Malware Analysis Using VirusTotal

Malware Classification Report

---

1. Introduction

This report presents a structured malware analysis conducted using **VirusTotal**, focusing on hash-based investigation, detection analysis, and behavioral indicators. The objective of this project is to demonstrate practical SOC (Security Operations Center) skills in identifying **malicious, benign, and test samples**, validating detections, and distinguishing real threats from false positives.

A total of **four samples** were analyzed, covering:

- Undetected / low-confidence sample
- Antivirus test sample (EICAR)
- Confirmed ransomware sample
- Benign / false positive validation

---

2. Tools and Methodology

- **Platform Used:** VirusTotal
- **Analysis Type:** Hash-based static and behavioral analysis
- **Approach:**
    - Hash submission to VirusTotal
    - Review of antivirus detections
    - Examination of YARA, Sigma, and sandbox behavior
    - Final classification based on evidence

No malware samples were downloaded or executed locally, ensuring safe and ethical analysis practices.

3. Sample Overview

Sample	Classification	Purpose
Sample 1	Suspicious / Undetected	Demonstrates low-confidence verdicts
Sample 2	Test Malware (EICAR)	Antivirus detection validation
Sample 3	Ransomware (WannaCry)	Real-world high-severity malware
Sample 4	Benign / False Positive	Noise reduction and validation

---

4. Detailed Analysis

Sample 1: Suspicious / Undetected File

Detection Result:

- No security vendors flagged the file as malicious

Observations:

- Absence of antivirus detections
- No behavioral or sandbox indicators
- No community comments or threat attribution

Assessment:
This sample represents files commonly encountered in SOC environments that appear suspicious but lack sufficient evidence for malicious classification.

Final Verdict:

Undetected / Low-Confidence – Requires contextual investigation

Sample 2: Antivirus Test Sample (EICAR)

Detection Result:

- Detected by the majority of antivirus engines

Observations:

- Identified as EICAR test string
- No malicious behavior or real payload
- Widely used for testing antivirus effectiveness

Assessment:
EICAR is not real malware and cannot harm systems. Its detection confirms correct antivirus functionality.

Final Verdict:

Test Malware – Non-malicious by design

Sample 3: Ransomware (WannaCry)

Detection Result:

- 67/71 security vendors flagged the file as malicious

Malware Classification:

- Type: Ransomware
- Family: WannaCry

Key Behavioral Indicators:

- Encryption-related activity
- Registry-based persistence mechanisms
- Dropped malicious artifacts
- Network communication attempts
- Evasion techniques (debug checks, long sleeps)

YARA and Sigma Rules:

- WannaCry ransomware signatures matched
- Multiple critical and high-severity Sigma rules triggered

MITRE ATT&CK Mapping:

- Execution
- Persistence
- Defense Evasion
- Command and Control
- Impact (Data Encryption)

Final Verdict:

Confirmed Ransomware – High Severity Threat

Sample 4: Benign / False Positive Case

Detection Result:

- 0/59 security vendors flagged the file as malicious

Observations:

- Extremely small file size
- No malicious logic or indicators
- No behavioral or network activity

Assessment:
This sample demonstrates correct false-positive handling, highlighting the importance of validating alerts before escalation.

Final Verdict:

Benign – False Positive Confirmed

---

5. Comparative Summary

Attribute	Sample 1	Sample 2	Sample 3	Sample 4
AV Detection	No	Yes	Yes	No
Behavior Observed	No	No	Yes	No
Malware Type	Unknown	Test	Ransomware	Benign
Severity	Low	None	Critical	None

6. Key Learnings

- Not all detections indicate real threats
- Antivirus consensus alone is insufficient without behavior analysis
- False-positive identification is a critical SOC skill
- Ransomware exhibits clear behavioral and signature-based indicators

---

7. Conclusion

This project demonstrates a complete malware triage workflow used in real-world SOC operations. By analyzing multiple sample types, the project highlights the importance of evidence-based classification, threat validation, and analytical judgment. These skills are essential for effective incident response and security monitoring roles.

Prepared by: Parijat Das
Role Target: SOC Analyst / Cybersecurity Intern
Platform: VirusTotal