# End - Point Ransomware Detection and Remediation

Karthik Amarnath Cholleti
*11605154*

Siva Nageswararao Mallavolu
*11520262*

Harika Naga Sai Sree Chandana Padala
*11519848*

Tinku Naga Sai Pavan Adapa
*11603383*

***Abstract*—The increase of ransomware attacks has become a major cause for concern for businesses of all sizes, because they severely disrupt daily operations and result in huge financial losses. To reduce the likelihood of ransomware attacks, this project's goal is to build an end-point security approach. The project will begin by locating the vulnerabilities in endpoint devices, including desktops, laptops, servers, and mobile devices. After that, the project will investigate different security tools like antivirus, firewalls, and intrusion detection systems to stop ransomware attacks. Based on how well they can identify and stop ransomware attacks, these solutions will be assessed. A response strategy for a ransomware attack will also be developed as part of this project. This plan will detail the actions to be taken in the event of an attack, including isolating infected devices, containing the attack, and recovering the data. To ensure that data is available in the event of an attack, the project will also investigate backup and recovery options.**

***Index Terms*—Ransomware, End - Point Security Approach**

## I. Introduction

In recent years, endpoint ransomware has grown to be a serious threat to organizations of all sizes. Computers, laptops, smartphones, and tablets are examples of the endpoints or individual devices that this kind of malware targets. After infecting the endpoint, the malware encrypts the files there and demands a ransom in order to receive the decryption key. Victims may suffer significant financial setbacks and interruptions to their businesses as a result. WannaCry, Petya, Locker Ransomware, and Bad Rabbit are a few instances of endpoint ransomware. Millions of devices were impacted by these attacks, which cost billions of dollars to repair. These attacks can have devastating effects on their victims, including data loss, interruption of business operations, and reputational harm.

Organizations must implement a thorough endpoint security strategy to combat the growing threat of endpoint ransomware. The implementation of security solutions to stop ransomware attacks, the identification of endpoint device vulnerabilities, and the creation of a response plan in the event of a ransomware attack should all be part of this strategy. To reduce the risk of ransomware attacks, the goal of this project is to develop a thorough endpoint security strategy. Organizations can safeguard their data and lessen the effects of ransomware attacks on their business operations by putting in place effective security measures.

## II. Literature Survey/Background

Endpoint security is now a top concern for businesses and organizations due to the sophistication and difficulty of ransomware attacks. Endpoint ransomware attacks frequently use a variety of tactics, including the delivery of payloads, operating system modification, file encryption, and network connectivity disruption. In this review of the literature, we'll look at the methods employed in some of the most well-known ransomware attacks, along with the corresponding detection and recovery tactics.

### *A. File Encryption*

File encryption is one of the main techniques employed in ransomware attacks. Attackers encrypt victims' files using encryption algorithms, making them inaccessible until a ransom is paid. For instance, the files of victims were encrypted by the Advanced Encryption Standard (AES) - 128 encoding algorithm during the 2017 WannaCry ransomware attack. Researchers have created several methods to spot these types of attacks, including behavioral analysis and machine learning algorithms, which can spot patterns in the characteristics and behavior of malware.

### *B. Modification to Operating System*

In 2016, Petya, a ransomware attack, changed the Master Boot Record (MBR) of the victims' systems, making it impossible for them to start up. Researchers have created several strategies to counteract this kind of attack, including the use of network segmentation to isolate infected endpoints and stop ransomware from spreading to other devices.

### *C. Disrupting Network Connectivity*

Another method used in ransomware attacks is network connectivity disruption. The 2017 ransomware attack known as NotPetya prevented its victims from accessing their systems or data by disabling their connectivity. Researchers have created several methods to identify and counteract these types of attacks, including the use of artificial intelligence-based solutions to analyze vast amounts of data and spot patterns and anomalies that could be signs of ransomware.

### D. Ransom Note

Another frequent component of ransomware attacks is the ransom note. In 2016, a ransom note was displayed to victims of Locker Ransomware, requesting money in exchange for the decryption key. Researchers have developed several techniques to identify and counteract these attacks, including using behavioral analysis to monitor the behavior of the endpoint and spot unusual activity that might be a sign of ransomware.

### E. Payload Delivery

Ransomware is one of the many payloads that Emotnet Malware, a well-known malware delivery platform, can deliver. Researchers have developed a number of techniques, such as the use of machine learning algorithms to classify and identify various types of malware, to detect and mitigate these kinds of attacks.

