INTERNSHIP REPORT

Malware Analysis and Threat Understanding

---

1. Task Title

Study and Analysis of Malware Types and Detection Techniques

---

2. Objective

The objective of this task was to understand different types of malware, analyze their behavior using threat intelligence platforms, and study malware lifecycle, propagation methods, and prevention techniques. This task aimed to build awareness of how malware operates and how cybersecurity tools detect and mitigate threats.

---

3. Introduction

Malware (Malicious Software) is one of the most common cyber threats affecting individuals and organizations. Malware is designed to damage systems, steal sensitive data, or disrupt normal operations. Understanding malware types, behavior patterns, and detection mechanisms is essential for cybersecurity professionals. This task focused on studying malware safely using known malware hashes and online analysis tools without executing malicious code.

---

4. Types of Malware Studied

4.1 Virus

A virus is a type of malware that attaches itself to legitimate files or programs. It spreads when the infected file is executed and can damage or modify system data.

4.2 Worm

A worm is a self-replicating malware that spreads automatically across networks without user interaction. Worms consume system and network resources and can cause large-scale damage.

4.3 Trojan Horse

A trojan disguises itself as legitimate software to trick users into installing it. Once executed, it can create backdoors, steal data, or download additional malware.

4.4 Ransomware

Ransomware encrypts user files and demands payment to restore access. It is one of the most dangerous malware types, often causing financial and operational losses.

---

5. Malware Sample Analysis Using VirusTotal

Instead of uploading live malware files, **known malware hash values** were submitted to VirusTotal for analysis.

Process Followed:

- Collected known malware hash values (MD5/SHA-256)
- Uploaded hashes to VirusTotal
- Reviewed detection results from multiple antivirus engines

---

6. Detection Report Analysis

VirusTotal provides a consolidated detection report from various security vendors.

Key Observations:

- Malware samples were detected by multiple antivirus engines
- Detection names varied across vendors
- Reputation scores indicated malicious behavior
- Some engines labeled samples as trojan, ransomware, or generic malware

This highlighted the importance of using multiple detection engines for accurate threat identification.

---

7. Behavior Indicators Observed

Based on VirusTotal reports and threat descriptions, common malware behavior indicators included:

- File system modifications
- Registry changes
- Suspicious network communication
- Creation of unauthorized processes
- Attempts to disable security features

These indicators help security analysts identify infected systems.

---

8. Malware Lifecycle

The typical malware lifecycle consists of the following stages:

1. **Creation** – Malware is developed by attackers
2. **Distribution** – Delivered through phishing, downloads, or exploits
3. **Execution** – Malware runs on the victim system
4. **Persistence** – Maintains access by modifying system settings
5. **Command and Control** – Communicates with attacker servers
6. **Action on Objectives** – Data theft, encryption, or system damage

---

9. Malware Propagation Methods

Malware commonly spreads through:

- Phishing emails and malicious attachments
- Infected software downloads
- USB drives and removable media
- Network vulnerabilities
- Exploit kits and compromised websites

---

10. Prevention and Mitigation Methods

Effective malware prevention techniques include:

- Using updated antivirus and endpoint protection software
- Regular system and software updates
- Avoiding suspicious links and email attachments
- Using firewalls and intrusion detection systems
- Enabling email and web filtering
- Maintaining regular data backups

---

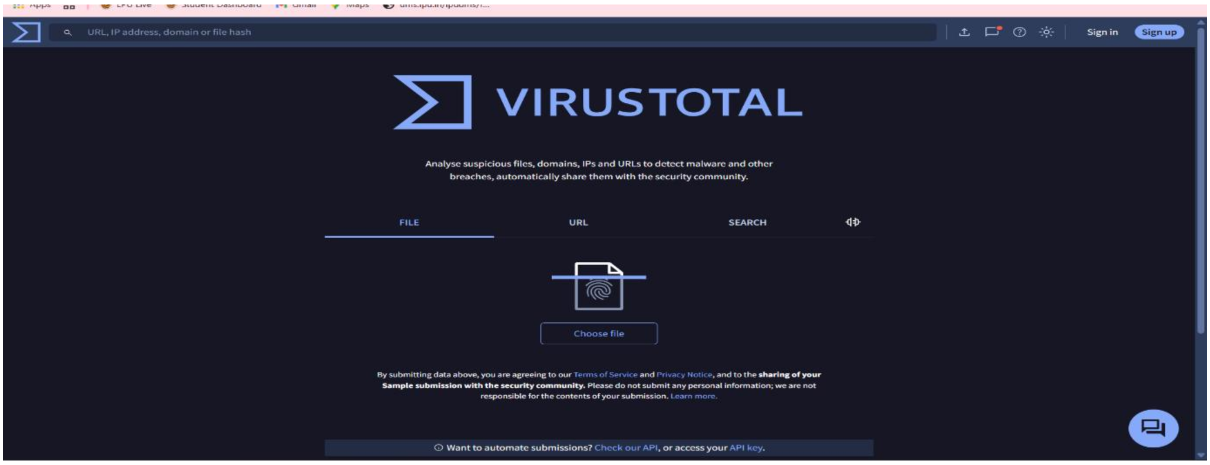
11. Outcome and Learning Experience

This task improved understanding of malware behavior, detection mechanisms, and analysis techniques. Learning to analyze malware safely using hashes and online tools provided valuable exposure to real-world cybersecurity practices without risking system security.

