Kaylyn King, Tasmania Tamboli, Jean-Charles Hekamanu, Ujjwal Rana Magar
CSCE 5550
Spring 2025

Literature Review: Ransomware

Ransomware is a common malware attack where an attacker holds a victim's files at ransom through asymmetric encryption, asking for money or an action to give the victim the private key. About 623.3 million ransomware attacks happened globally in 2021 with phishing being the most common entry point (Imber, 2025). However, any vulnerability present within an organization's digital and physical infrastructure can create an entry point for an attacker to execute a ransomware attack. This review will dive deeper into three common ransomware tactics to gain access to the files: phishing, man-in-the-middle attacks, and outdated software (RecordedFuture, n.d.).

Phishing is when an attacker creates a fake email, phone call, text message, or any other digital means to deceive a person into thinking it is real (KnowBe, n.d.). Once the victim is successfully deceived, the victim will unknowingly give the attacker sensitive information. This is very prevalent in a workplace environment when an attacker poses as another employee or manager to gain access to authorized information through an employee's credentials. The attacker can take this information, encrypt it, and send a ransomware ad to the CEO or a higher positioned employee of the organization for money. To prevent these phishing scams, companies can implement Simple Mail Transfer Protocol (SMTP) filtering to block or flag potential malicious email addresses. They can also implement employee training establishing the idea of "too good to be true" and typosquatting (KnowBe, n.d.).

Man-in-the-middle attacks are where an attacker secretly eavesdrops on a conversation between a sender and a receiver. The sender and receiver could be systems and/or people. Attackers are able to obtain personal information by intercepting a sensitive conversation or by posing as the sender or receiver. A common access point for these attacks is through

software-as-a-service applications like messaging services or remote worker applications where sensitive information is communicated (CrowdStrike, n.d.). Usually, attackers target an organization as a whole by gaining an individual's credentials rather than just stealing the individual's private information. With these credentials, they can gain access to the organization's sensitive files and implement their ransomware attack. A simple prevention technique for this attack is to use secure protocols like the Simple Mail Transfer Protocol Secure (SMTPS) and Hypertext Transfer Protocol Secure (HTTPS). These protocols use Transport Layer Security to ensure secure communication on the ports. An organization could also use a virtual private network (VPN) within their local network for more secure communications as well (Rapid7, n.d.).

Outdated software presents many vulnerabilities for different types of cyberattacks especially for ransomware. An attacker can find an organization using software that is not supported anymore, meaning the security of the software is not being updated. This makes it easier to find a zero-day vulnerability within the organization's infrastructure. Once this vulnerability is found, the attacker can insert malicious code to gain elevated privileges or spy on the victims to retrieve sensitive information, making it easy to encrypt sensitive files to implement a ransomware attack. The main thing to do to prevent this is update all software regularly. If the organization needs to use a legacy system, then they should separate it from the rest of the network so it does not cause a greater effect if a breach happens.

Once a vulnerability is found, there must be a way to exploit it. A common tactic is to secretly run an executable on the victim's machine to find the most valuable files. Most ransomware uses asymmetric encryption to encrypt the files once they are found

(*What Is Ransomware? | Trellix*, n.d.). Here, the attacker uses a pair of private and public keys with the private key being the one to decrypt the files when the ransom is paid. The victim is likely to pay it especially if they have not backed up their files, making it a good attack to steal money from the victim.

Any vulnerability presents a way for an attacker to deploy a ransomware attack. Therefore, it is important for organizations to decrease the attack surface, so that the entry points to the system are reduced to a more manageable state. Although it is important to focus on all potential entry points to conduct ransomware attacks, our group is focusing on the phishing tactic by deploying a fake website to host our encryption script which will then encrypt the user's file using asymmetric encryption.

References

Imber, D. (2025, January 22). The Latest Ransomware Statistics (updated January 2025) | AAG IT Support. *AAG IT Services*. https://aag-it.com/the-latest-ransomware-statistics/

Ransomware 101 | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/stopransomware/ransomware-101

RecordedFuture. (n.d.). *Top 6 Ransomware Attack Vectors (And how to Prevent them in the Enterprise)*. https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/ransomware-attack-vectors

KnowBe. (n.d.). *Phishing | What is phishing?* https://www.phishing.org/what-is-phishing

Man in the Middle (MITM) attack. (n.d.).

https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/man-in-the-middle-mitm-attack/

Man In the Middle (MITM) Attacks - Definition & Prevention | Rapid7. (n.d.). Rapid7.

https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

What is ransomware? | Trellix. (n.d.). Trellix.

https://www.trellix.com/security-awareness/ransomware/what-is-ransomware/

Kaylyn King, Tasmania Tamboli, Jean-Charles Hekamanu, Ujjwal Rana Magar
CSCE 5550
Spring 2025

Project Plan

Action

We will use OpenSSL with AES-256-CBC inside a bash script executable.

Infection

We will send a phishing email to the user and convince to download and execute the malicious executable file.

Monitoring

We will use Python's watchdog to watch over critical files combined with the "auditctl" program to see which process is editing the files.

Detection

We deploy a honeypot to see if the files are being access in an unauthorized manner. We will also see if the process that is editing the directory is leaving suspicious extensions such as ".encrypted".

Mitigation

We suspend the process that is detected as suspicious and ask the user if they want to kill it. We will also shut down the directory while the process is suspended.