Ransomware Threats

Nagaraja Seshadri
REVA Academy for Corporate Excellence
REVA University
Bengaluru, India

Rubia Fathima
REVA Academy for Corporate Excellence
REVA University
Bengaluru, India

***Abstract* - Ransomware is a malware that prevents users from accessing their system or limits their use of the system. It locks the system's screen or the users' files thus preventing them from accessing or using it. Demand for a ransom is made and access is denied unless ransom is paid. Now a days, some modern ransomwares, collectively called as crypto ransomware can encrypt certain file types on infected systems. The users are then forced to pay the ransom through certain online payment methods to get a decryption key.**

Ransomware incidents are targeted at various organizations across industries and geographies and have brought a threat of disruptive and destructive attacks.

The purpose of this paper is to examine and raise awareness on ransomware attack, its effects, and some of the preventive measures from both general and technical perspectives.

Keywords - Ransomware; Attack Vectors; MITRE ATT&CK; Malware; Kill Chain; Crypto and Locker

I. INTRODUCTION

Ransomware is a type of malicious software which encrypts data stored on computer networks with the intention of getting financial gains by selling the target's information.

Ransomware attacks are increasing day by day as also the variety of ransomwares. The number of reported incidents has spiked exponentially as well as the amount that the cyber hackers are extorting from the organizations. Below Fig.1 explains how Ransomware works [1].

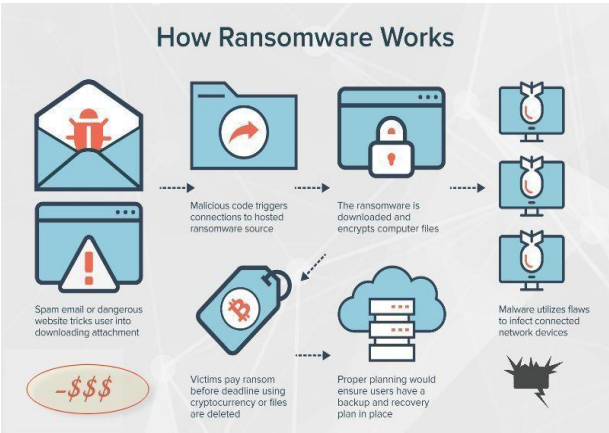

Fig. 1. Ransomware attack

However, the payment of ransom does not guarantee the encrypted files will be released. Similarly, when attackers send back the decrypted files after being paid the ransom that does not mean that the malware was removed from the attacked system.

Ransomware uses robust algorithms for encrypting data efficiently and it is exceedingly difficult to decrypt and restore the files. Ransomware can spread through critical vulnerabilities in the network, which may be through malicious email attachments, by blocking access to important files and a notification of demanding payment. The invention of cryptocurrencies gave the attackers an added advantage of anonymity.

II. IMPACT OF RANSOMWARE

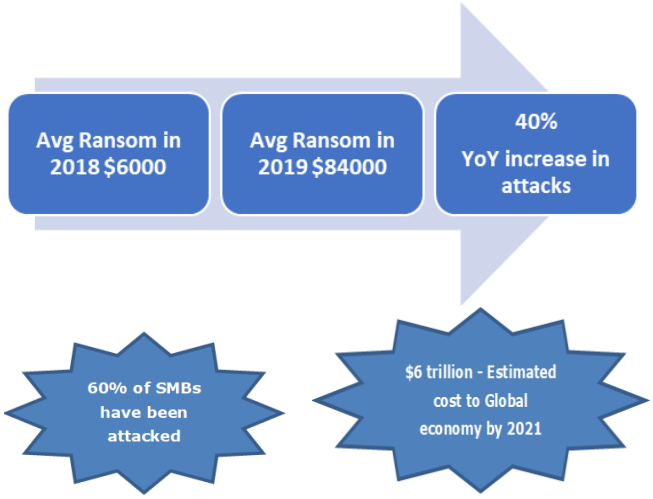

Fig. 2. Ransomware impact

Ransomware attacks have impacted the industries with loss of sensitive data and loss of hundreds of millions of dollars annually across the globe. Statistics show most of the companies that suffered a major attack filed for bankruptcy later.

