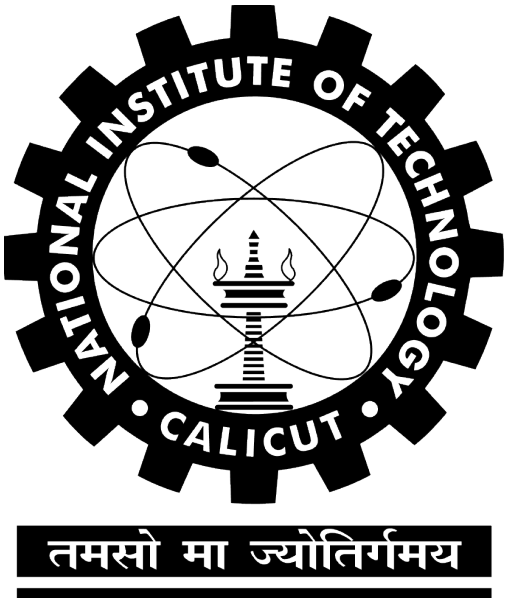
Project Report on

Simple Ransomware Program that Encrypts a Folder

Submitted by

Muhammad Azzaam B190735CS
Muhammed Jaseem Pallikkal B190703CS
Sachin Thomas B190738CS



Department of Computer Science and Engineering
National Institute of Technology Calicut
Calicut, Kerala, India - 673 601

March 26, 2023

Simple Ransomware Program that Encrypts a Folder

Muhammad Azzaam Muhammed Jaseem Pallikkal Sachin Thomas

Abstract: Information security is one of today's highest priorities. Ransomware has evolved as one of the more notable cyber threats in recent times, affecting individuals, businesses, and even government institutions. Ransomwares can cause serious damages such as data loss, financial losses, reputational harm, and operational disruption. These attacks typically block a user from accessing their files or their device itself and then demand a ransom payment in exchange for restoring access. As of late, the number of ransomware attacks has increased significantly, with perpetrators utilizing increasingly intricate methods to prevent detection and maximize revenue. This project's goal is to create a simple ransomware software that encrypts a specified folder. This report consists of a literature review to understand the nature, evolution, trends, and challenges of ransomware attacks and will also look at the technical aspects of the project, such as the various tools, algorithms, encryption methods, and the system environment used to create the ransomware.

1 Introduction

Over the past few years, ransomware has affected millions of people, making it a fast-growing concern. There were around 236.7 million ransomware attacks in the first half of 2022 and it is predicted that a ransomware attack will occur almost every 2 seconds by 2031 [1]. In most ransomware attacks, the target includes personal files such as documents, databases, photos, and videos. The ransom is usually paid through cryptocurrencies such as Bitcoin as they are less regulated and harder to trace than other forms of payment, making them attractive to hackers. Once the ransom has been received, the attacker displays a notice on the compromised computer device indicating the steps to be followed to retrieve the encrypted files [2].

1.1 History of Ransomware

The first known ransomware attack occurred in 1989, when a biologist named Joseph Popp distributed 20,000 floppy disks containing a program called AIDS Trojan to attendees of the World Health Organization's AIDS conference. The program claimed to measure the risk of AIDS infection based on a questionnaire, but it also encrypted the files on the disk after 90 reboots and displayed a message demanding $189 for the decryption key.

However, ransomware did not become widespread until the mid-2000s, when encryption algorithms became more sophisticated and online payment methods such as Bitcoin emerged. Some of the notable ransomware families that emerged during this period include CryptoLocker (2013), CryptoWall (2014), CTB-Locker (2014), TeslaCrypt (2015) and Locky (2016). These ransomware variants used asymmetric encryption to generate unique keys for each victim and communicated with command-and-control servers to receive payment instructions.

1.2 Evolution of Ransomware

Ransomware has evolved over time to become more stealthy, resilient and profitable. Some of the trends observed in recent ransomware attacks include the following:

1.2.1 Double Extortion

In addition to encrypting the victim's data, some ransomware operators also extract sensitive information and threaten to leak it online if the ransom is not paid. This increases the pressure on the victim to comply and prevents them from restoring their data from backups. Examples of double extortion ransomware include Maze (2019), Sodinokibi (2019) and DoppelPaymer (2019).

