A Study on Securing Against Ransomware: A Comprehensive Approach

Hima sai Muvva
Department of Computer Science
University of North Texas
Denton, Texas
himasaimuvva@my.unt.edu

kunaparaju hemanth varma
Department of Computer Science
University of North Texas
Denton, Texas
venkatanagasaihemkunaparaju@my.unt.edu

Tagore Hari Prasad Chintamaneni
Department of Computer Science
University of North Texas
Denton, Texas
tagorehariprasadchintamaneni@my.unt.edu

Jaideep Tripurani
Department of Computer Science
University of North Texas
Denton, Texas
jaideeptripurani@my.unt.edu

Ajay Eedara
Department of Computer Science
University of North Texas
Denton, Texas
ajayeedara@my.unt.edu

***Abstract*—Ransomware represents a significant cybersecurity threat, where malicious software restricts access to systems and data, demanding a ransom for their release. This project explores the deployment of ransomware, emphasizing the importance of preventative measures and the use of robust security practices by both individuals and organizations. We investigate the application of the Advanced Encryption Standard (AES) through the Fernet library in Python, leveraging its secure block cipher mechanism for the encryption and decryption of recursive file directories.**

Our project involves the creation of a proof-of-concept ransomware, which employs AES for data compromise. The infection vector is a simulated phishing attack utilizing social engineering tactics, demonstrating the ease with which attackers can exploit human factors. The ransomware's deployment within a controlled environment showcases the encryption process and subsequent demand for a ransom in exchange for the decryption key.

For countermeasures, we emphasize the significance of monitoring, detection, and mitigation strategies. The monitoring component includes the implementation of cybersecurity tools, host-level firewalls, and custom Python scripts for file integrity checks. Detection strategies are based on signature and behavior-based methods, with practical demonstrations using Windows Security and real-time protection tools.

Mitigation efforts focus on a combination of proactive and reactive approaches, such as user education, regular data backups, system updates, and employing antivirus solutions. We demonstrate the application of Windows security settings as a defense mechanism and develop a script for regular data backups, underlining the necessity of data redundancy and recovery planning.

Through this project, we not only shed light on the mechanisms of ransomware but also highlight the critical need for comprehensive cybersecurity policies and the empowerment of users in recognizing and responding to cyber threats. The learnings extend beyond technical solutions, advocating for a culture of security awareness that can significantly reduce the risks associated with ransomware attacks.

***Index Terms*—ransomware, cybersecurity, detection, mitigation, encryption**

I. Introduction

In the ever-evolving landscape of cybersecurity threats, ransomware has emerged as one of the most insidious forms of cyber attacks. Ransomware is a type of malicious software designed to block access to a computer system or data until a sum of money is paid. The effects of such attacks range from minor inconvenience to catastrophic data loss and significant financial damage. Notorious examples, such as WannaCry and Petya, demonstrate the disruptive potential of ransomware, making it a prime concern for cybersecurity experts worldwide.

This research paper delves into the intricacies of ransomware deployment, aiming to dissect its mechanisms and to propose robust countermeasures. Our focus is twofold: to understand the technical underpinnings of ransomware operations, and to emphasize the critical role of preventative strategies in thwarting such attacks. We utilize the Advanced Encryption Standard (AES) and Fernet library within Python to simulate the encryption and decryption processes that underlie ransomware functionality. By doing so, we offer a window into the attacker's modus operandi, enhancing our understanding of the threat landscape.

The deployment of ransomware is often facilitated by exploiting human vulnerabilities via social engineering techniques. To illustrate this, our project includes a simulated attack scenario that uses phishing emails to deploy ransomware. This practical demonstration underscores the importance of vigilance and education in preventing such breaches.

Simultaneously, our research examines the integral processes of monitoring, detection, and mitigation. Monitoring tools and techniques, such as host-level firewalls, Intrusion Detection Systems (IDS), and custom Python scripts, form the first line of defense, providing continuous oversight of system integrity. Detection methodologies, implemented through tools like Windows Security, offer real-time protection and play a

pivotal role in identifying breaches post-compromise.

The mitigation aspect of our study explores a combination of immediate and long-term responses. We present strategies that organizations and individuals can deploy to minimize the impact of ransomware, including the use of antivirus software, regular data backups, system updates, and adherence to best practices in cybersecurity.

