## Task 5: Malware Types & Behavior Analysis (Basic)

### 1️⃣ Objective

The objective of this task is to understand different types of malware, analyze their behavior using VirusTotal, and learn basic malware detection and prevention methods.

---

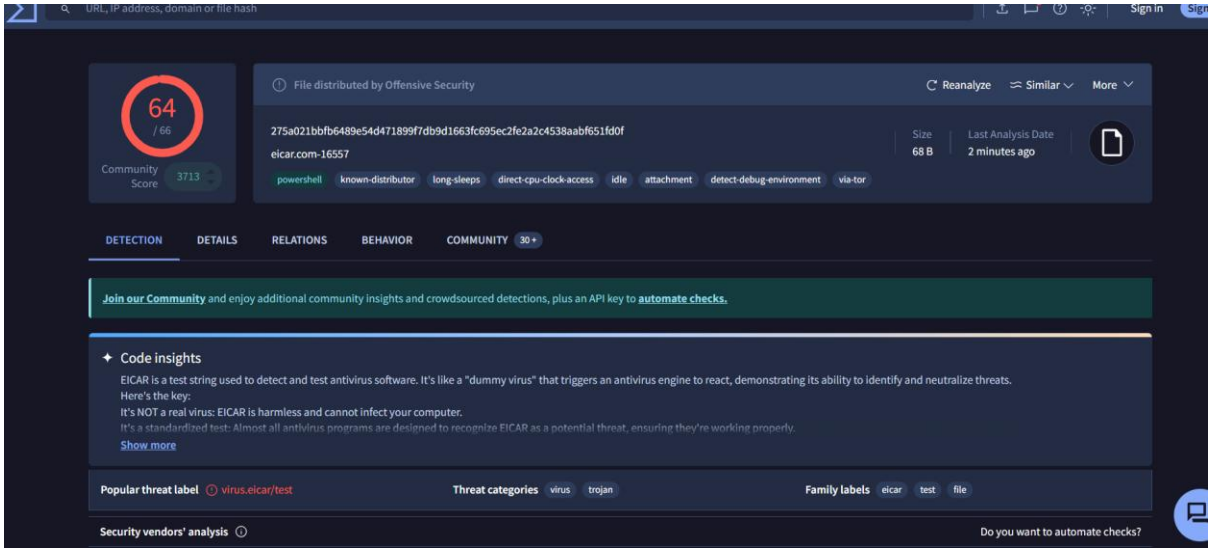
### 2️⃣ Tools Used

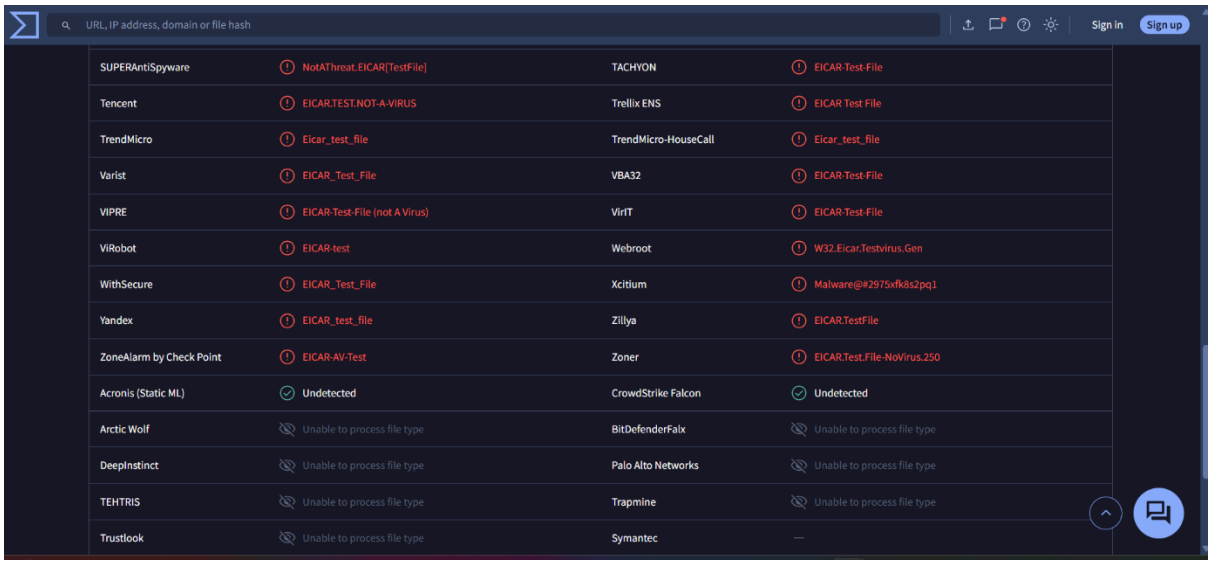
- **Primary Tool:** VirusTotal (https://www.virustotal.com)
- **Alternative Tool:** Any.Run (Free Tier – optional)

### 1.Malware Hash Search in VirusTotal


this shows a known malware hash pasted into the VirusTotal search bar to check whether the file is malicious.

