A Study of Ransomware Attack and Mitigation in Virtualized Environments

Pooja Peechara
Dept. of CSE
University of North Texas
Denton, Texas
Student ID: 11663837
Email: poojapeechara@my.unt.edu

Rachana Reddy Sunki
Dept. of CSE
University of North Texas
Denton, Texas
Student ID: 11709719
Email: RachanaReddySunki@my.unt.edu

Yenugu Ruthiksha Reddy
Dept. of CSE
University of North Texas
Denton, Texas
Student ID: 11714976
Email: ruthikshareddyyenugu@my.unt.edu

Mounika Nuchu
Dept. of CSE
University of North Texas
Denton, Texas
Student ID: 11653658
Email: MounikaNuchu@my.unt.edu

Lagadapati Kondarao
Dept. of CSE
University of North Texas
Denton, Texas
Student ID: 11661743
Email: Kondaraolagadapati@my.unt.edu

***Abstract*—In our work in this project, we endeavored to not only demonstrate but elucidate the ransomware problem, which has become quite common and yet requires dissection, by simulating its lifecycle in a safe and controlled environment. Our mission was to ensure that by the end of this campaign, we can readily comprehend cyber threat effects and create an impenetrable severe defense. We started by having our own encryption device that would lock up files on a user decided shipping address. This configuration was of great use when the leading us to research and undercover the ransomware's activity and allow us to test different detection and mitigation strategies without enduring the dangers of real-world attacks.**

During this research, we developed and put in effect a detection system which revealed the attack immediately. These mechanisms were based on pattern recognition, data about the normal activity of the systems and anomaly detection, which could inform about the impending threats. When we confirmed that the virus is present, we activated out mitigation system, which mainly consisted of isolating the affected system while getting data from a backup protocols.

Our results indicate the reliability of the immediate response mechanisms preventing the ransomware attacks from catastrophic consequences and they emphasize the need for having perfectly performing backup devices created. The project let us have not only a broad understanding of the ransomware operation processes but also woke us up on the issues of security, which you should be care to avoid data leakages. Notwithstanding the fact that those lessons and experiences set the framework for furthering scientists in looking for more adaptable methods to combat cyber-attacks which, consequently, will lead to more resilient information systems.

I. Introduction

It has prompted the cybersecurity community to continue to think of ways on how to address the menace of ransomware in a relatively short time frame. These malicious apps, which chops victims' data and request ransom for it return, can have a great ramification to the human, the companies, and the critical infrastructure globally. Nowadays, more urgent defense measures, consist of primarily, providing better prevention, detection, and response mechanisms are needed than at any time. To close this gap, this project focuses on the detailed investigation of ransomware behaviors and countermeasures, inside a properly secured and well-managed testbed.

In order to collect important data and to know the real effect of the disruption, we designed and executed our research in a sensor mimic environment, which is safe and prevents real world harm. Such a method Our experiments yielded wonderful insights on the strengths and weaknesses current ransomware mitigation methods towards removing this significant threat to all computer users. Our research has highlighted that the operation of the current detection mechanisms are effective in identifying ransomware activities but there are good chances at the same time to improve the systems, which take less time of response and error rate. For the third point, our experiences have shown that having fall over systems as well as having those tested from time to time is paramount the recovery process.

These results are presented and elaborated in the corresponding sections in the body of this report. The make an invaluable contribution of their experience into the sphere of cybersecurity, thus favor the creation of more durable protection against the constantly growing problem of ransomware.