---

12. Conclusion

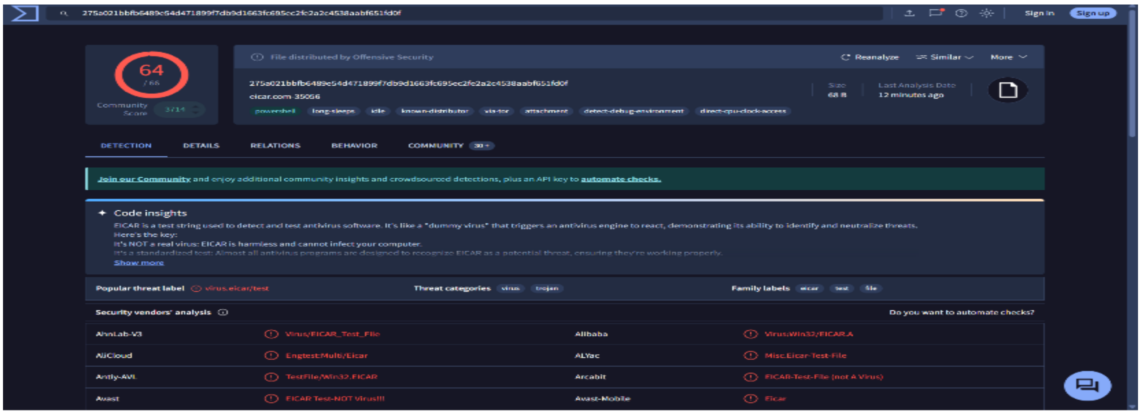
The malware analysis task provided comprehensive knowledge of malware types, detection methods, and prevention strategies. Understanding how malware spreads and operates is critical for defending systems against cyber threats. This task strengthened foundational skills required for further study in cybersecurity and threat analysis.



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

Want to automate submissions? Check our API, or access your API key.



File distributed by Offensive Security

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
eicar.com-35056

Size: 68 B
Last Analysis Date: 12 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

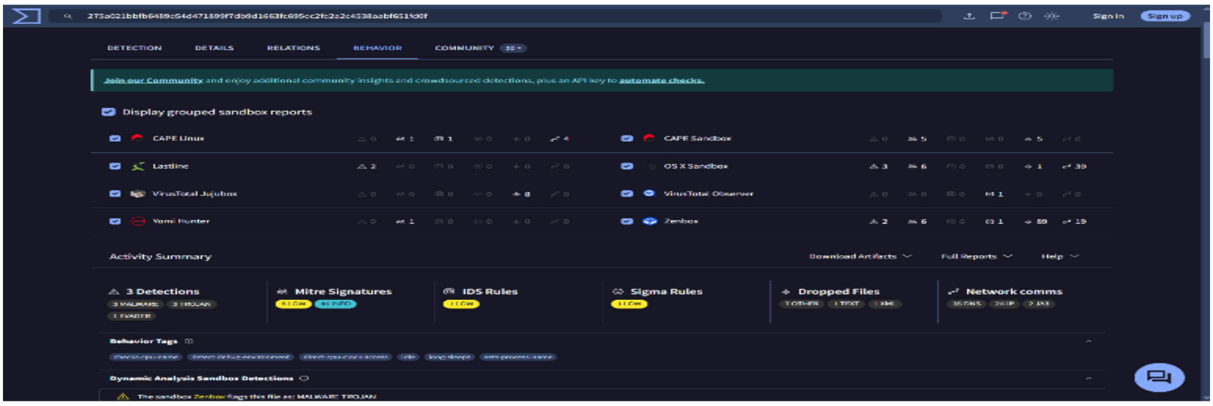
Code insights

EICAR is a test string used to detect and test antivirus software. It's like a "dummy virus" that triggers an antivirus engine to react, demonstrating its ability to identify and neutralize threats.
Here's the key:
It's NOT a real virus: EICAR is harmless and cannot infect your computer.
It's a standardized test: Almost all antivirus programs are designed to recognize EICAR as a potential threat, ensuring they're working properly.

Popular threat label: virus.eicar/test
Threat categories: virus, trojan
Family labels: eicar, test, file

Security vendors' analysis — Do you want to automate checks?

AhnLab-V3	Virus/EICAR_Test_File	Alibaba	Virus:Win32/EICAR.A
AliCloud	Engtest:Multi/Eicar	ALYac	Misc.Eicar-Test-File
Antiy-AVL	TestFile/Win32.EICAR	Arcabit	EICAR-Test-File (not A Virus)
Avast	EICAR Test-NOT virus!!!	Avast-Mobile	Eicar



275a021bbfb6489c54d471899f7db9d1663fc695cc2fc2a2c4538aabf651fd0f

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

☑ Display grouped sandbox reports

☑ CAPE Linux	0	1	1	0	0	4	☑ CAPE Sandbox	0	5	0	0	5	0
☑ Lastline	2	0	0	0	0	0	☑ OS X Sandbox	3	6	0	0	1	39
☑ VirusTotal Jujubox	0	0	0	0	8	0	☑ VirusTotal Observer	0	0	0	1	0	0
☑ Yomi Hunter	0	1	0	0	0	0	☑ Zenbox	2	6	0	1	89	19

Activity Summary

3 Detections
3 MALWARE 3 TROJAN 1 EVADER

Mitre Signatures
6 LOW 46 INFO

IDS Rules
1 LOW

Sigma Rules
1 LOW

Dropped Files
7 OTHER 1 TEXT 1 XML

Network comms
35 DNS 26 IP 2 JA3

Behavior Tags

check-cpu-name detect-debug-environment direct-cpu-clock-access idle long-sleeps sets-process-name

Dynamic Analysis Sandbox Detections

The sandbox Zenbox flags this file as: MALWARE TROJAN