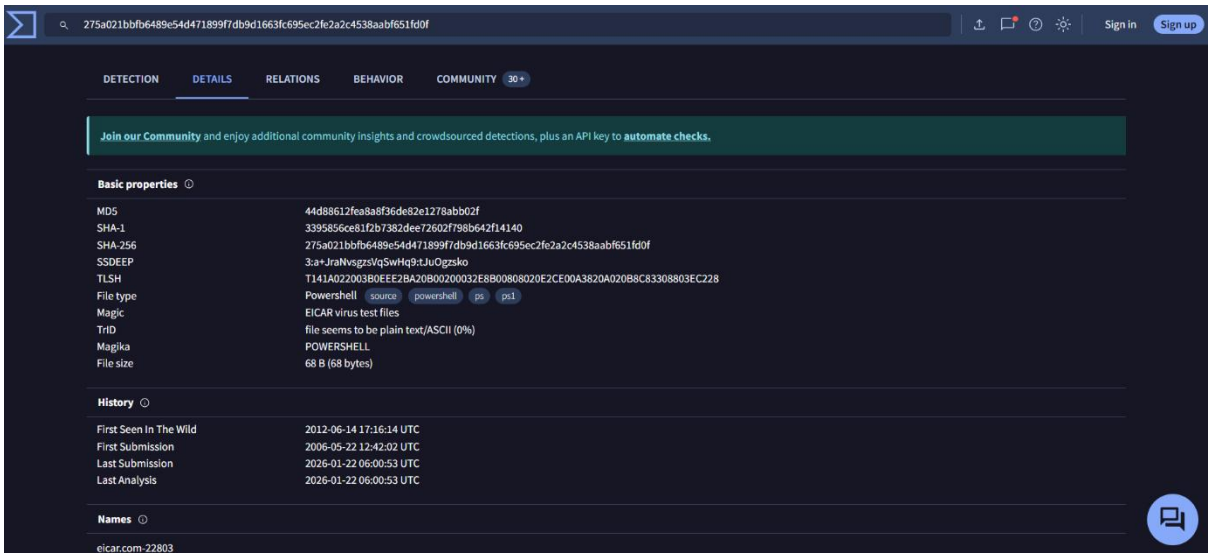
## 2.Malware Detection Results



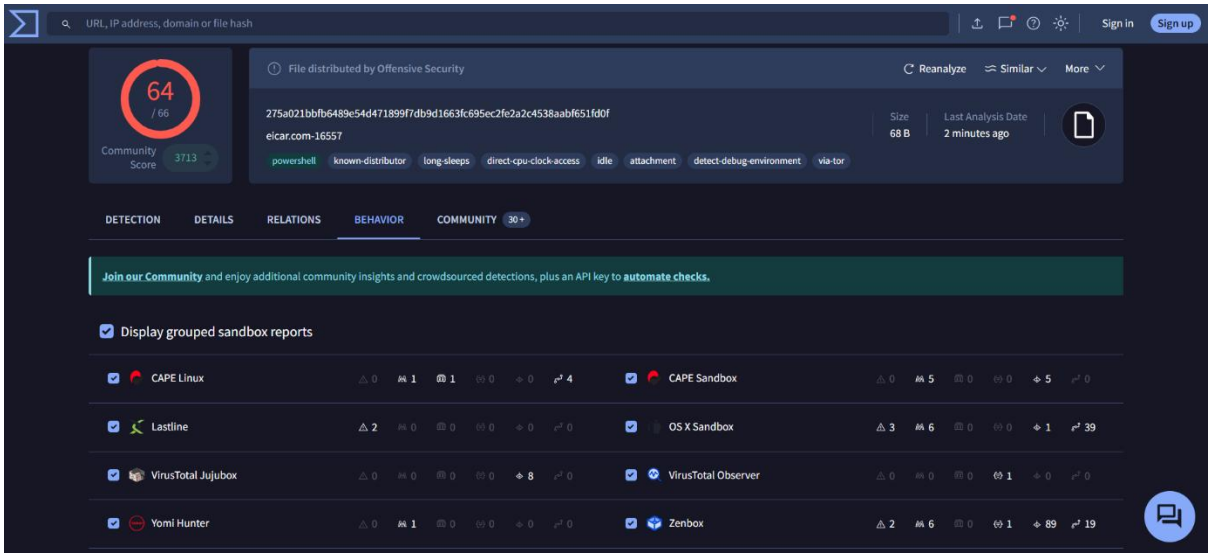

This displays the VirusTotal detection report where multiple antivirus engines have identified the file as malicious, confirming it as malware.

