Cybercrime Prevention Guide

Name

Institution

Class

Professor

Date

Cybercrime Prevention Guide

Cybercrime refers to any criminal activity that targets or uses a computer, network devices, or a computer network to carry out illegal activities such as fraud, trafficking, theft of intellectual property, and computer piracy (Brewer et al., 2019). It threatens the safety and operations of organizations and individuals when not detected early, prevented, or mitigated. Some of the common cybercrimes that threaten organizations today are ransomware (a form of malware) attacks, phishing, and Distributed Denial of Service (DDoS) (Brewer et al., 2019). Other forms of cybercrime reported frequently by organizations include email and internet fraud, theft and sale of corporate data, identity fraud, theft of financial/credit card data, cyberextortion, cyber espionage, network hacking, and copyright infringement (Brewer et al., 2019). This paper presents a cybercrime prevention guide that can be applied by the public and organizations to prevent and mitigate cybercrime.

Ransomware

A ransomware attack is one of the most common forms of cybercrime that may compromise the organization's operations and sustainability. It is malware that uses the encryption technique to lock out legitimate users from accessing their files until they pay a ransom within the specified time limit to have their files decrypted by the attacker and made accessible (Manjezi & Botha, 2019). Ransomware may also render the system unusable if it relies on encrypted files. In most cases, the ransomware attackers demand monetary ransom to decrypt the files. If the file owner fails to pay the ransom within the specified time limit, the files get permanently deleted, resulting in permanent data loss if no backup is done.

