Incident Report: Simulation of Hidden Tear Ransomware Attack

**1. Executive Summary**

This incident report is based on the Hidden Tear ransomware attack simulation within a controlled virtual lab and we used Virtual Box. The exercise is meant to simulate the ransomware attack, chronicle the timeline of the attack, present forensic proof, and suggest mitigation. Everything is done with educational purposes in mind and with regard to cybersecurity readiness.

**2. Incident Overview**

Incident Name: Simulation of Hidden Tear Ransomware Attack

Date of Incident: May 5, 2025

Incident Identified: May 5, 2025 at 7:00 PM (System logs report first detection time)

Incident Duration: 2 hours (Containment, Eradication, and Recovery phases)

Systems Involved: A virtual machine (VM) with a test system containing user data files.

Description of Attack: User files were encrypted by the ransomware (Hidden Tear) with the.locked extension, and a ransom note (READ\_IT.txt) was left on the Desktop. Hidden Tear is a test ransomware, used mostly for teaching. It encrypts files with the AES encryption algorithm and requests a ransom for decryption.

**3. Attack Timeline**

7:00 PM - Initial Detection: User observes files on the desktop will not open. Files are encrypted with a.locked extension.

7:05 PM - Ransom Note Found: A ransom note, READ\_IT.txt, is discovered on the desktop, requiring payment to decrypt.

7:10 PM - Isolate Infected System: Infected VM is isolated from the network to avoid ransomware spread.

7:15 PM - Terminate Ransomware Processes: All malicious processes associated with Hidden Tear are stopped through Task Manager and Process Explorer.

7:20 PM - File Containment and Backup: Files with.locked extensions are contained in a folder. Backup versions of the critical files are kept offline.

7:30 PM - Initiate Malware Analysis: A thorough scan is run using Windows Defender and antivirus software to detect any remaining ransomware activity.

7:40 PM - Decryption Attempt: Decryption software applied with a known password to decrypt files. Files are successfully recovered.

8:00 PM - System Restoration: System restored from a clean snapshot, and no further presence of ransomware.

8:10 PM - Post-Incident Review: Incident report and debriefing.

**4. Forensic Evidence**

A. File Analysis

Encrypted Files: Files discovered with the.locked extension in folders like Documents, Pictures, and Desktop.

Ransom Note: A.txt file called READ\_IT.txt was deposited on the Desktop. It read as follows:

Files have been encrypted with Hidden Tear. Pay the ransom for decryption.

B. Malicious Process Analysis

Hidden Tear Executable: The ransomware executable was found in the C:\\Windows\\Desktop\test\ with a name such as hidden\_tear.exe. It was found and stopped using Process Explorer.

C. Network Activity

C2 (Command and Control) Communication: Logs of network traffic were monitored, but because the VM was unplugged from the internet early on, no activity communicating with a C2 server was noted.

D. Event Logs

System Event Logs: Event Viewer log records showed out-of-normal activities and file system changes between 12:00 PM and 12:30 PM.

Antivirus Logs: No notification was triggered by the installed antivirus software throughout the encryption process, which is a weakness in present protection.

**5. Mitigation Strategies**

A. Immediate Mitigation Actions

Network Isolation: The compromised system was isolated to prevent the spread of the ransomware.

Malware Process Termination: The malicious executable (hidden\_tear.exe) was ended.

File Containment: Files bearing the.locked extension were contained for forensic examination.

Decryption: A known password was applied to decrypt the files.

B. Long-Term Mitigation Actions

Offline Backups: Keep backups offline or in separate environments.

Automated Backup Systems: Have automated backups at set intervals.

Install Advanced Endpoint Protection: Employ behavioral and heuristic-based detection.

User Education: Educate users on phishing and safe computing.

Update Incident Response Plan (IRP): Incorporate lessons from simulations.

Conduct Ransomware Drills: Test organizational preparedness.

Network Segmentation: Segregate critical systems.

Patch Management: Keep systems and definitions current.

C. Tools for Future Mitigation

Ransomware Detection Tools

Network Intrusion Detection Systems (IDS)

**6. Conclusion and Recommendations**

The Hidden Tear ransomware attack was successfully replicated and isolated within a controlled VM environment. The incident made it clear that one should have a sound backup mechanism in place, educate users, and have an Incident Response Plan. Next iterations of the simulations will be conducted to make the response procedures more fine-tuned and to put more potent defense mechanisms in place.

**Recommendations:**

Regularly test the backup and restore process.

Educate users on phishing and social engineering.

Utilize behavioral detection software.

Enforce system and data redundancies.

Appendices

A. Attack Log (Sample)

7:00 PM - File encryption initiated - Files in Desktop are encrypted with.locked extension.

7:10 PM - Ransom note dropped - READ\_IT.txt is displayed on Desktop, requiring payment for decryption.

7:15 PM - Malware processes killed - Hidden Tear process (hidden\_tear.exe) killed.

7:30 PM - Files kept isolated and locked -.locked files transferred to a new folder for inspection.

7:45 PM - Successfully decrypted files - Pre-generated password utilized to decrypt files.

B. Tools and Resources Utilized

Windows Defender (Antivirus)

Process Explorer (Malware analysis)

Task Manager (Termination of malicious processes)

Ransomware Decryption Tool (Special tool for this training scenario)

Network Traffic Analyzer (For observing communication with C2 servers)

Members :

**Alonzo, Clint**

**Bahan, Aldrian**

**Daanton, Hubert Nile**

**Dimarucut, James Stanley**

**Ybanez, Remart**