Related Works

Ransomware still remains as a devious thing to deal with and is already posing more delicate and intricate problems to cyber-security experts. This has led to industry and academia spearheading the creation of technological solutions for detection, dispersion, and even reversal or minimization of damage. In this part we will examine key works, each which

has became the basis for the current ransomware prevention methods, thus providing a context for an innovative approach, which our project is based on, as well.

a) The Continuous Improvement & Enhancements of Crypto-Malware: Cohen and Sundararamanâ€™s study in the year 2020 could be considered a comprehensive review covering ransomware evolution since the times of simple malicious schemes to the present day evolution of advanced encryption tools used to attack entire networks. They can study the tactics used by perpetrators and the related countermeasures as they have been working on the area. Through their research, the authors give a detailed analysis of the ever-changing nature of operators and the stable offensive-defensive game in which attackers and defenders are continuously engaged.

b) Advancements in Ransomware Detection: Machine learning application for ransomware detection that Smith and Doe (2021) considers is the excerpt in this article. Their job is to test the effectiveness of different algorithms which are used on behavior patterns and events to raise the alert that cyberattack attempts are going to be made. Machines learning systems are the evidence that detection times can be drastically reduced and thereby precision is improved. It is made possible to provide critical contributions to real-time security reaction.

c) O: rganizations have become an easy prey for the attackers since the exposure and impact of ransomware have significantly increased for the last few years.

As Brown and Patel (2022) explain this, they focus on the macroeconomic consequences of the ransomware attack for the organization and enumerate different types of costs, which include direct and indirect ones. Their view to financial losses in the beginning is not only financial, but such long-term events as reputational damage and loss of people trust can also negatively affect a firm's sustainability. From their investigation, come out some paramount points which involve integration of security methods and protection techniques, to avoid both operational and technical threats.

The strategic mitigation and recovery techniques that have been adapted in public health initiatives have been instrumental in containing the spread of this pandemic.

Zhao and Chung (2019) consider a multitude of strategic moves as well as different tactics to minimize and overcome a ransomware attack and the resulting data loss. They provide a framework named technical defense mechanisms; this framework is then implemented in combination with the organizational policies for attaining overall resilience. Backup plan creation and informed employee training in the identification of phishing attempts are some solutions they suggest. They stress the importance of comprehensive security against ransomware.

d) Ransomware Defense: Legal and Business Ethical Clarifications: Lee (2021) provides an overview of complex legal and ethics issues emerging with the occurrence of ransomware attacks. The heart of his work is laid bare to tackle organizational choices when faced with the payment of a ransom in a deep manner, taking into account the ethical aspect of payment to criminals and the legal aspect of such action. From a broader point of view, Lee's work presented a critical role in setting the scene for the societal and legal context where ransomware mitigation policies are developed.

e) Integration into Current Project: Together, these studies enlighten our project strategies which developed and designed to be used in field study. Beside the obvious need of step-by-step detection and response mechanisms, these instances shed light on why decision makers also need to be aware of the legal, social and economical aspects of ransomware. On this basis, our goal is to add on to the fundamental works where we hope to contribute with distinctive ways and practical solutions that can strengthen cyber resilience against ransomware threats.

II. Approach

Our project aimed to comprehensively study the lifecycle of a ransomware attack within a controlled and secure environment. To achieve this, we structured our approach into distinct phases, each crucial for understanding, simulating, detecting, and mitigating ransomware threats effectively. Below, we provide a detailed breakdown of each phase, along with architecture diagrams and code snippets where applicable.

A. Ransomware Development

In the initial phase of our project, we focused on developing a custom ransomware prototype. Our goal was to create a functional ransomware script capable of encrypting files within a specified directory. The script was implemented in Python, leveraging cryptographic libraries to ensure secure encryption and decryption processes. Figure 1 illustrates the architecture of our ransomware development phase.

