Ransomware Incident Report

Presented by:

Ahmed Elhalwagy
Ahmed Khaled
Ali Ibrahim
Anas Khalil
Priskila Nabil
Yosef Khaled

Presented for: Eng. Ahmed Abulhamd

Table of

CONTENTS

Situation

Preliminary analysis suggests that the ransomware entered the network via a phishing email received by an employee in the finance department.
The email contained a malicious attachment named 7labesa.zip that was protected with a password , when uncompressed it and run the file in it 7labesa.xlsx it executed the ransomware payload.

Date of Report : 09/05/2024

Entry point

We faced an unusual situation on our systems and after we investigated we found that there is a Ransomware stormed in our systems by phishing mail inside it there was an excel sheet and let's go to see our
investigate 👇

Affected Systems

- Number of Affected Workstations: 15
- Number of Affected Servers: 2 (File Server and Database Server)
- Network Segments: Corporate LAN, Finance Department

Impact Assessment

- Data Encrypted: Approximately 50 GB of critical financial data, customer records, and operational documents.
- Operational Downtime: Finance department operations were disrupted for 2:20 hours, resulting in delays in financial reporting and client services.
- Data Loss: No permanent data loss, as files were restored from backups.
- Financial Impact: Estimated at $50,000, including recovery costs, downtime, and potential fines.

Detection and Response Timeline

- **4:00 PM:** An Employee received an phishing email from the attacker contained a 7labesa.zip file protected with a password
- **4:20 PM:** The Employee uncompressed the zip file and ran the 7labesa.xlsx file
- **5:15 PM:** Unusual file activity detected on workstations by the Endpoint Detection and Response (EDR) system.
- **5:20 PM:** Initial investigation initiated by the SOC team.
- **5:30 PM:** Confirmation of ransomware activity (files encrypted with .7labsa extension).
- **5:35 PM:** Affected systems isolated from the network to prevent further spread.
- **5:40 PM:** Incident response team (IRT) mobilized, and a full-scale investigation initiated.
- **5:45 PM:** Ransom note discovered on affected systems, demanding 2 BTC (Bitcoin) for decryption keys.

Prioritizing Critical Updates

To effectively mitigate vulnerabilities, we prepared a strategy of prioritizing critical updates to software and systems that are most likely to be exploited by attackers. This included:

- Monitoring security advisories: We stayed informed about security advisories and release notes from software vendors to identify critical vulnerabilities.
- Prioritizing patches: We developed a patching schedule that prioritized updates for systems with the highest risk of exposure.

Threat Intelligence Platforms (TIP)

- Information gathering: TIPs provide insights into trending attacks, targeted companies, and hacker techniques.

SIEM Solutions

- Alert monitoring: SIEM solutions monitor alerts generated by security rules.

Endpoint protection:

- EDRs protect endpoints from attacks

Testing Backups

- To ensure the effectiveness of our backups in case of a disaster or breach, we prepared a strategy of regularly testing them. This involved:
- Creating test scenarios: We developed realistic scenarios that simulated data loss or system failures.
- Restoring data: We practiced restoring data from backups to verify their integrity and functionality.
- Automating recovery: We implemented automated recovery procedures to streamline the process of restoring systems and data in the event of a disaster.
- Regularly updating backups: We ensured that backups were updated frequently to capture the latest changes and prevent data loss.

- At 5:15 PM the EDR detected unusual file activity
- We noticed a high usage of 15 workstations resource
- we noticed spike in disk activity and increased CPU as the script uses up system resources to perform searches and encrypt the files.
- Inability to access certain files
- Backups are being tampered within an attempt to prevent the victim from restoring their files.
- Network is scanned inside your network, thus suggesting that the attackers are trying to move laterally from one system to another.
- The SIEM alerted for Detect CPU Usage Exceeding 80%
- Communication with a suspicious server was detected.

Rule used to detect on SIEM

Rule: Detect CPU Usage Exceeding 80%

Objective: Identify when the CPU usage on any system exceeds 80%, which could indicate a potential issue such as a ransomware activity, malware, or resource-intensive process.