III. RANSOMWARE KILL CHAIN

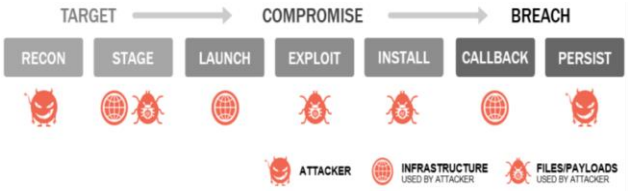

Fig. 3. Ransomware Kill Chain

Ransomware Kill Chain is depicted in the above Fig.3 [2].

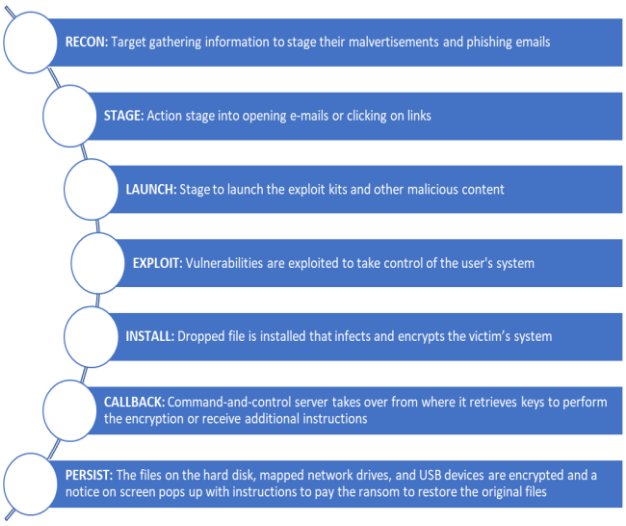

Fig. 4. Ransomware Kill Chain Details

IV. RANSOMWARE ATTACK VECTORS [3]

- Files and Apps - by shadow-IT, Drop Box shared folder, files and applications can be infected images or infected pirated applications.
- Exploit Kits - by means of toolkits to exploit multiple vulnerabilities in operating systems, third-party software, hardware etc.
- Malvertising - by ads which are basically pieces of software that perform malicious activities like download and install malwares.
- Compromised Websites - by attacking through the malicious website from where malware is downloaded and installed
- Phishing - by sending an email message to impersonate an official or familiar sender, urging to click open an attachment or click a link which in turn downloads and runs the malware.
- Instant Messaging - by acting as a graphics file to drop a malicious file while bypassing traditional file extension filters through instant messengers like WhatsApp and Facebook Messenger.
- Remote Access - by hijacking an RDP connection or brute-force their way into the network through an open RDP connection.

Below Fig.5 shows the Ransomware Attack Vector [4].

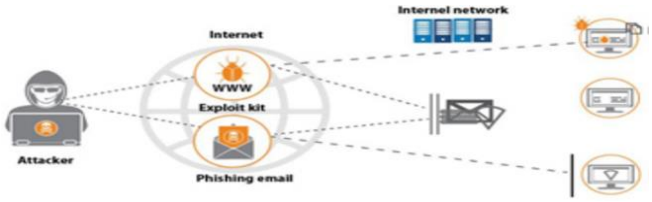

Fig. 5. Ransomeware Attack Vector

V. RANSOMWARE TYPES [4]

A. *Crypto Ransomware*

Crypto ransomware is a type of ransomware attack that finds and encrypts the organization's vital data stored on the network, making the data not usable unless the user gets the decryption key.

B. *Locker Ransomware*

Locker ransomware usually lock a victim's devices by affecting the operating system and applications and the network from performing usual operations and demanding the user to pay a ransom fee to restore it for use.

VI. RANSOMWARE FAMILY [4]

Ransomware families dominate with unique characteristics such as the system or device they infect, the kinds of files they target and the ransom amount. Many users, institutions, industries, and organizations have been exposed to ransomware threats, resulting in considerable financial and reputational loss.

Fig. 6. Ransomware family

- The **Petya Ransomware**, a malware that infects a target infrastructure, encrypts the crucial data from the server, and provides a message with a timeline explaining how

they can pay to get their data back. It can self-spread like a worm by attacking computers and spreading using the Eternal Blue exploit.