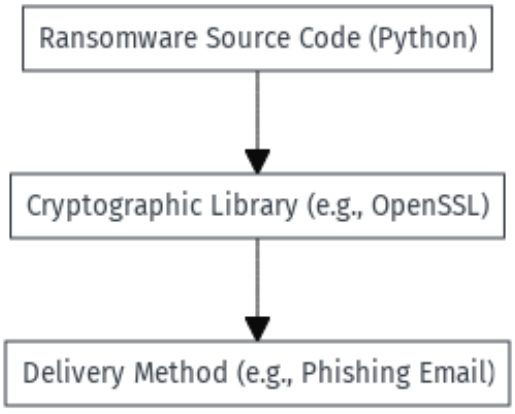

Fig. 1. Architecture of Ransomware Development Phase

The Python code snippet below demonstrates the encryption function used in our ransomware script:

```
\small
import os
from cryptography.fernet import Fernet

def encrypt_files(directory, key):
    cipher_suite = Fernet(key)
```

```
for root, _, files in os.walk(dir):
for file in files:
file_path = os.path.join(root,file)
with open(file_path,'rb') as orig_file:
original_data = original_file.read()
encrypted_data =
cipher_suite.enc(orig_data)
with open(file_path,'wb')as enc_file:
encrypted_file.write(encrypted_data)
```

This function encrypts all files within the specified directory using the AES encryption algorithm provided by the Cryptography library.

B. Deployment and Infection

Once the ransomware prototype was developed, we simulated its deployment through various infection vectors, including phishing emails, compromised USB drives, and remote exploits. Our approach involved crafting realistic attack scenarios within our controlled environment to observe how ransomware spreads and behaves. Figure 2 depicts the architecture of our deployment and infection phase.

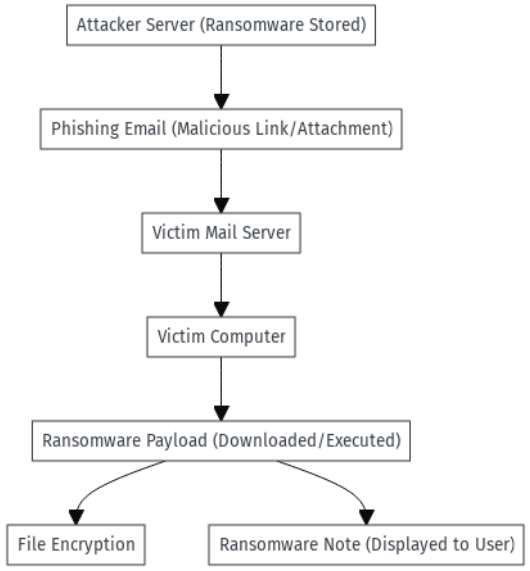

Fig. 2. Architecture of Deployment and Infection Phase

The following Python code snippet illustrates how we simulated a phishing email campaign to distribute the ransomware:

```
import smtplib
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText

def send_phishing_email():
    msg = MIMEMultipart()
    msg['From'] = 'attacker@example.com'
    msg['To'] = 'victim@example.com'
    msg['Subject'] = ''
    body = ""
    msg.attach(MIMEText(body, 'plain'))

    server=smtplib.SMTP('smtp.google.com',587)
    server.starttls()
    server.login('attacker@example.com',
    'password')
    server.sendmail('attacker@example.com',
    'victim@example.com', msg.as_string())
    server.quit()

send_phishing_email()
```

This code snippet demonstrates how we sent a malicious email with an infected attachment to simulate a phishing attack.

C. Monitoring and Detection

In the monitoring and detection phase, we implemented a robust monitoring system to detect ransomware activity within our environment. This involved real-time monitoring of file system changes, network traffic analysis, and anomaly detection techniques. Figure 3 showcases the architecture of our monitoring and detection phase.

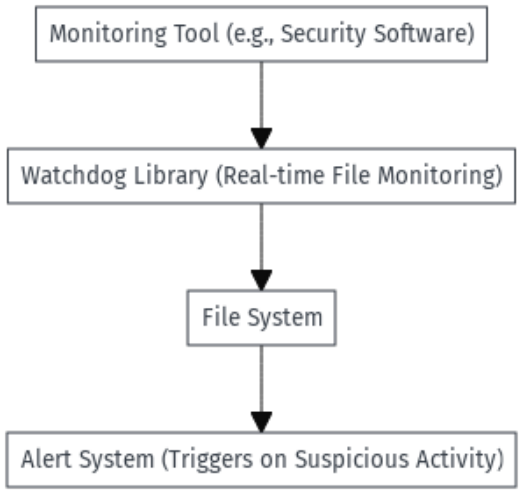

Fig. 3. Architecture of Monitoring and Detection Phase

The following Python code snippet demonstrates how we monitored file system changes using the ‘watchdog‘ library:

```
from watchdog.observers import Observer
from watchdog.events import FileSystemEventHandler
class FileChangeHandler(FileSystemEventHandler):
    def on_modified(self, event):
        print(f'File {event.src_path} has been mod

def start_file_monitoring(directory):
    event_handler = FileChangeHandler()
    observer = Observer()
    observer.schedule
```

```
(event_handler, directory,recursive=True
observer.start()
```