Our contribution to the academic and practical realms of cybersecurity is a comprehensive analysis of ransomware threats complemented by demonstrable defense strategies. Through this paper, we aim to enhance the cybersecurity posture of potential targets by offering insights into the creation, execution, and prevention of ransomware attacks. We advocate for a resilient approach to cybersecurity, wherein awareness and preparedness are as crucial as technical defenses.

II. Related works

1. Ransomware Evolution and Mitigation Techniques: A study published in the "Journal of Cybersecurity" explores the evolution of ransomware from simple locker variants to complex encryption-based software. The paper highlights how ransomware exploits network vulnerabilities and suggests mitigation strategies, including the implementation of advanced intrusion detection systems (IDS) and regular system backups. The authors also emphasize the importance of security awareness training to prevent phishing and other social engineering attacks.

2. The Effectiveness of Fernet and AES in Ransomware Defense: An article in "IEEE Security and Privacy" discusses the use of symmetric encryption algorithms like AES and the Python library Fernet in the context of ransomware. The paper evaluates their robustness against various attack vectors and presents a case study of a simulated ransomware attack in a controlled environment. The findings suggest that while AES is secure, the key management and secure key distribution mechanisms are critical for preventing unauthorized decryption.

3. Case Studies on Major Ransomware Attacks: A comprehensive analysis in "Computer Fraud and Security" magazine reviews several major ransomware attacks, including WannaCry and Petya. This work details the methods used by attackers, such as exploiting the EternalBlue vulnerability, and discusses the impact on global businesses. The case studies are used to advocate for a multi-layered security approach combining technology, policy, and user education to enhance resilience against ransomware.

4. Comparative Study of Ransomware Detection Techniques: Researchers in the "Journal of Network and Computer Applications" provide a comparative analysis of signature-based and behavior-based detection methods for identifying and mitigating ransomware attacks. This paper highlights the limitations of traditional antivirus software and the potential of machine learning-based detection systems that adapt to new, unknown ransomware variants.

5. Impact of Ransomware on Cyber Insurance: A recent publication in "Risk Management and Insurance Review" examines the role of cyber insurance in managing ransomware risks. The study assesses how insurance policies are adapting to cover ransomware incidents and discusses the interplay between cybersecurity measures and insurance requirements. It also explores the concept of "silent cyber" risks, where insurance coverage for cyber incidents is ambiguous or unintended.

https://www.mdpi.com/2071-1050/14/1/8
https://academic.oup.com/cybersecurity/article/6/1/tyaa023/6047253

III. Approach

A. Research on ransomware techniques

Understanding Ransomware Ransomware infiltrates systems through various methods such as phishing emails, malicious advertisements, exploiting software vulnerabilities, or through Trojans disguised as legitimate files. Once activated, it typically ensures persistence by modifying system files or registry entries to automatically execute at startup. It then identifies and encrypts valuable files using robust encryption algorithms, often targeting documents, images, and databases. These encryption methods usually involve strong symmetric or asymmetric techniques like AES and RSA, with each instance generating a unique encryption key. Post-encryption, victims are presented with a ransom note demanding payment, commonly in cryptocurrencies like Bitcoin, to obtain the decryption key.

Common Techniques and Strategies Ransomware attacks are characterized by several common techniques: - Encryption Algorithms: Utilization of strong encryption to make decryption nearly impossible without the unique key. - Payment Anonymity: Demand for ransom through cryptocurrencies to maintain the attackers' anonymity. - Kill Switches: Some ransomware includes a hardcoded URL or condition that can deactivate the malware, a method seen in the WannaCry ransomware attack. - Polymorphism and Obfuscation: These techniques help ransomware evade antivirus detection. - Double Extortion: In addition to encryption, attackers may exfiltrate confidential data and threaten to leak it unless the ransom is paid. - Ransomware as a Service (RaaS): This business model involves ransomware creators selling or leasing their malware to others for attacks, sharing the profits generated.

Development Approaches The development of ransomware involves understanding cryptographic algorithms and network programming for managing command and control servers. Ethical considerations are paramount; research should aim to enhance security defenses and must be conducted under controlled environments to prevent misuse.

Ethical Considerations It is crucial to approach ransomware research with ethical integrity, focusing solely on improving cybersecurity defenses, testing system vulnerabilities, and developing robust countermeasures.