### F. Antivirus and Security Software

Some ransomware attacks are made to work around antivirus and security software. The 2016 Cerber Ransomware attack was well-known for its capacity to defeat security and antivirus programs. Researchers have created several strategies to counteract these kinds of attacks, including the use of real-time advanced threat detection and response solutions.

Organizations must adopt thorough endpoint security strategies that combine detection and mitigation techniques because the threat of ransomware attacks is only going to increase. Machine learning, behavioral analysis, backup and recovery tools, network segmentation, artificial intelligence-based solutions, and sophisticated threat detection and response tools are a few examples of these techniques. Organizations must adopt best practices to safeguard their data and systems and stay up to date on the most recent developments in endpoint security as the ransomware threat evolves.

## III. Basic Structure/Steps Involved

### A. Creating a Connection

In this step a connection between the attacker's device and the victim's device is created. Typically, social engineering techniques like phishing emails or malicious links are used to accomplish this. The ransomware is downloaded onto the victim's device as soon as they click the link or download the attachment, giving the attacker access to the device.

### B. Generating Keys

To create a unique encryption key for each infected device, the ransomware employs a complex algorithm. The files of the victim are encrypted using this key, and it is necessary to decrypt those files as well. In most cases, the attacker's server is used to generate the encryption key, making it challenging for the victim to access or retrieve it.

### C. Encryption and Decryption

The encryption key is used by the malware to encrypt the victim's files during a ransomware attack, rendering them inaccessible. To decrypt the files and regain access to them, the victim needs the decryption key. The files will remain encrypted and inaccessible to the victim without the decryption key, though.

### D. Attack

The ransomware starts its attack as soon as the attacker gains control of the victim's device. The victim's files will begin to be encrypted by the ransomware, rendering them inaccessible to the victim. A ransom note requesting payment in exchange for the decryption key will then be displayed by the attacker. Typically, the ransom note contains instructions on how to pay, such as how to use cryptocurrency.

### E. Demand

In exchange for the decryption key, the attacker demands a ransom from the victim. Cryptocurrency like Bitcoin or Ethereum is frequently demanded as the ransom payment. If the money is not transferred within a predetermined timeframe, the attacker may threaten to delete or publish the victim's data.

### F. Analysis

It is crucial to carry out a thorough analysis of the attack following a ransomware attack. This analysis entails determining the ransomware type employed, the devices' vulnerabilities, and the effect of the attack on the victim's data and operations. This analysis is essential for creating a strategy for responding to the attack and putting protective measures in place.

### G. Mitigation

The recovery of the victim's data and the prevention of further attacks are steps that must be taken in order to lessen the effects of a ransomware attack. In order to do this, it may be necessary to restore the victim's data from backups, put security tools like firewalls and antivirus software in place, train staff on how to spot social engineering attacks, and install security solutions like intrusion detection systems and firewalls. The main objectives of mitigation are to lessen the effect of the attack on the victim's operations and to stop further attacks.

## IV. Phishing

Phishing is a type of cyberattack in which a perpetrator poses as a trustworthy organization in order to trick a victim into disclosing sensitive data, such as login credentials, credit card information, or personal information. A typical attack method involves the attacker sending an email, text message, or instant message that appears to be from a reputable source, like a bank, social media platform, or government organization.

The attacker creates an email that appears to be from a trustworthy source in a typical phishing attack. To get the victim to click on a link, the attacker may use a variety

of tactics, including feigning urgency, fear, or curiosity. For instance, in this instance, the attacker made a false claim about a flash sale that was only valid for two hours on the website Temu to entice the victim to click on the link right away.

Setting Up a Mail Server for Phishing attack – On the Kamatera cloud platform, an SMTP mail server was configured for the "zero.xyz" domain. The actions were as follows:

### A. Purchasing and configuring a domain

The 'zero.xyz' domain was first ordered from Namecheap, and the DNS records were set up to direct visitors to our mail server.

### B. Installing the Kamatera Cloud Platform

On the Kamatera cloud computing platform, we made an account and set up a server with the following settings: 'zero.xyz' as the hostname, 2A CPU, 4096MB of memory, and a 20GB disk 1 are all specifications for the Ubuntu 20.04.5 LTS operating system.

### C. Install iRedMail

We downloaded the installation script from the iRedMail website and ran it with sudo rights on our freshly installed Ubuntu Server 20.04.1.

### D. Configuring iRedMail

After the installation, we went to http:// 83.225.9.90/iredadmin to the iRedMail web interface and configured our email domain and administrator account.