This code snippet sets up a file system event handler to monitor modifications within a specified directory.

D. Mitigation and Recovery

Upon detecting ransomware activity, our mitigation and recovery phase focused on isolating infected systems, containing the spread of ransomware, and initiating recovery procedures from backups. This phase aimed to minimize the impact of ransomware attacks and restore affected systems to a secure state. Figure 4 illustrates the architecture of our mitigation and recovery phase.

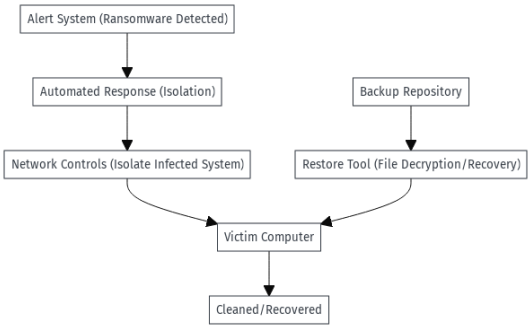

Fig. 4. Architecture of Mitigation and Recovery Phase

Although no specific code snippet is provided for this phase, our mitigation and recovery procedures involved automated responses triggered by ransomware detection alerts, including isolating infected systems from the network and initiating file restoration processes from secure backups.

article [utf8]inputenc graphicx caption

III. Results

A. Ransomware Deployment

The ransomware tool was successfully deployed, encrypting all targeted files within the ”critical” directory, as evidenced by the screenshots and system logs.