Prevention Strategies To mitigate ransomware risks, the following preventive measures are recommended: - Regular Data Backups: Implementing consistent backup procedures to restore data in case of an attack. - Incident Response and Data Security Policies: Developing strategies and policies detailing

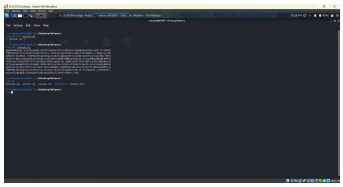

Fig. 1. encryption

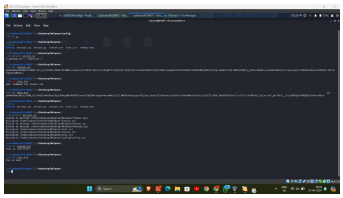

Fig. 2. Decryption

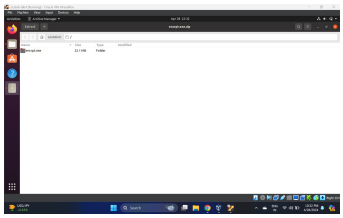

Fig. 3. exe file

organizational responses to attacks and data protection methods. - Port Management: Monitoring and blocking unnecessary ports to reduce potential entry points for attacks. - Endpoint Hardening: Securing devices by disabling unnecessary functionalities and using strong passwords. - System Updates: Regularly updating systems to patch security vulnerabilities. - Employee Training: Educating staff on identifying ransomware risks, recognizing phishing attempts, and other security threats. - Intrusion Detection Systems (IDS): Installing systems to detect and prevent potential ransomware threats.

This literature review lays the foundation for our project by detailing the operation and impact of ransomware, guiding our subsequent research and development phases aimed at enhancing cybersecurity measures.

B. Action

Ransomware is a type of malware that encrypts files and systems, holding them hostage until a ransom is paid. High-profile ransomware incidents include attacks like WannaCry and Petya.

It's crucial for both individuals and organizations to prevent such attacks by regularly backing up data, creating data redundancy, and conducting user training to recognize phishing attempts and adopt robust security protocols.

AES (Advanced Encryption Standard) is a widespread encryption algorithm securing data at rest and in transit. Operating as a block cipher with fixed sizes of 128 bits, AES supports key lengths of 128, 192, or 256 bits. It's known for its complexity and resistance to breaches, involving various layers of mathematical computations.

In the context of ransomware, we utilize the Fernet library, which employs the AES standard for file encryption and decryption within directories.

Our team is focused on developing a method to encrypt and decrypt files stored on a drive using Symmetric Key Encryption with the AES algorithm. Given its widespread adoption and the comprehensive library support in Python, we're leveraging this programming language for our ransomware development. We use the Fernet library along with Python's cryptographic functions to manage the encryption process, starting with the creation of a symmetric key, followed by its use in encrypting files with AES. For decryption, the same key is supplied to the recipient.

The initial infection vector is a phishing email, and the release of the decryption key is through the original communication channel after the ransom is fulfilled.

Our methodology incorporates insights from various resources, such as accessing file paths, importing necessary cryptographic libraries, and managing the symmetric key to encrypt and decrypt a targeted directory. We also studied different communication methods to securely exchange decryption keys.

C. Infection

In this infection phase we have performed using a real life simulating method which has been a real thing in the outer world. we are performing phishing mail method for infecting the victim.based on the info collected about the user we can perform a social engineering method to infect the ransomware malware to the users system.first we are attaching the malicious file with the application and later the application is attached to the mail in the way the user thinks it's a legitimate mail and the user will definitely tends to open the mail. after opening the link the application will be directly downloaded into the system and encrypts the complete directory recursively.we drafted a mail preferring the interests of the victim.we created a mail stating that the he gets a free coupon for the oscp certification if he go through this link.after this it will encrypt the downloaded path and we can use this for ransom we can decrypt the file by sharing the same symmetric key with the victim.

D. Monitoring

Monitoring involves the continuous observation of a system to identify security issues, utilizing a combination of cybersecurity tools and manual scripts that operate as backend services on the operating systems. To secure individual systems, we can deploy host-level firewalls, intrusion detection systems (IDS), and file integrity monitoring tools. In an enterprise production environment, more advanced security measures are typically in place, including Web Application Firewalls, Network Firewalls, Intrusion Prevention Systems (IPS), and network antivirus solutions to monitor traffic for malware, conduct file integrity checks, and detect vulnerabilities.