- The **WannaCry Ransomware** targets Microsoft's widely used operating systems by encrypting the crucial data, critical documents, and files. This attack preyed on unsuspicious users by get the most out of on an imperfection in the structure of Microsoft windows operating systems referred to as server message block protocol.

- The **Bad Rabbit Ransomware**, a malware distributed through drive-by downloads on infected websites, are tricked into clicking the malware by falsely alerting them that their adobe flash player requires a vital update.

- The **Crypto-locker Ransomware**, a malware which encrypts files using AES with a random key, which is then encrypted with a 2048-bit RSA public key by entering through a protected network through email, file sharing, and downloads.

- The **Locky Ransomware**, a malware uses RSA-2048 + AES-128 with Electronic Code book mode to encrypt files, infection involves receiving emails that contain a Word document, spreadsheet, PowerPoint, zip file, etc., where the attachment is infected using malicious macros.

- The **Crypto wall Ransomware**, a malware which is a file-encrypting ransomware program that targets earlier versions of windows. crypto-wall encrypts data by checking through its command-and-control server and reporting the IP address of the infected computer by taking control of database.

- The **Ryuk Ransomware**, a malware which identifies and encrypts files along the network, while at the same time deleting the shadow copies stored on the endpoints which includes the process starts with phishing attacks and later branches into network mapping, password scraping, and droppers in different combinations.

VII. MAZE RANSOMWARE ANALYSIS

The Maze ransomware is a malware created to disrupt and steal information by moving across the network to encrypt files in the systems for extortions. Its intrusion method includes creation of malicious crypto currency sites, copying government agency sites and security product companies.

This attack is targeting IT, Banking, Healthcare and other sectors by delivering emails with MACRO attachments that include FALLOUT or SPELEVO exploit kits.

Fallout Exploit kit [5] takes the user's browser profile patterns and distributes malicious content to the user who is redirected from the original page to the exploit kit landing page URL. Discovered in August 2018, this exploit kit gains access through Adobe Flash Player and Microsoft Windows flaws. The attacker downloads additional malware onto the victim's computer during the effective infection.

The Spelevo Exploit Kit [6] is used to deliver ransomware to internet users via Adobe Flash Player vulnerabilities. It is used to gain access to remote systems via corrupted advertisements, spam emails with fixed scripts, misleading Adobe Flash Updates.

Attack Stages

Maze ransomware TA2101 threat actor uses 2048-bit RSA and the ChaCha20 stream cipher to encrypt files, adds different extensions to the files throughout the encryption progression.

The user's desktop wallpaper is changed to a message about the encrypted files and the ransom note filename is dropped. The labels used to specify the computer types are like home computer, standalone server, backup server, primary domain controller, etc. Fig.7 below shows the various stages of attack [7]