Actions:

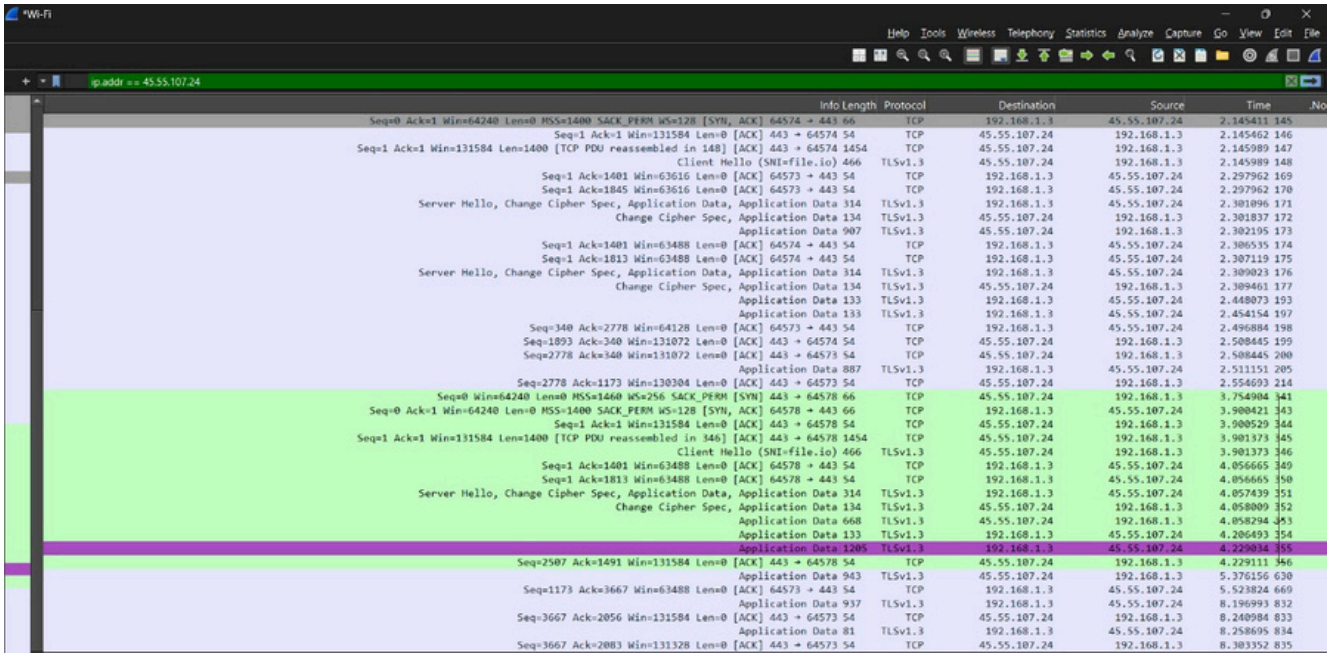
- Alert: Trigger an alert when CPU usage exceeds 80% for more than the specified duration.

- Notification: Send a dashboard notification to the relevant SOC team.

Note: if a process like 7labesa.xlsx starts encrypting files and consumes significant CPU resources, the SIEM would detect the CPU spike, generate an alert, and initiate the investigation process.

Scoping

- We detecting malicious traffic to this IP 45.55.107.24 in our environment So we added all the hosted communicated with this IP to the inflicted scope
- We added all endpoints that came from it an EDR alert in the inflicted scope



Containment

- **Horizontal Segmentation: We began the containment process by isolating all identified compromised hosts. Each affected system was moved to a dedicated VLAN to prevent lateral movement and limit the scope of the infection.**
- **Dedicated VLANs: The VLANs were configured to ensure that isolated hosts could not communicate with each other or with other segments of the network. This helped in preventing the ransomware from spreading further and reduced the risk of cross-contamination.**
- **Apply firewall rules or network segmentation to restrict traffic from or to affected systems.**

Root Cause Analysis:

- an employee received attachment

named was 7labesa.zip when he uncompressed it
the 7labesa.xlsx file showed up

- the employee opened 7labesa.xlsx
- The exploitation happened using excel macros

Extracting IOCs:

- by analysis the excel file we identified the c2 server IP 186.144.12.3
- also We calculated the md5 hash and sha1 hash of the 7labsa.xlsx
- md5: 0a2b88cbe9165d09105023720db7de6b
- sha1: 4a6617c7ffdc23be51dd22910497296fff6744ba
- Archive Name: 7labesa.zip
- File Name: 7labesa.xlsx

Identify persistence

Attackers used WMI to maintain persistence on a compromised system by creating WMI event subscriptions.
This subscription is triggered after 5 mins of booting

At 6:30 pm we started Re-imaging the inflicted systems
We restored the golden image of our system to make sure we completely wiped up the malware

Recovery

introduction:

