CSCE 5550 Spring 2025 Project "Ransomware"

Group - 3

Anila Arram - 11719939

Durga Shankar Dalayi - 11757864

Sai Keerthana Thummalapalli - 11695371

Mounika Yarram - 11710264

Research on Ransomware Techniques

Malicious software (malware) used to deny a computer user the right of access to their computer system or data until a payment demanded by a hacker is made. Ransomware is one of the biggest cybersecurity threats of recent years, and gets distributed through phishing emails, exploit kits or by means of visiting a malicious site. In this research we will show the types of ransomwares and how it works, the encryption techniques used for this and the infection methods that can be seen on modern ransomware attacks.

Types of Ransomwares

crypto ransomware and locker ransomware are both forms of ransomware but with a difference.

1. **Crypto-Ransomware**: Crypto-ransomware breaks into a victim's system, encrypts the victim's files, and makes them unreadable. After hacking the victim's data, the attacker demands payment, and most of the time, they demand it on cryptocurrency as the way to be able to get back into their files with the decryption key. Typically, it's based on asymmetric encryption where the encryption process involves unique public key and decryption requires the hidden private key.

Notable examples of crypto-ransomware include:

- **EternalBlue:** Exploited a vulnerability in the Windows operating system and was used to widespread their rapid spread across networks, and encrypting files. RSA encryption was used that would render files completely undecipherable without the decryption key**.**
- **Ryuk:** An encryption ransomware variant that helps penetrate large businesses and demands its much high ransom payments. It uses AES and RSA together to encrypt the communications**.**

2. **Locker Ransomware**: Instead of encrypting files, locker ransomware blocks the victim out of his system. The attacker assumes control of the system resources, and therefore the victim cannot access the desktop, files, or operating system. Locker ransomware does not always involve encryption, unlike crypto ransomware. The system's access is restored in exchange for ransom demanded by the attacker.

An example of locker ransomware is Win Locker, the ransomware, which locks the screen or operating system before the payment of its ransom.

3. **Double-Extortion Ransomware**: A new trend is double extortion ransomware by which besides files encryption attackers steal sensitive data and threaten data leak if the ransom is not paid. So when victims are threatened with public exposure the pressure is increased as the damage is just as grave as being cut off from files.

How Ransomware Works

First of all, the operation of ransomware can be divided into the following phases: infection, encryption, demand, payment..

1. **The first of ransomware attack is infection. This usually happens through:**
    - There are phishing emails that are sent out with the malicious attachment or a link to a compromised website. Malware is then triggered when the victim opens the attachment or clicks on the link unwittingly.
    - Ransomware can also be delivered through Exploit Kits that spread the malware by attacking software vulnerabilities (old web browsers or plugins) to the victim's machine.
    - Certain types of ransomwares are the result of visiting a malicious website or clicking on a compromised online ad that automatically installs the ransomware on a victim's computer.
2. Once the infection vector has been executed the ransomware is executed in background often presenting itself as an innocent process. With this, it may exploit the system vulnerabilities for privilege escalation and attain the control over the system. In addition, the malware may even disable antivirus software and other security measures to ensure it cannot be detected.
3. On successful infection by the ransomware, it starts encrypting files in the victim's device. Using the sensitive or valuable information files (i.e., documents, images, videos, and database), the attacker encrypts files before making the sensitive data unavailable to the system's users. The most common encryption process is where

almost complex cryptographic algorithms are used to make any file unreadable without decryption.

Encryption Algorithms Used by Ransomware:

- **AES:** It is a symmetric encryption algorithm which is used to offer data security. When it comes to ransomware attacks, AES is usually used to encrypt files. AES is, therefore, fast and secure enough to be used to encrypt large quantities of data**.**
- **RSA –** Rivest–Shamir–Adleman, is used for secure transmission of data through a network using asymmetric encryption algorithm. For key exchange, RSA is usually used in the context of ransomware. The attacker has the corresponding private key to decrypt the files, whereas he gives the victim the public key to encrypt files**.**
- **ChaCha20:** A newer symmetric encryption algorithm, this encryption is growing in use behind some ransomware attacks as many perceive it to be both speedy and secure. It is preferred on hardware where hardware acceleration for AES has not been made available.