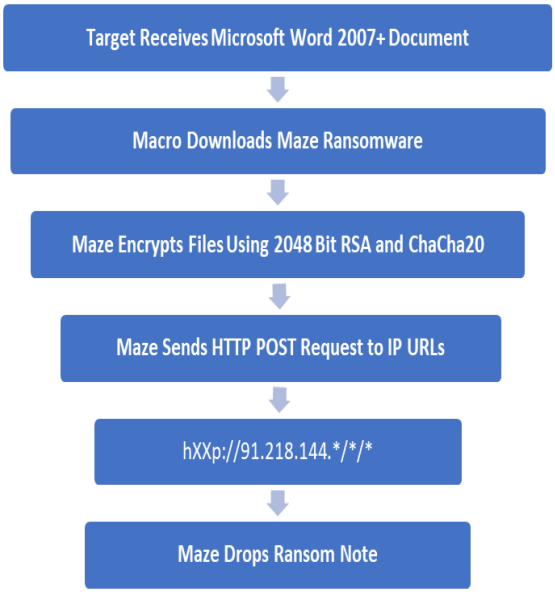

Fig. 7. Maze Ransomware Attack Stages

Ransomware Note

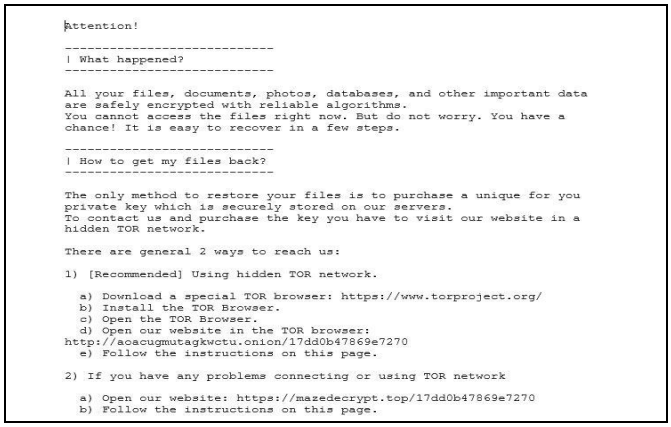

Fig. 8. Ransomware Note

Above Fig.8 shows a typical Ransomware note [8]. The ransomware amount is based on the device type it detects during the attack.

VIII. Preventive Stategy for Ransomware

MITRE ATT&CK™ MATRIX [9]

MITRE Corporation, an American non-profit organisation developed ATT&CK as a model to document and track techniques attackers use during the different stages of a cyberattack to intrude the network and breach the data. Below Fig.9 compares MITRE ATT&CK can Cyber Kill Chain [9].

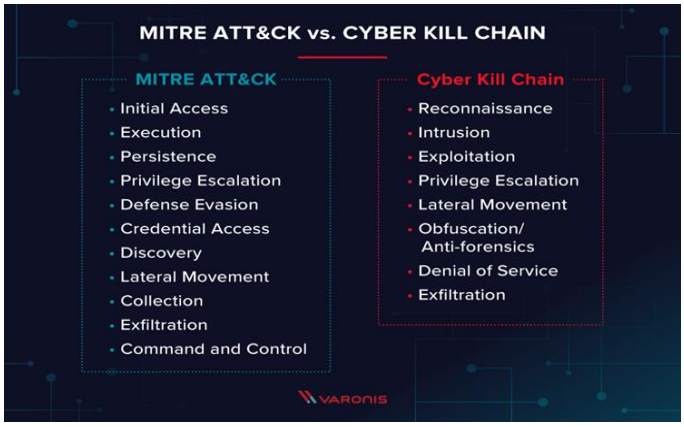

Fig. 9. MITRE ATT&CK Matrix

ATT&CK [10] specifies Adversarial Tactics, Techniques, and Common Knowledge. The framework is a pattern of various cyberattack techniques classified by different tactics.

Based on MITRE ATT&CK framework, mitigations can be designed at three levels:

- **Assessment** – analysing current configuration and security practices to find security vulnerabilities and holes by testing Weak Passwords, Privileged Accounts, detect misconfigurations, open RDP servers with no NLA, servers with no SMB signing, etc
- **Detection** – monitor network traffic and data continuously and detect malicious activity simultaneously. Credentials detection by scanning, dumping domain hashes, creation of fresh privileged accounts, or code execution in the domain controller, etc
- **Prevention** – by defining clear custom conditional access policies to block access or trigger MFA based on varying behaviour pattern, this well-defined approach reduces user conflicts when accessing applications and resources.

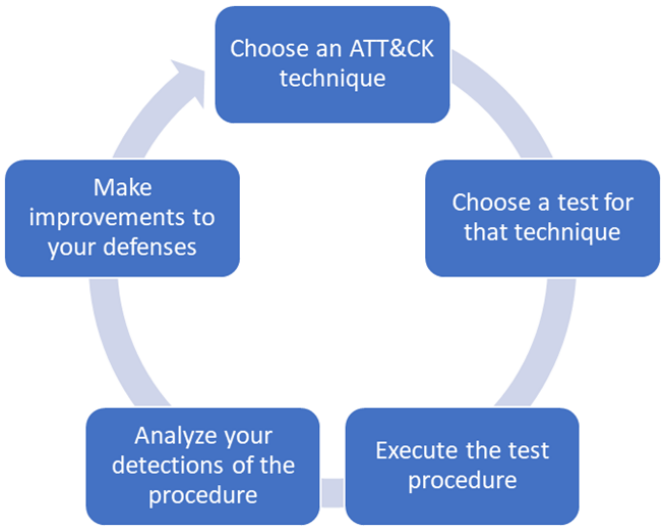

Fig. 10. MITRE ATT&CK Mitigation Steps

Mitigation steps in the MITRE ATT&CK framework [10] is shown in the above Fig.10.