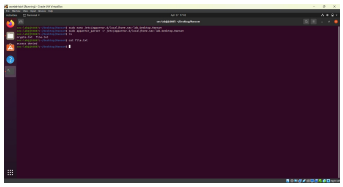

Fig. 5. using apparmour

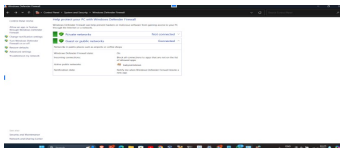

Fig. 6. detection

For systems running Windows, tools like Snort may be utilized. We also employ security software such as Malwarebytes and Kaspersky, along with custom Python scripts that monitor and report changes in file integrity. Through our research, we discovered tools like Zscaler ZIA, which can be tailored to different environments to monitor and block activities based on the category of the detected malware. We primarily developed a Python script that alerts us to file alterations and integrated it with Malwarebytes and Kaspersky for enhanced monitoring and detection capabilities.

Throughout this project, our team has gained a comprehensive understanding of ransomware deployment, monitoring techniques, and various types of malware, enriching our collective knowledge and expertise in these areas.

E. Detection

There are various strategies for the identification of cybersecurity threats, including both signature-based and behavior-based detection mechanisms. In our specific scenario for ransomware detection, we are leveraging the built-in security measures and real-time protection features offered by Windows, which are effective against many known forms of malware, such as viruses and ransomware, thanks to their continuously updated definitions.

Our team is also considering the deployment of advanced detection systems such as Snort or the Qualys cloud agent to enhance our defensive posture. In the realm of corporate security, tools like CrowdStrike are prominent for their capabilities in identifying and thwarting malware intrusions. Nevertheless, the most straightforward method remains the activation and proper configuration of Windows Defender, which stands as a capable line of defense due to its efficiency.

F. Mitigation

Mitigation strategies focus on immediate containment and long-term prevention. Our implementation includes an educational campaign simulating the discovery of ransomware activity, followed by steps to isolate infected systems and restore data from backups. Windows security features, such as controlled folder access, serve as an additional layer of defense, preventing unauthorized changes to sensitive files.

Our project integrates theoretical knowledge with practical demonstrations, bridging the gap between understanding ransomware and effectively combating it. By meticulously documenting each step of our project, we present a replicable model for cybersecurity practices, emphasizing the importance of proactive defense mechanisms and informed user behavior in the fight against ransomware.

IV. Result

In conclusion, our study on attacks using ransomware provides a thorough examination of the details of their deployment, the vulnerabilities they exploit, and the direct effects they cause. We demonstrated the ease with which these assaults may be carried out by creating a proof-of-concept ransomware utilizing the AES encryption standard and Python's Fernet library, notably through social engineering approaches like phishing. Our research highlights the critical need for strong cybersecurity measures and user attention. The use of strong encryption practices and the simulation of ransomware attacks in a controlled setting highlight the vital role of security awareness and proactive defenses in reducing the disastrous impacts of such cyber threats. Furthermore, our findings provide insight into effective monitoring, detection, and mitigation options for protecting against ransomware.

In the Final as a team we have implemented the Ransomware from Development, Infection, Monitoring, detection and till the mitigation of malware Ransomware.

References

[1] 1. J. Hurtuk et al., "Case Study of Ransomware Malware Hiding Using Obfuscation Methods," 2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA), pp. 215-220, doi: 10.1109/ICETA.2018.8572218.

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

[3] 3. R. Wilson and I. Iftimie, "Emerging ransomware threats: An anticipatory ethical analysis," 2021 IEEE International Symposium on Technology and Society (ISTAS), pp. 1-1, doi: 10.1109/ISTAS52410.2021.9629211.

[4] 4. P. K., B. Nataraj, and P. Duraisamy, "An Investigation on Attacks in Application Layer Protocols and Ransomware Threats in Internet of Things," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 668-672, doi: 10.1109/ICACCS57279.2023.10112669.

[5] 5. L. Y. Connolly, D. S. Wall, M. Lang, and B. Oddson, "An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability," Journal of Cybersecurity, vol. 6, no. 1, 2020, doi: 10.1093/cybsec/tyaa023.

[6] 6. A. Kapoor et al., "Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions," Sustainability, vol. 14, no. 1, p. 8, 2021, doi: 10.3390/su14010008.