### E. Configuring the SMTP Server

Next, we set up DNS records like MX records, configured firewall rules to permit incoming traffic to the server, and checked that the SMTP server was listening on the appropriate ports to configure the SMTP server to accept incoming emails from the internet.

### F. Configure Outgoing Email Routing

Then, in order to prevent our outgoing emails from being marked as spam, we set up SPF and DKIM records on the SMTP server, configured the routing and relaying settings, and configured the SMTP server to route outgoing emails to their intended recipients.

### G. Implementing Security Measures

We set up security measures like firewall rules and TLS encryption to prevent the server from being accessed by unauthorized users and to guarantee the privacy of email communication. For these uses, we employed the Let's Encrypt SSL/TLS certificates and the Ubuntu UFW firewall.

### H. Configuring Mail Policies

To better manage our email accounts and lower the amount of spam or unwanted email that our users receive, we used iRedMail to set up mail policies like spam filters, email forwarding, and mailbox quotas.

### I. Testing the server

For the purpose of identifying and troubleshooting any configuration issues that might be keeping our server from operating properly, we tested the server by sending and receiving emails to and from other email addresses.

## V. Attack - Reverse Shell

In a reverse shell attack, the attacker can access the victim's computer system and send commands to it from a distance. In this attack, a backdoor is built on the victim's computer system by the attacker, who then uses it to connect to a remote server. Once the connection is made, the attacker can use the remote server to issue commands to the victim's system, effectively seizing control of the victim's computer. Reverse shell attacks are frequently used in cyber espionage, cybercrime, and other malicious activities. Because the attacker gains access to the victim's computer rather than the victim's computer reaching out to the attacker, reverse shell attacks can be challenging to spot.

**Performing Reverse shell**

- The script imports the socket module to enable socket programming.
- The IP address and port number that the server will listen on are set in the script.
- The buffer size is set to receive messages from the client.
- A separator string is set to separate command results and the current working directory in messages sent by the client.
- A socket object is created to allow communication between the server and the client.
- The socket is bound to the specified IP address and port.
- The socket option is set to allow the port to be reused.
- The server starts listening for incoming connections.
- The script enters a loop that prompts the user for a command to execute on the client machine.
- The results of the command are received from the client, printed to the console, and the connection to the client is closed.

## VI. Generating keys

One of the most well-known and frequently used public-key cryptographic algorithms is the RSA one. Based on the mathematical tenet that it is simple to multiply two large prime numbers together, but very difficult to factor the product back into its original primes, it is used for secure data transmission. In this project, we used keys with a 3072-bit length to implement the RSA algorithm.

Particularly when using long key lengths like 3072 bits, the RSA algorithm is regarded as being very secure. The algorithm is more secure the larger the key size because it is more challenging for an attacker to factorize the keys. Python, a popular programming language in the field of cryptography, was used to implement the algorithm.

We used a well-known algorithm that involves picking two big prime numbers and multiplying them together to create the 3072-bit keys. The public and private keys were then generated

using these prime numbers. While the private key is required for decryption, the public key is used for encryption.

Data transmission over the internet using our implementation of the RSA algorithm with 3072-bit keys is secure. We now have a better understanding of how public-key cryptography functions and how the RSA algorithm can be used to ensure secure data transmission as a result of this project.

The "rsa" module is imported and the function "generate_keys()" is defined in the proposed code. Using the "rsa.newkeys()" method, this function creates a 3072-bit public and private key pair. The "save_pkcs1()" technique is then used to save the public and private keys as PEM-encoded files with the names "pub_key" and "priv_key", respectively.

## VII. Encryption

The RSA-3072 bit encryption algorithm is utilized in end-point ransomware attacks. A public key and a private key for an RSA pair are generated by the attacker. The victim's files are then encrypted using a symmetric key created using the public key. Then, a ransom demand and the encrypted symmetric key are transmitted to the attacker's server. To decrypt the symmetric key and grant the victim access to their files once more, the attacker must have the private key. The RSA-3072 bit encryption algorithm ensures that the attacker can demand a ransom in exchange for access to the decryption key because it is challenging to decrypt data without the private key.

## VIII. Decryption

Decryption during a ransomware attack is only possible if the victim has access to the private key that was used to encrypt the files. The attackers typically hold the private key instead and demand a ransom in exchange for it. The attackers may or may not supply the key to decrypt the files if the victim chooses to pay the ransom. The victim may attempt to use third-party tools or services to decrypt the files if they do not have access to the private key. There is no assurance that the files will be fully recovered because of the variable success rates of these techniques.