IX. PREVENTIVE MEASURES [11]

- Install ad blockers to fight exploit kits that are distributed via malicious advertising.
- Protect personal/official devices with licensed Antivirus.
- Implement strong email security protection software that detects Word attachments which is possibly implanted with malicious macros.
- Lockdown Remote Desktop Protocol.
- Deploy effective backup plans including keeping the backup safe at remote location, so that they can be used to recover lost data in the event of breach.
- Use legitimate VPN services instead of free services.
- Enforce sessions with specific time periods.

- Adopt advanced protocols like IPSEC to establish a connection,
- Enforce multifactor authentication in advance for every user activity.
- Do not plug any unattended external media into the devices.
- Validate sender's emails IDs before opening an email.
- Install a sandbox solution to detect malware not detected by antivirus software.
- Perform regular updates of operating systems and application software

X. CONTAINMENT, RECOVERY AND RESPONSE [12]

- **Network traffic analysis**: To limit the ransomware's ability to spread and create damage by monitoring network traffic, detect suspicious communications that cannot be detected by signature-based security systems, analyse and block data on end devices.

- **Malware analysis:** To detect paths quickly and efficiently, keep malicious code from becoming fixed in systems while preventing the infrastructure from being re-infected, neutralize threats that have already spread and become deep-rooted.

- **Forensic analysis:** To identify where the compromise originated, how the attackers moved across the network, what tools were used and what vulnerabilities were exploited

It is crucial to recover from the attack and to quickly return to normal IT services and business operations.

XI. CONCLUSION

The cybersecurity world is advancing at a rapid pace and attackers are targeting the victim with new tactics to attain their goals. Frameworks like MITRE ATT&CK are essential to developing a stronger cybersecurity program. With proper implementation of ATT&CK framework, security team will be able to measure the efficiency of their security program.

Simple steps like monitoring for weak passwords, limiting account privileges, and enforcing strict authentication steps can reduce most of the risk of being the ransomware victim. It is essential for computer users to follow the general and technical protective procedures to reduce such attacks.

REFERENCES

[1] Dealing with Cyber Crime in 2019 by Peter Bowey Computer Solutions. https://www.peterboweycomputerservices.com.au/blog/dealing-with-cyber-crime-in-2019
[2] Combating Ransomware challenge with Cisco Ransomware Defense solution - Cisco Security Newsletter-Issue 7_June 20
[3] Seven Ways Ransomware Infects Your Network – https://www.maya-security.com/blog
[4] Ransomware attack – what is it and what is it impact – https://blog.eccouncil.org/ransomware-attack-what-is-it-and-what-is-it-impact/
[5] Fallout Exploit Kit is Back with New Vulnerabilities and Payloads by Sergiu Gatlan – https://www.bleepingcomputer.com/news/security/fallout-exploit-kit-is-back-with-new-vulnerabilities-and-payloads/
[6] Spelevo EK Exploits Flash Player Vulnerability to Deliver Maze Ransomware by David Bisson – https://securityintelligence.com/news/spelevo-ek-exploits-flash-player-vulnerability-to-deliver-maze-ransomware/
[7] MAZE Ransomware Campaign spoofs Italian Revenue Agency Correspondence – https://www.infoblox.com/wp-content/uploads/threat-intelligence-report-maze-ransomware-campaign-spoofs-Italian-revenue-agency-correspondence.pdf
[8] MAZE Ransomware NASSCOM-DSCI Advisory – https://www.dsci.in/sites/default/files/Maze_Ransomware_Advisory.pdf
[9] MITRE ATT&CK Framework – https://www.varonis.com/blog/mitre-attck-framework-complete-guide/
[10] Getting Started with ATT&CK: Adversary Emulation and Red Teaming by Blake Strom – https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3
[11] What is MITRE ATT&CK: An Explainer by Tim Matthews Chief Marketing Officer – https://www.exabeam.com/information-security/what-is-mitre-attck-an-explainer/
[12] Ransomware Uncovered: Attackers' Latest Methods – https://www.group-ib.com/whitepapers/ransomware-uncovered.html