1.2.2 Targeted attacks

Instead of indiscriminately infecting as many devices as possible, some ransomware operators conduct targeted attacks against specific organizations or sectors that are more likely to pay high ransoms or have critical data or services. These attacks often involve reconnaissance, exploitation of vulnerabilities or phishing campaigns to gain access to the network, and then move laterally to compromise as many systems as possible. Examples of targeted ransomware include Ryuk (2018), BitPaymer (2017) and SamSam (2016).

1.2.3 Ransomware-as-a-service

Some ransomware developers offer their malware as a service to other cybercriminals who pay a commission for each successful infection or payment. This lowers the entry barrier for aspiring ransomware operators and increases the diversity and distribution of ransomware variants. Examples of ransomware-as-a-service include Cerber (2016), GandCrab (2018) and REvil (2019).

With the world adapting to the digital era, the number of people online has increased considerably, thereby creating a greater opportunity for cybercriminals. Ransomware-as-a-service acts as a business model where ransomware variants are leased to cybercriminals. With the growing demand for the confidentiality of data, there is a pressing need to detect and prevent ransomware attacks.

2 Literature Review

2.1 Classification of Ransomware

Ransomware can be classified into different categories based on various criteria such as encryption method, attack vector, etc. Some of the common classifications are:

2.1.1 Encryption Mechanism

Ransomware can be classified into two categories based on its encryption mechanism: symmetric and asymmetric [3]. Symmetric ransomware uses the same key for encryption and decryption, while asymmetric ransomware uses a public key for encryption and a private key for decryption. The private key is usually stored on the attacker's server and only released after the ransom is paid.

2.1.2 Infection Method

Another way to categorize ransomware is based on its infection method: locker, crypto or scareware [4]. Locker ransomware typically does not encrypt any data containing files. Instead, it locks the victim out of their device. Crypto ransomware, on the other hand, encrypts the user's privileged files but does not interfere with basic computer functions. Unlike locker ransomware, crypto-ransomware is usually irreversible as it is almost nearly impossible to revert the current encryption techniques if implemented properly. Some ransomware variants combine both methods to increase their impact. Scareware is a type of malware that convinces the user of the presence of a virus in the system and prompts them to buy or download malicious software to resolve the issue. Similar to trojans, scarewares trick the users and aim to exploit their fear and come in the form of pop-ups.

2.1.3 Delivery Mode

Ransomware can also be distinguished by their delivery mode: manual or automated. Manual ransomware requires human intervention from the attacker to execute the payload on the target sys-

tem, while automated ransomware relies on self-propagation mechanisms such as worms or botnets.

Some examples of well-known ransomware families are [4]:

- CryptoLocker: One of the first asymmetric crypto ransomware that emerged in 2013 and infected millions of computers worldwide.
- WannaCry: A worm-based crypto ransomware that exploited a vulnerability in Windows SMB protocol in 2017 and affected more than 200,000 systems across 150 countries.
- Ryuk: A manual crypto ransomware that targets high-value organizations such as hospitals, governments and corporations since 2018.
- Maze: A crypto-locker hybrid ransomware that encrypts data and exfiltrates it to the attacker's server and threatens to publish it online if the ransom is not paid since 2019.

2.2 Attack vectors and techniques

Ransomware attackers use various techniques to infiltrate their victims' systems and execute their malicious code. Some of the most common attack vectors are [5]:

- Phishing emails: Emails that contain malicious attachments or links that trick users into downloading or opening them.
- Drive-by downloads: Websites that host malicious scripts or exploits that download malware onto visitors' browsers or devices without their consent.
- Remote Desktop Protocol (RDP): This is a network protocol that allows remote access to another computer over the internet. Attackers can exploit weak passwords or vulnerabilities in RDP services to gain access to target systems.
- Software vulnerabilities: Flaws or bugs in software applications or operating systems that can be exploited by attackers to execute arbitrary code on target systems.
- Malvertising: Online advertisements that contain malicious code or redirect users to malicious websites.

