement.
   - Delete Registry values & files.
4. Develop & prepare employee training programs for recognizing scams, malicious links, and attempted social engineering.
5. Run frequent penetration tests on the network as often as possible and practical.

A. Decryption Tools

- https://www.avast.com/ransomware-decryption-tools
- https://rb.gy/w5hno8 - KnowBe4
- https://www.nomoreransom.org/en/decryption-tools.html
- https://noransom.kaspersky.com/
- https://rb.gy/9n6nax - Macfee
- https://www.avg.com/en-in/ransomware-decryption-tools
- https://www.quickheal.com/free-ransomware-decryption-tool/

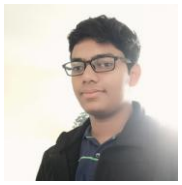
VIII. CONCLUSION

Ransomware is malicious software that comes into effect due to cyber negligence. It takes advantage of the vulnerabilities or negligence and affects the systems then displays warning or a message demanding a ransom to decrypt your data. This research addressed the future concerns and threats to the education sector and other organizations. As the funding of the education sector mainly focused on the education quality, interactive & skill-based activities that support education development; hence there's negligence over the technology infrastructure. And due to this Coronavirus pandemic, they have to shift their whole operation over the internet. Therefore, this sector is most vulnerable and has become the prime target of attackers. There's no doubt that the future attacks would not just be the simple encryption of the files. But we will be dealing with more advanced AI-based ransomware. In this, we have observed that most of the ransomware has similar characteristics and working. Understanding the steps & patterns of attacking the systems by ransomware, we have concluded that it could be prevented in its early stages. So, we believe that the presented preventive measures & responses to these attacks would be beneficial. There is a requirement to follow cyber sanitization, spread awareness among the peer groups, understand the working of malware infections and implement the defensive measures discussed in this paper.

REFERENCES

1. Mark Howard, Unusual Ransomware: Attention Gmail and Microsoft exchange users. Available: https://www.businessit.co.nz/bits-blog/ransomware-alert-gmail-microsoft-users/
2. Wendy Zamora, How to beat ransomware: prevent, don't react. Available:https://blog.malwarebytes.com/101/2016/03/how-to-beat-ransomware-prevent-dont-react/
3. US-CERT, CISA, Ransomware. Available: https://www.us-cert.gov/Ransomware
4. Berkeley Security, Frequently asked questions. Available: https://security.berkeley.edu/faq/ransomware/
5. CISA, Don't wake up to a ransomware attack. Available: https://dhsconnect.connectsolutions.com/pqvnckoanlst/
6. Sophos, How ransomware attacks. Available: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf
7. Sophos, Resolving outbreaks of Emotet and TrickBot malware. Available: https://community.sophos.com/kb/en-us/127218
8. MalwareBytes, Available: https://www.malwarebytes.com/ransomware/ https://rb.gy/nddgru
9. Wendy Zamora, Something's phishy: How to detect phishing attempts. Available:https://blog.malwarebytes.com/101/2017/06/somethings-phishy-how-to-detect-phishing-attempts
10. Peter Arntz, Five easy ways to recognize and dispose of malicious emails. Available: https://blog.malwarebytes.com/101/2018/06/five-easy-ways-to-recognize-and-dispose-of-malicious-emails/
11. US-CERT, Recognizing and avoiding Email Scams. Available: https://rb.gy/rvkuix
12. KnowBe4, Ransomware. Available: https://www.knowbe4.com/ransomware
13. US-CERT, Alerts TA16-091A. Available: https://us-cert.cisa.gov/ncas/alerts/TA16-091A
14. Edward L. Haletky, Anti Ransomware: All about architecture. Available: https://rb.gy/xqfdjg
15. No More Ransom, About. Available: https://www.nomoreransom.org/en/about-the-project.html

AUTHOR PROFILE



Anant Gangwar, I am a Web Security Specialist & Ethical Hacker. I have been actively engaged in the research in Cybersecurity field under the guidance of Mr Rakshit Tandon (Cybersecurity Expert). I have developed several IoT & Web-based projects and prospecting for security tools with better security & usability. Passionately learning Spanish & growing towards the Network Security and Digital Forensics field. Currently, I am pursuing undergraduate studies in Electrical Engineering at Maharaja Agrasen Institute of Technology, Delhi (graduation year - 2022).