The generated and secretly stored private key can be used to perform decryption on the code. The rsa.PrivateKey.load_pkcs1 method can be used to load the private key from a file. The rsa.decrypt method can then be used to read the encrypted file and decrypt it by passing the private key as an argument. Depending on the desired outcome, the generated plaintext can then be written to a new file or displayed on the console. Decryption cannot be done, though, if the victim does not have the private key.

## IX. Detection

Several techniques were be used to find end-point ransomware, such as -

### *A. Using End-Point Protection Software*

Installing end-point protection programs like Microsoft Defender, Kaspersky Endpoint Security, Sophos Endpoint Protection, and others can assist in identifying the presence of ransomware on the end-point devices. These tools keep an eye on the system for any suspicious activity, such as ransomware activity, and notify the user if anything is found.

### *B. Monitoring Network Traffic*

Monitoring network traffic can assist in identifying ransomware attacks that spread over a network. Network traffic can be monitored and ransomware activity can be found using tools for network traffic analysis like Wireshark, SolarWinds Network Performance Monitor, etc.

### *C. Analysis of User Behavior*

Ransomware attacks frequently cause users to alter their behavior, such as by clicking on dubious email attachments or visiting malicious websites. Tools for analyzing user behavior like Varonis or Splunk can be used to spot such unusual behavior and notify users.

### *D. Email filtering*

Phishing emails are a common way that ransomware spreads. To identify and stop suspicious emails and their attachments, use email filtering tools. These tools analyze email content and spot phishing emails using machine learning algorithms.

### *E. Regular Vulnerability Scanning*

Regular vulnerability scanning can assist in identifying system flaws that ransomware may exploit. In order to scan the system for vulnerabilities and provide recommendations for patching them, vulnerability scanning tools like Nessus or Qualys can be used.

### *F. Endpoint detection and response (EDR)*

EDR is an all-encompassing security solution that offers immediate threat detection, reaction, and remediation. To identify and stop ransomware attacks, EDR tools combine signature-based detection, behavior-based detection, and machine learning. In-depth information about the attack can also be provided by these tools, which can be used for additional research and correction.

## X. Analysis

### *A. A Known Vulnerability was Exploited*

The ransomware targeted Windows-based computers using the open 443 port to exploit. The malware was able to spread quickly across the internet due to the vulnerability.

### *B. Worm-like Propagation*

The malware was created to spread throughout networks, automatically infecting additional vulnerable computers. Because of this, the ransomware was extremely contagious and quickly infected entire computer networks.

### C. Files Encrypted (RSA - 3072 bit)

The ransomware used RSA-3072 encryption to encrypt the files on the affected computers. Users couldn't access the files as a result until the ransom was paid.

### D. Cryptocurrency Payment

Bitcoin was the cryptocurrency that was demanded as payment by the ransomware. This made it possible for the attackers to remain undetected and made it challenging for law enforcement to track the payments.

### E. Backdoor was installed

The ransomware also put a backdoor on the computers it infected, giving the attackers remote access to the systems. The use of this backdoor could be made to carry out additional attacks or steal confidential data.

## XI. Mitigation

- Disable TLS 1.0 and SSLv3 because these outdated protocols are known to be weak points. The majority of attacks that rely on these protocols can be stopped by disabling them.
- Ensure TLS 1.2 or later: It is advised to use TLS 1.2 and later as they are more secure than SSLv3 and TLS 1.0.
- Implement certificate pinning: By comparing the server's certificate to a predefined one, a client can confirm the server's identity using certificate pinning. Man-in-the-middle attacks can be avoided by doing this.
- Implement firewall rules: By using firewall rules, only legitimate traffic can pass through port 443 while malicious traffic is blocked.
- Use a trusted certificate authority: Using a trusted certificate authority can help you avoid using forged or fake certificates for SSL/TLS.
- Update and patch software frequently: By applying the most recent security patches and updates, you can stop known vulnerabilities from being exploited.
- Install intrusion detection and prevention tools: These tools can identify and stop any suspicious activity occurring on port 443.
- Consider using a virtual private network (VPN): By encrypting the traffic that passes through port 443, a VPN can add an additional layer of security.