Once inside the victim's system, ransomware attackers use various techniques to evade detection, escalate privileges, spread across networks, encrypt data and extort payment. Some of these techniques are:

- Obfuscation: Hiding or altering the appearance of malware code to avoid being detected by antivirus software or security tools.
- Encryption: Encrypting malware code or communication channels to prevent analysis or interception by security researchers or authorities.
- Polymorphism: Changing malware code dynamically during execution or infection to create new variants that can bypass signature-based detection methods.
- Process injection: Injecting malware code into legitimate processes running on target systems to blend in with normal activity and avoid suspicion.
- Lateral movement: Moving from one compromised system to another within a network using stolen credentials or exploits.

2.3 Detection and Analysis Techniques

They aim to identify ransomware infections or activities on a system or network and provide information about its characteristics, behaviour or origin. Some common detection and analysis techniques include:

- Monitoring system performance, network traffic or file system changes for any anomalies or indicators of compromise that may signal a ransomware infection.

- Analyzing malware samples using static or dynamic analysis tools such as disassemblers, debuggers or sandboxes to extract features such as encryption algorithms, keys, payloads or command-and-control servers used by ransomwares.

2.4 Recovery and Decryption Methods

They aim to restore the victim's data or access without paying the ransom. Some common recovery and decryption methods include [6]:

- Restoring data from backups if they are available and unaffected by the attack.
- Exploiting weaknesses in the encryption scheme used by ransomwares, such as weak keys, flaws in random number generation or reuse of keys across different victims.
- Using decryption tools developed by security researchers or vendors that can decrypt some types of ransomware based on known keys, algorithms or patterns.

2.5 Encryption Algorithms

2.5.1 AES (Advanced Encryption Standard)

Advanced Encryption Standard (AES) is a symmetric encryption algorithm that is widely used for securing data transmission and storage in various applications, such as communication, data communication and wireless communication. It is an iterative cipher and not a Feistel cipher [7]. AES operates on 128-bit (16 bytes) blocks of data and uses a secret key of 128, 192 or 256 bits to encrypt and decrypt the data. These 16 bytes are represented in a 4x4 matrix, and AES operates on a matrix of bytes. AES is considered to be one of the most efficient and secure encryption algorithms, as it is resistant to various types of attacks and has a high speed of execution.

The design of AES is based on a mathematical structure called a substitution-permutation network (SPN), which consists of several rounds of transformations that mix the data and the key [8]. Each round consists of four operations: SubBytes, ShiftRows, MixColumns and AddRoundKey. The number of rounds depends on the key size: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys [9]. The first round does not include the MixColumns operation, and the last round does not include the ShiftRows and MixColumns operations. The encryption process starts with an initial AddRoundKey operation, and the decryption process ends with an inverse AddRoundKey operation. The key used for decryption is the same as the one used for encryption and the process is similar to the encryption process, but in the reverse order [7].

2.5.2 RSA (Rivest, Shamir, Adleman)

RSA [10] algorithm is an asymmetric cryptography algorithm. The rationale behind RSA is that it is difficult to factorise a huge number. The public key is made up of two integers, one of which is a multiplication of two huge prime numbers. The same two prime numbers are also used to generate the private key.

The initial procedure begins with the selection of two prime numbers, namely p and q, and then calculating their product n. Choose a number e such that e is co-prime to (p - 1) x (q - 1). The public key is $< e, n >$. Private Key d is calculated from the numbers p, q and e. The mathematical relationship between the numbers is ed = 1 mod ((p - 1)(q - 1)).

Due to the difficulties of breaking RSA, it is widely used for password exchange, banking, online shopping, and even cable television. If someone is able to factor the huge number, the secret key is compromised. As a result, encryption strength is entirely dependent on key size, Thus doubling or tripling the key size improves encryption strength significantly.

2.6 Ransomware Implementation Techniques

Some of the methods in which ransomware encryption and decryption are implemented are [11]:

2.6.1 Symmetric Encryption

In this method, algorithms such as AES are used to encrypt the victim's files at a large speed rate. It encrypts all of the user's files with the chosen encryption algorithm and stores the key on the device itself. When the victim pays the ransom, the decryptor will open this file containing the keys and start decrypting the encrypted files. However, this naive approach encourages researchers to find this file, and since it's not encrypted, make some tools to decrypt the files using the keys.