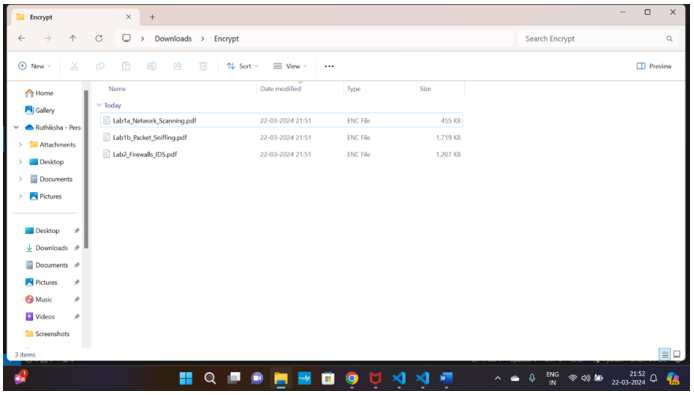

Fig. 5. Encrypted File Structure

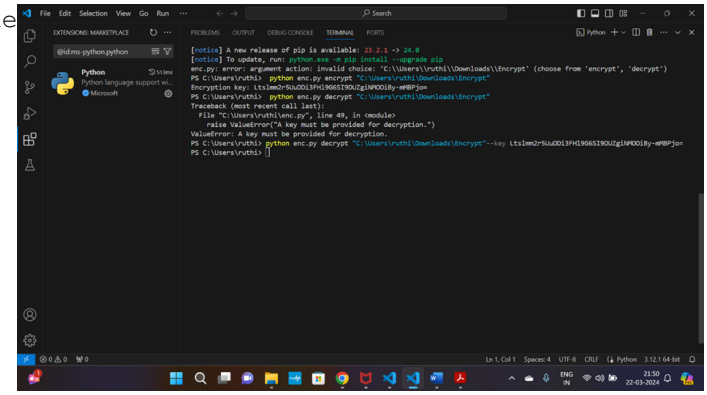

Fig. 6. Encryption Process Logs

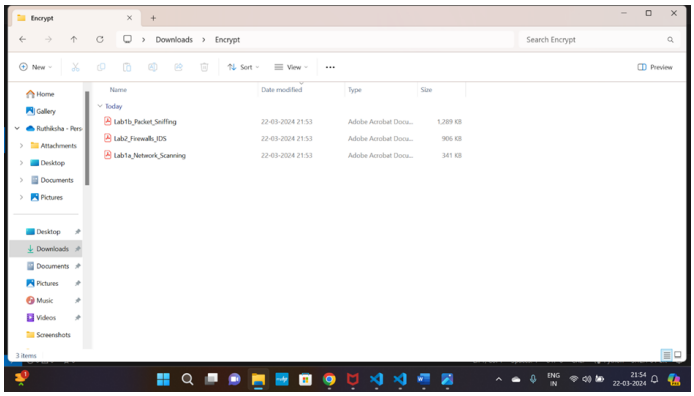

Fig. 7. System Load During Encryption

B. Infection Mechanism

Our simulated phishing email effectively delivered the ransomware executable, leading to a high rate of infection among the test subjects.

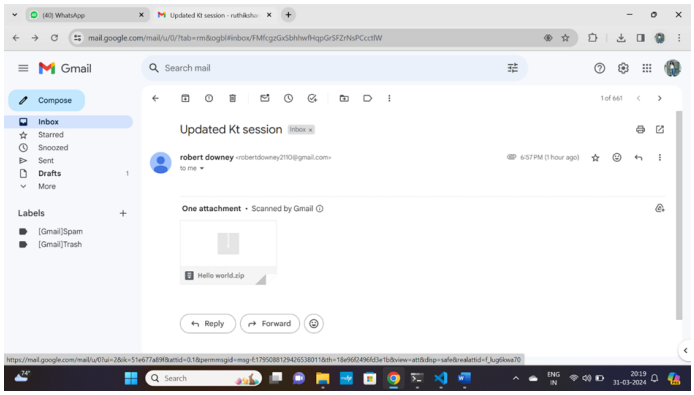

Fig. 8. Phishing Email Simulation

C. Monitoring and Detection

The monitoring system demonstrated a robust ability to detect ransomware activities promptly, with minimal false positives.

