Cybersecurity Incident Response Report – MacRansom & Magniber Decryption Tools Case Study

1. DETAILS :-

Incident Title	MacRansom and Magniber Ransomware Case Simulation
Date/Time Reported	July 23, 2025 – 17:53
Analyst Name	Mishthi Chavan
Status	Closed
Project Tool	MacRansom Decryption Utility & Magniber Decryptor

2. SUMMARY OF INCIDENT :-

As part of a cybersecurity internship training activity conducted on July 20, 2025, a simulated ransomware attack involving MacRansom and Magniber ransomware strains was executed within a controlled lab environment. Specific sample files were intentionally encrypted using malware payloads associated with these ransomware variants. The encrypted files displayed characteristic extensions and ransom notes.

The primary objective was to understand the infection behavior and then utilize available decryption tools to restore the files. For MacRansom, a publicly available decryption utility was applied, while a custom script-based decryptor was used for Magniber.

This report outlines the steps taken, analysis performed, forensic findings, and final remediation activities as part of this case simulation.

3. INVESTIGATION DETAILS :-

1. Who discovered/reported the incident?
-> Intern Mishthi Chavan during a cybersecurity lab exercise.

2. What alert triggered the response?
->Endpoint security alert showed suspicious file behavior.

3. What were the first actions taken?
->Disconnected the virtual machine, initiated a malware scan, and began isolating encrypted files.

4. What systems/hosts were affected?
->Localhost Virtual Machine (Hostname: MACLAB01, User: analyst101).

5. Has this issue occurred before?
->No. It was a planned exercise.

6. Were business processes/data at risk?
->No. Only dummy files were affected.

7. What logs generated alerts?
->MacOS security logs, malware sandbox output, Windows Event Viewer.

8. Any unauthorized account activity or privilege escalation?
->No unusual privilege escalation was observed.

9. Any unusual network connections?
->Yes. MacRansom attempted an outbound connection to an unknown IP (obfuscated for safety).

10. Did anyone open suspicious files/links/emails?
->Yes. Two test executables macinvoice.pkg and win_update.exe were launched.

11. What remediation steps were taken?
->Used MacRansom decryptor for MacOS samples, and script-based decryptor for Magniber files. Malware payloads were deleted.

12. Other notable actions?
->Hashes of encrypted and decrypted files were logged, screenshots of decryption success were captured.

4. TOOLS & ANALYSIS PROCESS :-

Tools Used:

- MacRansom Decryption Utility (open-source, community-supported)
- Magniber Decryptor Script (Python-based recovery for older Magniber variants)

Affected Files:

- intern_docs.docx.encrypted
- project_data.xlsx.magniber

File Hashes (pre-decryption):

- mac file: a9f2d1c438f89a1f15c8bc11f239d1a7
- windows file: b3c6c2f412fa8a91e45c9df839c2e2aa

Decryption Outcome:

Both files were successfully restored to their original formats:

- intern_docs.docx
- project_data.xlsx

5. LOG & FORENSIC ANALYSIS :-

AREA	TOOL USED	FINDINGS
Network Traffic	Wireshark	Detected suspicious POST to encrypted IP
File Behavior	Process Monitor	File encryption observed during runtime
Registry	Regedit (for Windows VM)	Registry persistence entries under Run key
Sandbox	Any.Run	Ransom behavior and file modification verified
VirusTotal	Online Scan	macinvoice.pkg flagged by 51/65 vendors

6. REMEDIATION & OUTCOME :-

- MacRansom: Decrypted using the designated utility.

- Magniber: Recovered using an offline decryptor tailored for known key leaks.

- Residual malware files were quarantined and removed.

- Network traffic logs were saved and reviewed.

- Integrity checks were performed on restored files.

- Virtual environment was cleaned and reset.

- A final report was compiled and submitted to the internship supervisor.