4. Once the encryption process is over, ransom crop up to the victim on the ransomware. Typically, the note demands that the receiver of the mail pay a ransom, typically in cryptocurrency such as Bitcoin and will instructs them on how to pay. The ransom note can also provide threats like destruction of the decryption key if payment is not made within a particular period.
5. Payment: The victims will often pay the ransom in order to recover their files. However, the attacker is not required to keep this decryption promise. Admittedly some victims who pay the ransom will find their files are not recovered, or they will be tripped up in an endless campaign of extortion.

Encryption Techniques Used in Ransomware

There are a number of different encryption algorithms used by ransomware that have their own strengths and weaknesses. The type of encryption algorithm used will be based on the type of ransomware and the attacker's goals. Below is some encryption techniques used commonly with ransomware attacks:

1. **Symmetric Encryption** (AES):
    - AES is the most frequently used form of encryption in a ransomware attack. It is fast, secure and efficient for encrypt large files.

- In ransomware attacks, AES is usually used together with asymmetric encryption (RSA) for initial communication (key exchange). In this case, the victim receives an encrypted file and will have to have the decryption key in order to view the file.

2. **Asymmetric Encryption** (RSA):
    - RSA is frequently teamed up with AES. Although AES is much faster and more efficient than RSA, it is very secure in key exchange. In this, the target is provided an encrypted file which can be decrypted only if the private key was under the attacker's control.
    - With RSA, it is impossible for victims to decrypt their files without the private key of an attacker, and thus decides to pay the ransom.
3. **Hybrid Encryption**:
    - Since many current ransomware attacks apply a hybrid encryption, they use both symmetric and asymmetric encryption. RSA encrypts the AES key with which it then encrypts the files with a fast algorithm such as AES. This guarantees speed of AES encryption and security of RSA being used for key exchange.
4. **Fileless Ransomware**:
    - The newer type of ransomware is called o Fileless ransomware, which doesn't work on traditional file-based encryption. It works solely in system's memory hence it's much harder to catch. Ransomware attack of fileless type may do its attack through scripting languages like PowerShell or Windows Management Instrumentation (WMI).

Infection Methods Used in Ransomware Attacks

A successful infection is usually how a ransomware attack starts. Several primary infection methods exist:

1. **Phishing Emails**:
    - One of the most popular infection vectors is phishing emails. Malicious attachments (e.g., PDF files, Word documents), or links to malicious website is included in most of the emails. The ransomware infection is initiated when the victim unknowingly clicks on the attachment/ link.
2. **Exploiting Vulnerabilities**:

- Many ransomware attacks exploit vulnerabilities in software or operating systems. For example, the **EternalBlue** exploit, used by WannaCry, took advantage of a vulnerability in older versions of Windows.
- Ransomware can also be distributed through drive-by downloads or through vulnerabilities in web browsers or browser plugins.

3. **Malicious Ads (Malvertising)**:
    - Malvertising involves embedding malicious code into legitimate online advertisements. When the victim clicks on the ad or views it, the malware is delivered, often without the victim's knowledge.
4. **Remote Desktop Protocol (RDP) Attacks**:
    - Ransomware can also be spread through RDP brute-force attacks. Attackers gain access to a victim's system by guessing weak passwords or exploiting known vulnerabilities in RDP.
5. **Network Propagation**:
    - Some ransomware is designed to spread across a network, infecting multiple machines. Once the initial machine is infected, the ransomware attempts to move laterally through the network to other vulnerable systems.

Conclusion

Ransomware is a persistent and growing threat in the world of cybersecurity. Understanding how it works, the encryption techniques it employs, and the methods of infection it uses is crucial for developing effective mitigation strategies. As ransomware continues to evolve, it becomes increasingly sophisticated, often combining multiple encryption techniques and infection methods to maximize its effectiveness. To protect against ransomware, organizations must implement robust security measures, including regularly updated software, secure backup strategies, and comprehensive user education.