At 8:00 PM we start the recovery phase , We focused on restoring essential data like financial records, customer information, and intellectual property.

recovery for a vertical and horizontal containment on server

Re-establish Network Connectivity (Horizontal Recovery)

We re-established network connectivity to the server in a controlled and phased manner. Starting with limited connectivity, we carefully monitored network traffic for any signs of malicious activity. Once we were confident that the threat had been neutralized, we tested communication between the server and other critical systems(by Ping Test Send ,ICMP echo requests to the server from different network locations to verify basic connectivity.) to ensure proper functionality. Then, we gradually re-enabled essential services and processes, ensuring that each was secure and necessary before proceeding to the next. This phased approach minimized the risk of reintroducing the threat and allowed us to restore full functionality while maintaining a high level of security.

Reinstate User Access (Vertical Recovery)

We gradually restored user permissions and roles, starting with administrative accounts. We implemented stricter access controls and monitored user activities closely. We reviewed and strengthened authentication mechanisms, such as passwords, multi-factor authentication (MFA), and access control policies. We ensured that any compromised user credentials were reset and strengthened to prevent unauthorized access.

monitor the affected machine :

Proactive Threat Detection with Log Review

It was essential to review system logs to safeguard our systems' integrity and security. By examining logs from the operating system, firewall, and other security tools, we could identify potential threats and take appropriate countermeasures. Additionally, scrutinizing logs from critical applications enabled us to detect unusual errors or unauthorized access attempts. Through a comprehensive analysis of these logs, we could proactively address security risks and ensure the protection of our valuable data and systems.

Ensuring Data Integrity with Verification Procedures

To maintain data integrity, rigorous verification procedures are essential. Hash verification involves comparing the hashes of critical files before and after recovery. File comparison tools can further verify the content of important files, ensuring they match their original versions. Checking the consistency of databases and other critical systems is also crucial to prevent data loss or corruption. Through these verification processes, we can maintain data reliability and accuracy, protecting it from potential threats and ensuring business continuity.

Restoring Backup:

We restored affected systems and data from clean and offline backups, which allowed the organization to resume normal operations without having to pay the ransom or use the attacker’s decryption tool, which might not have worked.
Ideally, we aimed to restore as much lost data as possible using backed-up data. However, caution was necessary, as ransomware could have dwell times of up to six months, potentially including malware in archival backups. Before restoring, we ran an anti-malware package on all systems.

system checkup:

Work with the Finance Department to resume operations, ensuring that all critical systems are functional.
Communicate with clients about potential delays and ensure transparency.

- **Increase Employees Awareness:**

1. Learn the most common signs of malwares
2. Examine the links and file attachments before clicking them.
3. Understand how phishing works and check email addresses of incoming messages.
4. Teach them that if they found any wired email to consult the SOC team first

- **Regularly update our EPP:**
  Regularly update our EPP with new malwares signatures

- **Regularly scan your infrastructure**

Install and use anti-malware software that will notify you of any possible threats, identify potential vulnerabilities, and detect ransomware activities in your infrastructure. Modern anti-ransomware tools enable you to scan your entire system for existing viruses and active malware threats. Moreover, such computer scans can run either on demand or based on a schedule you set up, thus minimizing the management input on your part.

- **Restrict access to critical systems and applications**

Apply the principle of least privilege when granting employees permissions to systems. The principle involves giving an employee access only to those files and system resources that are required to do their work efficiently. Any action or access that is not necessary for an employee to perform their duties should be prohibited by the admin to avoid accidental infections.

- **Threat Intelligence and Collaboration:** Share details about the attack and IOCs with relevant Information Sharing and Analysis Centers Participate in threat intelligence sharing groups to stay informed about emerging threats and TTPs

Invest in Email Detection and Response

- platforms that provide real-time visibility into phishing attempts. These tools can automatically analyze and quarantine suspicious emails, helping reduce the likelihood of users interacting with malicious content

Threat Hunting

- **Deep Analyze Logs:** Review logs from the SIEM to identify unusual patterns or activities around the time of the attack to identify other intention for the malware
- **Identify the TTPs the attacker used in our Environment:** After Identifying this TTPs the threat hunters hunted in all of our environments for this attack.
- **Trace the Group that was responsible for this Attack:** using Threat intelligence the Threat hunters were able to identify the group that did the attack
- **Identify Persistence Mechanisms**: Examine logs for signs of persistence
- **Hypothesis-driven investigation:** giving insights into attackers' latest tactics, techniques, and procedures (TTP)