2.6.2 Client Asymmetric Encryption

In this approach, the ransomware generates an RSA key pair, encrypts all the files with the public key and sends the private key to the server to be stored. This encryption method is quite slow as RSA encryption will take a long time to encrypt large files. The ransomware also needs to send the private key to a server. In this scenario, the infected computer is connected to the internet, and the server has to be online. If any of the two parties aren't connected, there will be a problem. Either the ransomware needs to stop its execution or it'll encrypt every file with the public key and delete the private key without the possibility of decryption as it hasn't been stored on the server. The solution to this issue would be to temporarily store the private key on the disk for later decryption/transfer to the server.

2.6.3 Server Asymmetric Encryption

In this scheme, the server will generate a public and private key pair. The public key will be hard coded in the ransomware program, and for each file, it'll encrypt the file with the server's public key. The files can be decrypted only using the server's private key. But there is a flaw in this method as well. If the server sends the private key to the client to decrypt the files, researchers can get the private key and distribute it to all the victims. The other way for decryption is for the victim to send all their encrypted files to the server to decrypt and get the decrypted files back. This is a very slow method and will not be viable to send large encrypted files over the internet.

2.6.4 Server And Client Asymmetric Encryption + Symmetric Encryption

This scheme is used by most modern ransomwares. It's a hybrid model, using both symmetric and asymmetric encryption, and it does not require an internet connection for encryption, only for decryption.

In this scheme, both, the ransomware programs on the victim's machine and the server will generate their respective RSA key pairs. The ransomware program will have the server's public key hard-coded into it. It'll encrypt the victim's private key with the server's public key. The files will get encrypted with AES and all the AES keys will be encrypted with the victim's public key.

To decrypt the files, the victim will need access to the AES keys, which are encrypted. To decrypt it, the victim will need its private key, which is already encrypted with the server's public key. The server is the only one that will have that key to decrypt the victim's encrypted private key.

2.7 Prevalant Ransomware Attack Groups

2.7.1 BlackByte

BlackByte [12] exploits the ProxyShell vulnerabilities to infiltrate the system. After initial access into the system, the attackers use Certutil to download and execute the components that it needs to propagate in the network. The actors use network discovery tools to get a good view of the victim's network environment. After network reconnaissance, the attackers deploy AnyDesk for an additional level of control over the system. It also terminates certain pro-

cesses and services related to security applications to evade detection.

Once the attackers have infiltrated the victim's network and identified valuable files, it exfiltrates them using WinRar to archive the files and upload them into file sharing sites. It also connects to its C&C server where it looks for a certain PNG file that contains information critical to encryption and is used to derive the AES128 key. This key is then protected using an embedded RSA key which will then become undecryptable without the private key. The ransomware then deletes shadow copies in the system using vssadmin.

2.7.2 Conti

Conti [13] software uses its own implementation of AES-256 that uses up to 32 individual logical threads, making it much faster than most ransomware. Conti also leverages double extortion techniques, and have resorted to also selling access to victim organizations that refused to pay the ransom. Conti can arrive in the system through phishing emails containing a Google Drive link that downloads the malware. It can also arrive via exploiting the FortiGate firewall vulnerabilities or the ProxyShell Microsoft Exchange vulnerabilities.

Since the operators employ double extortion tactics, they actively look for files to exfiltrate in the discovery stage. The ransomware mostly relies on finding the domain admin credentials to gain full access to the domain. The attackers dump cached credentials on systems to allow them to move laterally or elevate their privilege. The attackers also use batch files to disable security tools and to automate the distribution of its tools in the domain. These tools include scripts to terminate existing security software. These files are executed through scheduled tasks. The attackers perform data exfiltration on the system with the use of the Rclone and WinSCP, and sync files to the cloud, such as Mega cloud storage. The ransomware also inhibits system recovery by deleting shadow copies using WMI.