How Ransomware Attack Occurs

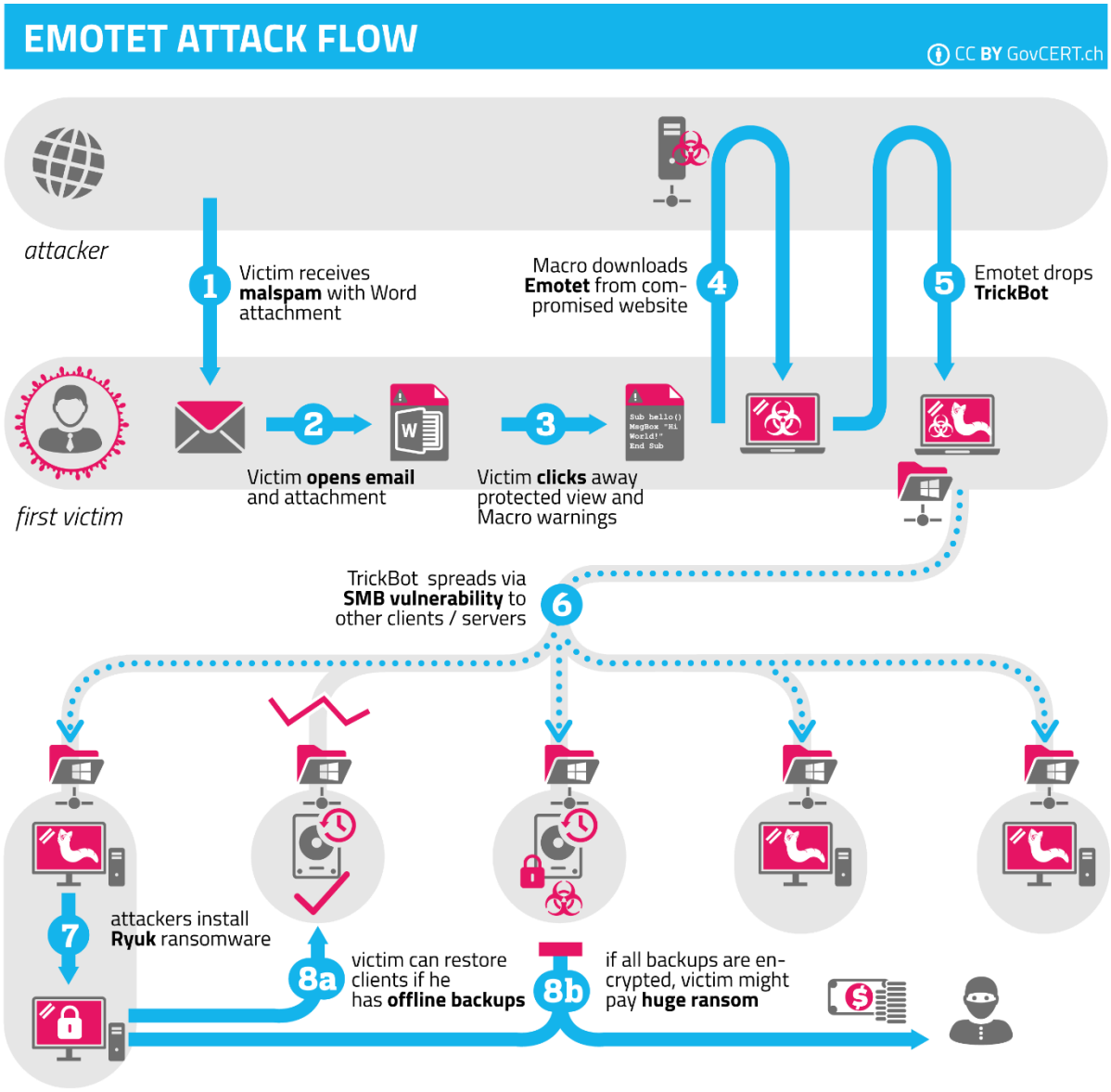

Figure 1: Ransomware attack process

The initial step of a ransomware attack involves the attacker sending phishing mail with a malicious link or attachment to the target computer. If the unsuspecting user clicks the link or opens the attachment, a malicious file is downloaded and installed into the computer without the user's knowledge, as shown in *fig.1*. The trojan quickly spreads to other clients or serves on the network via the Server Message Block protocol (SMB protocol) and installs the ransomware in all devices connected to the servers (GovCERT.ch, 2019). It encrypts as many files as possible to

ensure the user is completely locked out. At this stage, the legitimate user is locked out and cannot access the files until the ransom is paid as directed on the screen, as in *fig.2*.

Figure 2: Ransomware attack example

The attackers usually demand the ransom to be paid in cryptocurrency (bitcoins) to conceal their identities. They prompt the user to feed the payment details to complete the transaction and retrieve the private key to decrypt the files (Manjezi & Botha, 2019). Ransomware attackers use dark web browsers such as Tor and DuckDuckGo to prevent users from identifying their identities. During the payment process, the attacker may further steal the payment details and transfer all the funds to the organization's or individual's account.

Indicators of an Ongoing Ransomware Attack

Numerous organizations lack the necessary visibility and detection tools, and resources to detect and prevent ransomware. Some ransomware attacks take hours, while others vary from days to weeks or months. Regardless of the time taken, the organization should be aware of the following signs as they often indicate a ransomware attack in progress.

Suspicious Emails (Phishing)

The ransomware attack usually starts with a phishing email containing a malicious link or attachment. The attackers send social engineering emails that appear legitimate to lure the user into clicking the malicious link or opening the attachment to create an attack vector (Mixon, 2021). Users should always avoid clicking suspicious links or opening unknown attachments. They should also report suspicious emails received out of operation time or received when no email is expected from such a client. Frequent suspicious emails are clear indications of a potential or ongoing ransomware attack. Organizations should train all their staff on cybersecurity measures to equip them with the knowledge to differentiate phishing emails from legitimate emails.

Unexpected Network Scanners

The unexpected network scanners that keep popping up on the network but are unknown and have no value to the organization, particularly on the server network, indicate ransomware attacks (Mixon, 2021). Cyberattackers use such scanners to dig into the network to find the server protocols and identify additional vectors to exploit and further the attack to other systems connected to the network (Mixon, 2021). The organization should be aware of unexpected scanners because the attackers often use advanced network scannings tools like the Advanced Port Scanner and AngryIP to scan the target network domains.

