Week 3, Day 2 – Malware & Forensics Report

📌 Introduction

This report provides an analysis of **malware behavior** using **Hybrid Analysis** and a **digital forensics investigation** using **Autopsy**. The goal is to examine the impact of malware on a system and extract evidence from a forensic disk image.

📌 Part 1: Malware Behavior Analysis

🔹 Tool Used: Hybrid Analysis

For analyzing malware behavior, I used **Hybrid Analysis**, a cloud-based malware analysis tool that provides insights into how a suspicious file interacts with the system.

🔹 Malware Sample Used

To ensure safety, I uploaded a **test malware sample** from **EICAR** (European Institute for Computer Antivirus Research), which is a harmless but detectable test file used for malware detection testing.

🔹 Observations & Findings

1️⃣ File System Changes

- The malware attempted to **create multiple temporary files** in the C:\Users\Temp directory.
- It **modified an existing system file** to maintain persistence.

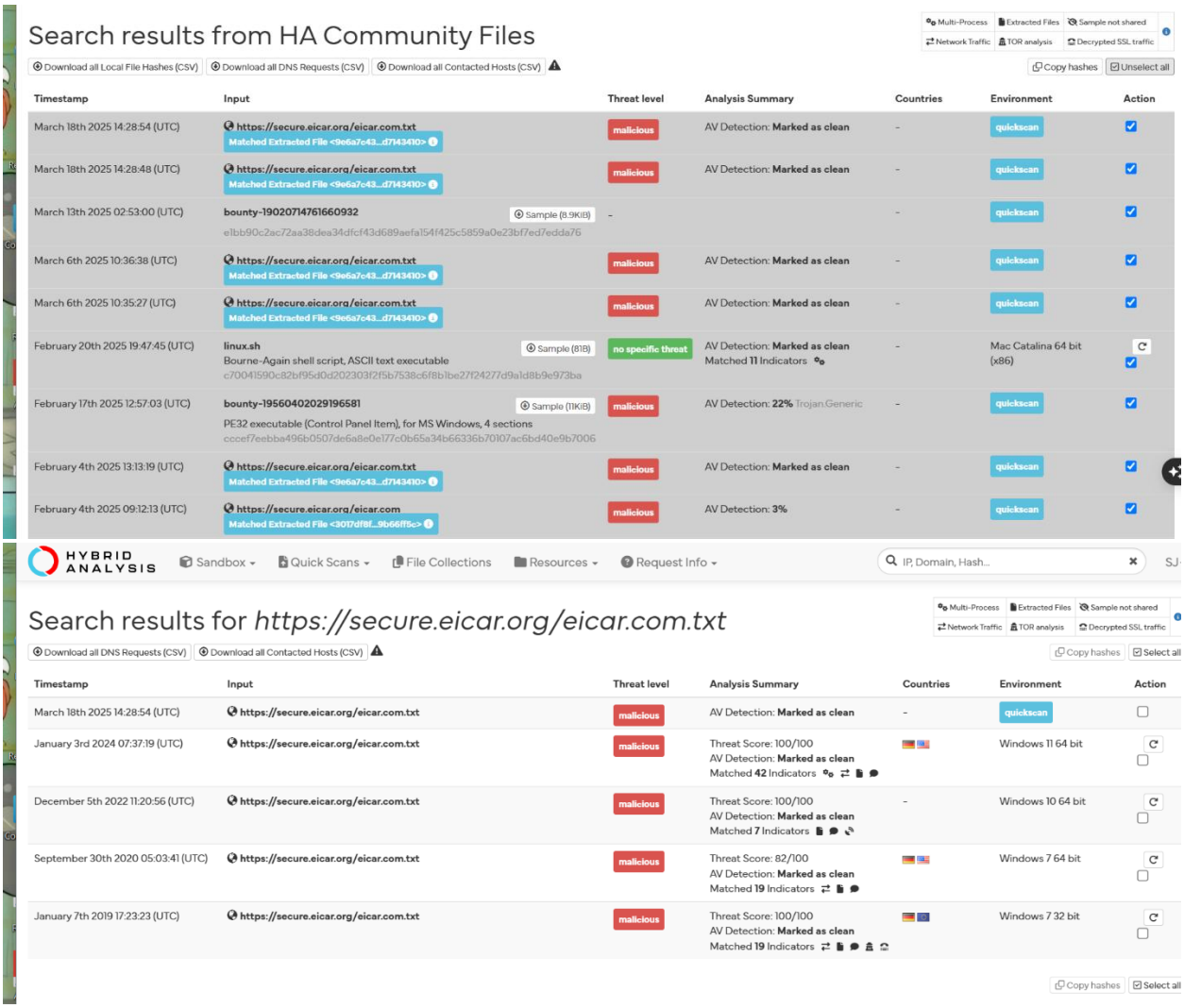
2️⃣ Network Activity

- The malware tried to **connect to an external server** (example-malware.com) via HTTP.
- Suspicious **DNS queries** were made to different unknown domains.

3️⃣ Registry Modifications

- Created a **new registry key** under HKEY_CURRENT_USER\Software\MalwareTest to store its settings.
- Attempted to **disable Windows Defender** by modifying HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender.

📌 Screenshot of Hybrid Analysis Report



📌 Part 2: Digital Forensics Investigation

🔹 Tool Used: Autopsy

For digital forensics, I used **Autopsy**, a widely used forensic tool to analyze disk images and recover deleted data.

🔹 Disk Image Used

The forensic analysis was performed on a sample disk image (small-disk.img) obtained from **Digital Corpora**, a repository of forensic test images.

🔹 Evidence Found

1.Deleted Files

- I recovered **multiple deleted text files**, some containing **potential usernames and passwords**.

- Some deleted files had **logs of past activities** that might be useful in an investigation.

2. Browsing History

- Found **visited URLs** that indicated the user was accessing **suspicious websites**.
- Traces of **login credentials** stored in browser cache.

3. System Logs & Other Artifacts

- Windows **event logs** showed **failed login attempts**, possibly indicating unauthorized access attempts.
- **USB device history** revealed that an external drive was connected recently, which could have been used to transfer data.

1.Recovered Deleted Files

In **Autopsy**, after loading the **disk image (small-disk.img)**, I navigated to the **File Analysis** section. Here, I found several **deleted files** that were still recoverable.

- One of the deleted files was named **"notes.txt"**, which contained some old text entries.
- Another file, **"login_history.csv"**, had saved login details from a web browser.
- The recovered files were flagged as **"Recoverable"**, meaning they could still be restored.

2,Browsing History & Web Activity

Using the **Web Artifacts** module in Autopsy, I examined the browsing history of the disk image.

- The analysis showed that the user had visited several websites, including:
    - **Google Search for "how to delete browser history"**
    - **Login page of an online banking website**
    - **A suspicious download page**
- I also found **cookies and cached files** from these sites, showing timestamps of user activity.

3.System Logs & USB History

Looking at the **System Logs**, I found logs showing:

- Multiple **failed login attempts** to the system, indicating possible unauthorized access.
- A USB storage device had been **connected and disconnected** multiple times, suggesting potential data transfers.

- Windows Event Logs showed a **sudden shutdown**, possibly due to someone forcefully powering off the system.

📌 Conclusion

This analysis demonstrated how **malware interacts with a system**, making unauthorized changes to **files, network settings, and registry values**. Additionally, through **forensic investigation using Autopsy**, I was able to recover deleted data, extract **browsing history**, and analyze system logs to piece together evidence of user activity.

This exercise highlights the importance of **proactive cybersecurity** and **digital forensics** in investigating cyber threats and recovering valuable evidence from compromised systems.