2.7.3 Lockbit

LockBit [14] uses a ransomware-as-a-service (RaaS) model and employs double extortion methods. One of its notable tactics was the creation and use of the malware StealBit, which automates data exfiltration. LockBit operators mostly gain access via compromised servers or RDP accounts, or via spam email. LockBit is usually executed via command line or via created scheduled tasks. There are also reports of it being executed using PowerShell Empire, a pure PowerShell post-exploitation agent.

Infections were observed to have used GMER, PC Hunter, and/or Process Hacker to disable security products. In some observed attacks, a Group Policy was created to disable Windows Defender. Network Scanner, Advanced Port Scanner, and AdFind were also used to enumerate connected machines in the network. It uploads stolen files via cloud storage tools like MEGA or FreeFileSync. The ransomware payload will proceed with the encryption routine upon execution. Encryption includes both local and network encryption. It encrypts files using AES and encrypts AES key with RSA encryption. For faster encryption, it only encrypts the first 4KB of a file and appends it to ".lockbit."

2.7.4 Ryuk

Ryuk [15] tops the list of the most dangerous ransomware attacks. When Ryuk infects a system, it first shuts down 180 services and 40 processes. These services and processes could prevent Ryuk from doing its work, or they are needed to facilitate the attack.

At that point, the encryption can occur. Ryuk encrypts files using AES-256 encryption. The symmetric encryption keys are then encrypted using asymmetric RSA-4096. Ryuk is able to encrypt remotely, including remote administrative shares. In addition, it can perform Wake-On-Lan, waking computers for encryption. Ryuk mostly spreads through phishing emails.

In many cases, days or weeks may elapse between the time hackers initially gain access to a system before the massive encryption occurs, as the criminals penetrate deeper into the network to inflict maximum damage. Ryuk is an especially pernicious type of malware because it also finds and encrypts network drives and resources. It also disables the System Restore feature of Microsoft Windows that would otherwise allow restoring the computer's system files, applications, and Windows Registry to their previous, unencrypted state.

3 System / Network Environment

Any computer system that has access to the internet with python 3.0 installed in it. The client system should be able to make HTTP requests to a server through the internet, and the ransomware program should have the required permissions to access and modify the file directory.

4 Design

The hybrid ransomware we aim to program consists of a client and a server. The ransomware is hybrid because it uses both symmetric and asymmetric encryption. Figure 1 shows the attack process of the ransomware. For development purposes, the client and server can be programs running in different ports within the same system. In practice, internet connectivity would be required for the client to communicate with the server during the decryption phase.

The server initially generates a public and a private key pair and publishes the public key. This public key can also be hard-coded into the client program for encryption to work even when the client system is not connected to the internet. The client also generates its public and private key pair. This private key is encrypted using the server's public key and stored within the file directory of the client system. The client's private key is encrypted and not stored as plain text to prevent the user from going through

