

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

☒ 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.

☒ 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.

☒ 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

Search results from HA Community Files

 Multi-Process
 Extracted Files
 Sample not shared
 Network Traffic
 TOR analysis
 Decrypted SSL traffic

Download all Local File Hashes (CSV)
 Download all DNS Requests (CSV)
 Download all Contacted Hosts (CSV)

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
March 18th 2025 14:28:54 (UTC)	https://secure.eicar.org/eicar.com.txt Matched Extracted File <9e6a7e43..d7143410>	malicious	AV Detection: Marked as clean	-	quickscan	<input checked="" type="checkbox"/>
March 18th 2025 14:28:48 (UTC)	https://secure.eicar.org/eicar.com.txt Matched Extracted File <9e6a7e43..d7143410>	malicious	AV Detection: Marked as clean	-	quickscan	<input checked="" type="checkbox"/>
March 13th 2025 02:53:00 (UTC)	bounty-19020714761660932 e1bb90c2ac72aa38de34dcf43d689ae0154f425c5859a0e23bf7ed7edda76	<input type="checkbox"/> Sample (8.9KB)	-	-	quickscan	<input checked="" type="checkbox"/>
March 6th 2025 10:36:38 (UTC)	https://secure.eicar.org/eicar.com.txt Matched Extracted File <9e6a7e43..d7143410>	malicious	AV Detection: Marked as clean	-	quickscan	<input checked="" type="checkbox"/>
March 6th 2025 10:35:27 (UTC)	https://secure.eicar.org/eicar.com.txt Matched Extracted File <9e6a7e43..d7143410>	malicious	AV Detection: Marked as clean	-	quickscan	<input checked="" type="checkbox"/>
February 20th 2025 19:47:45 (UTC)	linux.sh Bourne-Again shell script, ASCII text executable c7004590:c82b95cd0d2023032ff5b7538c6f8b1be27f24277d9a1d8b9e973b	<input type="checkbox"/> Sample (81B)	no specific threat	AV Detection: Marked as clean Matched 11 Indicators	Mac Catalina 64 bit (x86)	<input checked="" type="checkbox"/>
February 17th 2025 12:57:03 (UTC)	bounty-19560402029196581 PE32 executable (Control Panel Item), for MS Windows, 4 sections cc0cf7eeba496b050/0de6a8e0e177c0b65a34b66336b70107ac6bd40e9b7006	<input type="checkbox"/> Sample (11KIB)	malicious	AV Detection: 22% Trojan.Generic	quickscan	<input checked="" type="checkbox"/>
February 4th 2025 13:13:19 (UTC)	https://secure.eicar.org/eicar.com.txt Matched Extracted File <9e6a7e43..d7143410>	malicious	AV Detection: Marked as clean	-	quickscan	<input checked="" type="checkbox"/>
February 4th 2025 09:12:13 (UTC)	https://secure.eicar.org/eicar.com.txt Matched Extracted File <0107df8f_9b66f85c>	malicious	AV Detection: 3%	-	quickscan	<input checked="" type="checkbox"/>

Hybrid Analysis
 Sandbox
 Quick Scans
 File Collections
 Resources
 Request Info

IP, Domain, Hash...
SJ...

Search results for https://secure.eicar.org/eicar.com.txt

 Multi-Process
 Extracted Files
 Sample not shared
 Network Traffic
 TOR analysis
 Decrypted SSL traffic

Download all DNS Requests (CSV)
 Download all Contacted Hosts (CSV)

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
March 18th 2025 14:28:54 (UTC)	https://secure.eicar.org/eicar.com.txt	malicious	AV Detection: Marked as clean	-	quickscan	<input type="checkbox"/>
January 3rd 2024 07:37:19 (UTC)	https://secure.eicar.org/eicar.com.txt	malicious	Threat Score: 100/100 AV Detection: Marked as clean Matched 42 Indicators	DE	Windows 11 64 bit	<input checked="" type="checkbox"/>
December 5th 2022 11:20:56 (UTC)	https://secure.eicar.org/eicar.com.txt	malicious	Threat Score: 100/100 AV Detection: Marked as clean Matched 7 Indicators	-	Windows 10 64 bit	<input checked="" type="checkbox"/>
September 30th 2020 05:03:41 (UTC)	https://secure.eicar.org/eicar.com.txt	malicious	Threat Score: 82/100 AV Detection: Marked as clean Matched 19 Indicators	DE	Windows 7 64 bit	<input checked="" type="checkbox"/>
January 7th 2019 17:23:23 (UTC)	https://secure.eicar.org/eicar.com.txt	malicious	Threat Score: 100/100 AV Detection: Marked as clean Matched 19 Indicators	DE	Windows 7 32 bit	<input checked="" type="checkbox"/>

Copy hashes
 Select all

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.