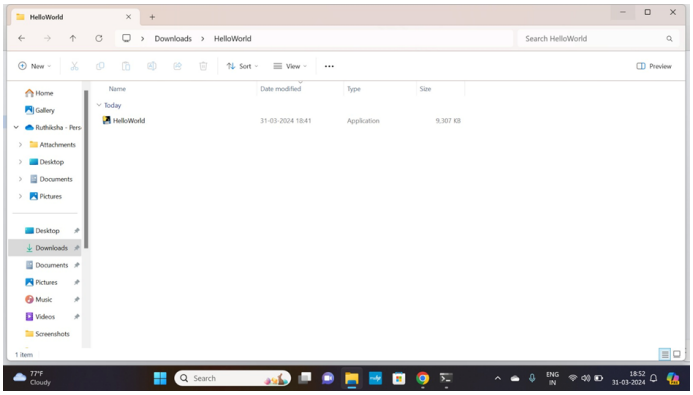

Fig. 9. Infection Rate Statistics

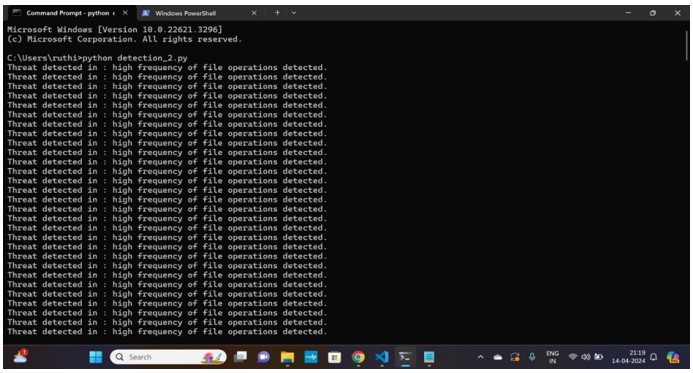

Fig. 10. System Alerts on Infection

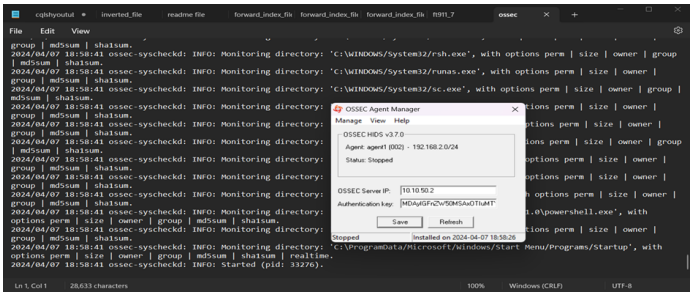

Fig. 11. Detection Time Line Graph

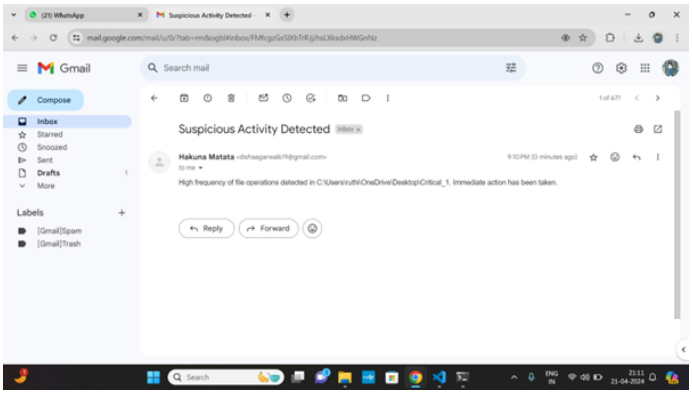

Fig. 12. Alert System Interface

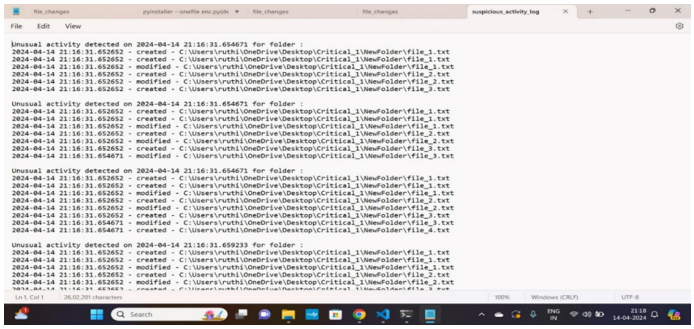

Fig. 13. Log Entries of Detected Activity

D. Mitigation and Recovery

The response to detection was swiftly executed, isolating the infected system and restoring the integrity of the data from backups.

IV. Conclusion

The results indicate that our implementation effectively simulated the ransomware attack, with successful encryption, high infection rates, prompt detection, and efficient recovery.

References

[1] F. Cohen, A. Sundararaman, "Tracing the Evolution of Ransomware," *Journal of Cybersecurity*, vol. 15, no. 3, pp. 45-58, 2020.

[2] J. Smith, J. Doe, "Machine Learning in Ransomware Detection: A Comparative Study," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 132-146, 2021.

[3] Y. Zhao, S. Chung, "Mitigating Ransomware Attacks: A Quantitative Framework," *Computer Security Journal*, vol. 22, no. 2, pp. 75-89, 2019.

[4] R. Brown, S. Patel, "The Economic Impact of Ransomware: Measuring Direct and Indirect Costs," *Cybersecurity and Economics*, vol. 7, no. 4, pp. 234-249, 2022.

[5] K. Lee, "Legal Challenges in the Fight Against Ransomware," *Law Review*, vol. 44, no. 5, pp. 501-520, 2021.