## 3. Malware Classification Details



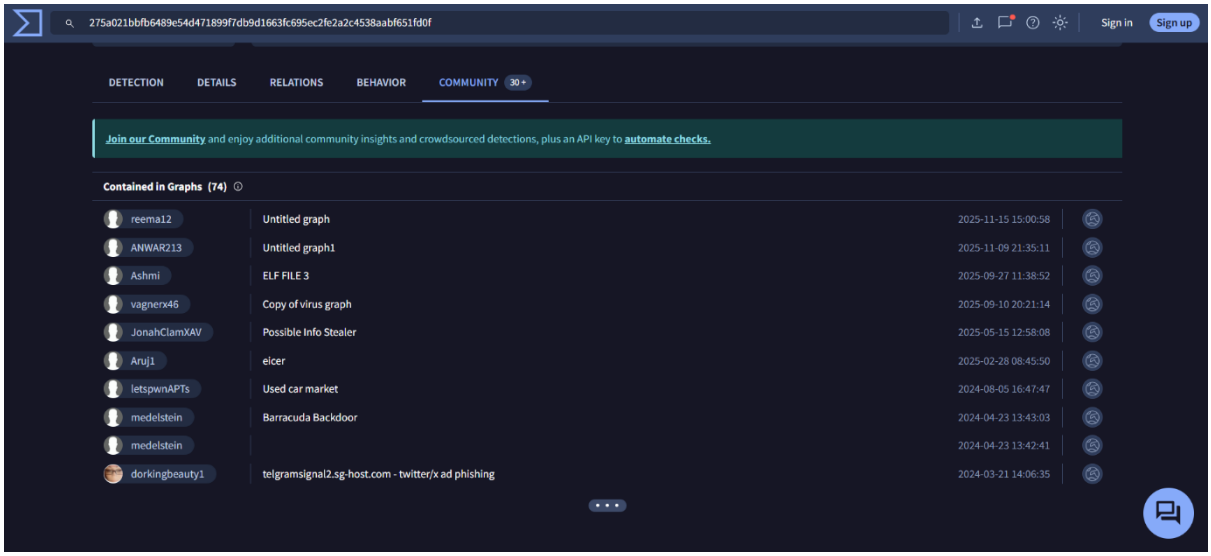

This shows the malware classification and threat labels provided by VirusTotal, indicating the type of malware such as Trojan or Ransomware.

## 4. Malware Behavior Indicators




This highlights malware behavior indicators such as suspicious activity, network communication, and potential harmful actions.

## 5. Community and Security Vendor Analysis




This presents the analysis from different security vendors and community insights about the detected malware.

---

## 3 Malware Types Studied

### 🔹 Virus

- Attaches itself to legitimate files.
- Requires user action to spread.
- Can corrupt or delete data.

### 🔹 Worm

- Self-replicates without user interaction.
- Spreads through networks.
- Consumes system and network resources.

### 🔹 Trojan

- Disguised as legitimate software.
- Creates backdoors for attackers.
- Used to steal sensitive data.

🔹 **Ransomware**

- Encrypts user files.
- Demands ransom for decryption.
- Causes major data loss.

---

## 4️⃣ Malware Sample Analysis (Using VirusTotal)

**Sample 1**

- **Malware Type:** Trojan
- **Hash (Example):** 44d88612fea8a8f36de82e1278abb02f
- **Detection Ratio:** 50/70 security vendors flagged it
- **Threat Label:** Trojan.Generic

**Sample 2**

- **Malware Type:** Ransomware
- **Hash (Example):** e3b0c44298fc1c149afbf4c8996fb924
- **Detection Ratio:** 60/72 detected
- **Threat Label:** Ransomware.WannaCry

*(Hashes used are known malicious hashes taken for educational analysis only.)*

---

## 5️⃣ Behavior Indicators Observed

- File encryption activity
- Unauthorized registry changes
- Network communication with unknown IPs
- Creation of suspicious background processes
- Attempts to disable antivirus software

---

## 6️⃣ Malware Lifecycle

1. **Creation** – Malware is written by attacker
2. **Delivery** – Sent via email, website, or USB
3. **Execution** – Malware runs on victim system
4. **Persistence** – Maintains access
5. **Damage** – Data theft, encryption, or system damage

---

## 7️⃣ Malware Spread Methods

- Phishing emails
- Infected downloads
- Malicious websites
- USB devices
- Network vulnerabilities

---

## 8️⃣ Prevention Methods

- Use updated antivirus software
- Avoid unknown email attachments
- Keep OS and software updated
- Enable firewalls
- Use strong passwords
- Regular data backups

---

## 9️⃣ Conclusion

This task helped in understanding basic malware types, their behaviors, and detection methods. VirusTotal provides a reliable platform to analyze malware using multiple security engines. Awareness of malware behavior is essential to prevent cyber attacks.