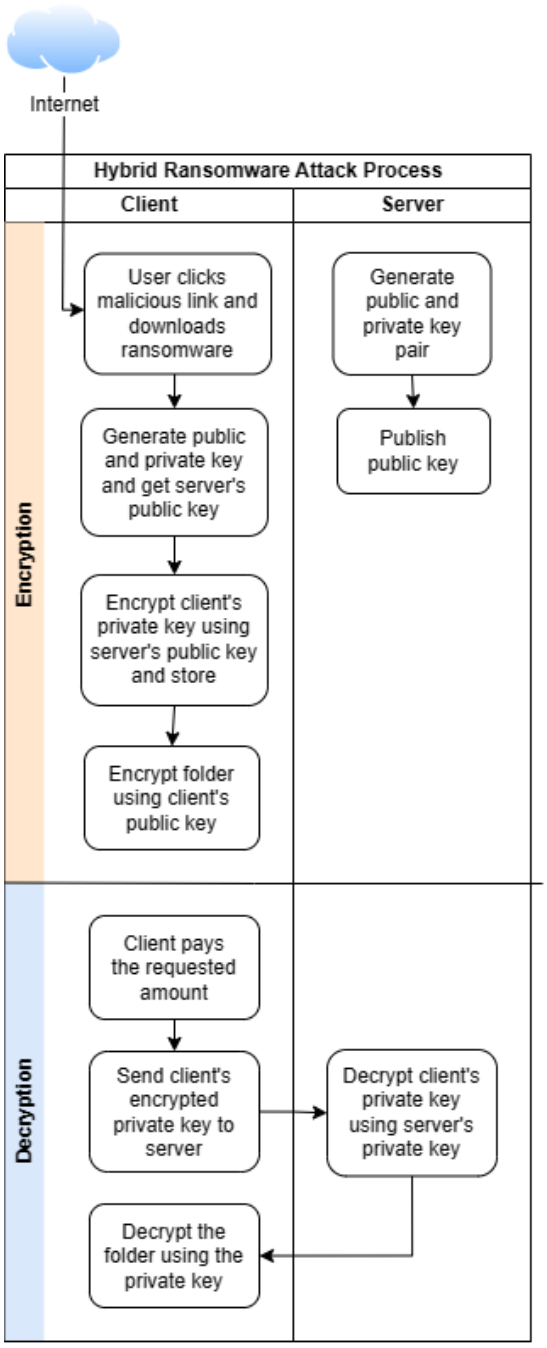


Figure 1: Hybrid Ransomware Attack Process

the directory and directly decrypting the folder. The client then uses AES and its public key to encrypt a folder and deletes the original folder from the system. A message that a folder is encrypted by ransomware is displayed to the user, along with the ransom that must be paid.

The client cannot directly decrypt the folder as the AES private key required to decrypt is encrypted using the server's public key. So, when the user eventually pays the ransom, the client program sends the encrypted client's private key to the server. The server uses its private key to decrypt the encrypted client's private key. This is then sent back to the client, and it uses this private key to decrypt the folder.

The client's private key should never be sent to the server as plain text and it should also never be written to disk, even if it will be encrypted later. To prevent file recovery tools from recovering the original files, the original files should be "shredded" (overwritten with random bytes) and then deleted.

5 Conclusion

By exploring various resources, we were able to gain insightful knowledge on the intricacies revolving around ransomware, its existence, creation and propagation. We studied and realized the different encryption techniques that can be used to encrypt a file with ransomware. We also dug deep into the working of two encryption algorithms, namely AES and RSA. Using the obtained knowledge, we were able to come up with a simple program to encrypt a specified folder with ransomware.

References

[1] https://www.getastra.com/blog/security-audit/ransomware-attack-statistics/

[2] C. C. Joseph, "After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity", Trend Micro White paper, 2017.

[3] Q. Zhang, "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption," 2021 2nd International Conference on Computing and Data Science (CDS), Stanford, CA, USA, 2021, pp. 616-622, doi: 10.1109/CDS52072.2021.00111.

[4] Ekta and U. Bansal, "A Review on Ransomware Attack," 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 2021, pp. 221-226, doi: 10.1109/ICSCCC51823.2021.9478148.

[5] Zimba, Aaron. "Malware-Free Intrusion: A Novel Approach to Ransomware Infection Vectors". International Journal of Computer Science and Information Security XV(2), pp. 317, 2017.

[6] https://www.enterprisenetworkingplanet.com/security/ransomware-recovery/

[7] A. Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data", Cryptography and Network Security, 2017.

[8] Mohamed, A. A., Madian, A. H. (2010, December). A Modified Rijndael Algorithm and its Implementation using FPGA. In Electronics, Circuits, and Systems (ICECS), 2010 17th IEEE International Conference on (pp. 335-338).

[9] Pramstaller, N., Gurkaynak, F. K., Haene, S., Kaeslin, H., Felber, N., Fichtner, W. (2004, September). Towards an AES crypto-chip resistant to differential power analysis. In Solid-State Circuits Conference, 2004. ESSCIRC 2004. Proceeding of the 30th European IEEE (pp. 307-310).

[10] Rivest, R.; Shamir, A.; Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Volume 21,Issue 2, February 1978 (pp. 120-126).

[11] https://medium.com/@tarcisioma/ransomware-encryption-techniques-696531d07bb9

[12] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbyte

[13] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-conti

[14] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit

[15] https://www.trendmicro.com/en_in/what-is/ransomware/ryuk-ransomware.html