Presence of MimiKatz and Microsoft Process Explorer

MimiKatz is a Windows (x32/x64) software program that extracts passwords, PINS, hash, and Kerberos tickets from memory (Mixon, 2021). The presence of MimiKatz is a red flag indicating an ongoing ransomware attack. This open-source tool for gathering credentials is one

of the most common tools used by hackers to steal individuals' access codes, passwords, and authentication information (Mixon, 2021). The presence of MimiKatz and Microsoft Process Explorer (MPE) is worse because the attackers use the legitimate MPE to convince the user that everything is okay while they attempt to penetrate the network. The organization should perform ethical hacking (penetration testing) to ensure the network is secure and the attackers cannot penetrate the network's security system.

Presence of Software Removal Programs

The presence of software removal programs is a clear indication of an ongoing attack. Whenever the attacker gains administrative privileges in the system, the first step is to disable or remove the security software like the antivirus (Mixon, 2021). They often use legitimate application removals software such as the Process Hacker, PC Hunter, and IOBit Uninstaller to remove the programs (Mixon, 2021). Although this is a late-stage indicator, the user can still mitigate the attack impacts by reacting immediately to stop the ransomware from removing the software.

Small-Scale Dry Run Test Attacks

The attackers usually run the simulation of the ransomware attack through a small-scale dry run to identify network or endpoint vectors to exploit (Mixon, 2021). The simulation helps them determine the best attack point to use to achieve their goals. The organization should implement advanced security tools like endpoint detection and response tools or SIEM to detect smaller ones before they lead to a severe ransomware attack.

How the organization can Prevent Ransomware Attack

Provide Cybersecurity Education and Training to all Employees

Ransomware occurs when the unsuspecting member of the organization whose computer is connected to the organizational network clicks a malicious link or opens a similar attachment. In most cases, such individuals lack the knowledge and awareness to differentiate between legitimate and phishing emails. Educating and training the employees continuously on cybersecurity best practices promotes their awareness and help them avoid falling into the traps of attackers. This enables the organization to prevent ransomware from occurring.

Regular System and Software Update

The organization should regularly update its security systems and software to ensure the latest security measures are enforced. For example, the organization should implement cloud SIEM and endpoint detection and response tools to prevent, detect, report, and respond to suspected ransomware attacks. Updating the existing systems and software helps seal the vulnerabilities that the attacker can exploit to carry out the ransomware attack. This will help prevent and mitigate the impacts of future attacks.

Preventive Measures

To prevent ransomware attacks, the organization should encourage all employees to carefully examine the email addresses in all the corresponding emails and thoroughly scrutinize the website URLs before clicking them or replying to the email (US.Gov., n.d.b). Another vital measure is creating strong and unique access codes with multi-factor authentication for every online account to enforce strong security (US.Gov., n.d.b). No payments should be sent to unknown people or organizations, especially those seeking urgent financial support (US.Gov., n.d.). All unexpected emails or attachments should not be reported and should instead be reported to the cybersecurity team to assess them.

The system and security software should be regularly updated to keep off attackers that use new approaches to launch the attack. No personal or organization's sensitive information should be shared on online platforms such as social media to prevent potential attackers from accessing them (US.Gov., n.d.a). Network segmentation should be implemented to protect the corporate network from attacks launched through the public network. The network and database servers with critical organizational information should be segmented from the public network to keep them safe when the public network is attacked (GovCERT.ch, 2019). Finally, the organization should back up all its information remotely in real-time to prevent permanent data loss in case an attack occurs.

References

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. Springer Nature.

Manjezi, Z., & Botha, R. A. (2019). Preventing and Mitigating Ransomware. In *International Information Security Conference* (pp. 149-162). Springer, Cham.

Swiss Government Computer Emergency Response Team (GovCERT.ch). (2019). Severe Ransomware Attacks Against Swiss SMEs.

US.Gov. (n.d.a). The Cyber Threat***. Cyber Crime.*** https://www.fbi.gov/investigate/cyber

US.Gov. (n.d.b). Ransomware Guide. *Stop Ransomware.* https://www.cisa.gov/stopransomware/ransomware-guide