## XII. Containment

Containing an end-point attack is the first step in responding to it. The actions that should be taken to stop a ransomware attack are as follows:

- Disconnect the infected device from the network to stop the ransomware from infecting additional networked devices.
- Isolate the device: To stop the ransomware from spreading, the device should be isolated in a different VLAN or subnet if it cannot be disconnected from the network.
- Disable network access: To stop communication with the attacker's command and control server if the device cannot be isolated, network access should be disabled at the firewall.
- Restart the device: Restarting the device will stop the ransomware from encrypting files further.

## XIII. Recovery

The next step is to recover from the attack after it has been stopped. The actions that should be taken to recover from a ransomware attack are as follows:

- **Restore from backups:** The data on the infected device can be restored to a clean state if the company has a recent backup of it. Before restoring the backup, it is crucial to make sure it is free of ransomware.
- **Use decryption tools:** Some ransomware varieties can be broken open using freely accessible software. It's crucial to do some research on the specific ransomware strain to find out if a decryption tool is available.
- **Pay the ransom:** Although it is not advisable, some businesses might decide to do so in order to recover their data. This should only be used as a last resort because there is no assurance that the data will be returned safely in this way.

## XIV. Prevention

The best defense against end-point attacks is prevention. The best practices for avoiding a ransomware attack include the ones listed below:

- Maintain software updates: To stop the exploitation of known vulnerabilities, make sure that all software and operating systems are up to date with the most recent security patches.
- Use anti-malware software: To identify and stop ransomware attacks, use anti-malware software on all end-point devices.
- Put security awareness training into practice: Inform staff members of the dangers of ransomware attacks and instruct them on how to spot shady emails and links.
- Data backups should be done on a regular basis to ensure that they can be recovered in the event of a ransomware attack.

## XV. Conclusion

The "End-point Ransomware Detection and Mitigation" project has given us a thorough understanding of the dangers and effects of ransomware attacks on end-point devices. By using a reverse shell attack to access a victim's computer through a phishing email that appeared to be from a reliable source, we have shown the severity of the attack. A crucial component of a ransomware attack, we have also demonstrated how we created keys using RSA 3072 bits and used them to encrypt and decrypt files.

Attacks from ransomware must be detected and mitigated. We have demonstrated in this project how regular network traffic monitoring, user behavior analysis, email filtering, and vulnerability scanning can be used to identify ransomware attacks. Additionally, we've shown that mitigation is possible

by isolating the infected device and retrieving the encrypted files using backup copies.

To stop ransomware attacks from getting worse, containment and recovery are also essential. This project has demonstrated how containing the infected device by cutting it off from the network can stop ransomware from spreading. Encrypted files can also be recovered using recovery techniques like restoring from backup files.

We have emphasized the necessity of steps like routine software updates, employee training and awareness campaigns, and the adoption of security measures like endpoint protection software in order to stop future ransomware attacks. To protect end-point devices from ransomware attacks, this project has highlighted the significance of readiness, detection, mitigation, containment, recovery, and prevention.

## REFERENCES


[1] "7 Tips to Boost Endpoint Security: IEEE Computer Society." 7 Tips to Boost Endpoint Security — IEEE Computer Society, https://www.computer.org/publications/tech-news/trends/7-tips-to-boost-endpoint-security.

[2] S. Chandel, S. Yu, T. Yitian, Z. Zhili and H. Yusheng, "Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat," 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, 2019, pp. 81-89, doi: 10.1109/CyberC.2019.00023.

[3] A. Kamruzzaman, S. Ismat, J. C. Brickley, A. Liu and K. Thakur, "A Comprehensive Review of Endpoint Security: Threats and Defenses," 2022 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 2022, pp. 1-7, doi: 10.1109/ICCWS56285.2022.9998470.

[4] Chandel, Sonali, et al. "Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat." 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2019, https://doi.org/10.1109/cyberc.2019.00023.

[5] Karantzas, George, and Constantinos Patsakis. "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors." Journal of Cybersecurity and Privacy, vol. 1, no. 3, 2021, pp. 387–421., https://doi.org/10.3390/jcp1030021.

[6] Fabian, Michael. "Endpoint Security." Proceedings of the 4th Annual Conference on Information Security Curriculum Development, 2007, https://doi.org/10.1145/1409908.1409935.

[7] Chakroun, Imen, et al. "Using Unsupervised Machine Learning for Plasma Etching Endpoint Detection." Proceedings of the 9th International Conference on Pattern Recognition Applications and Methods, 2020, https://doi.org/10.5220/0008877502730279.

[8] Richings, Dan. "Rethinking Endpoint Management for the Modern Age." Network Security, vol. 2022, no. 10, 2022, https://doi.org/10.12968/s1353-4858(22)70060-8.