

Task 5: Malware Types & Behavior Analysis (Basic)

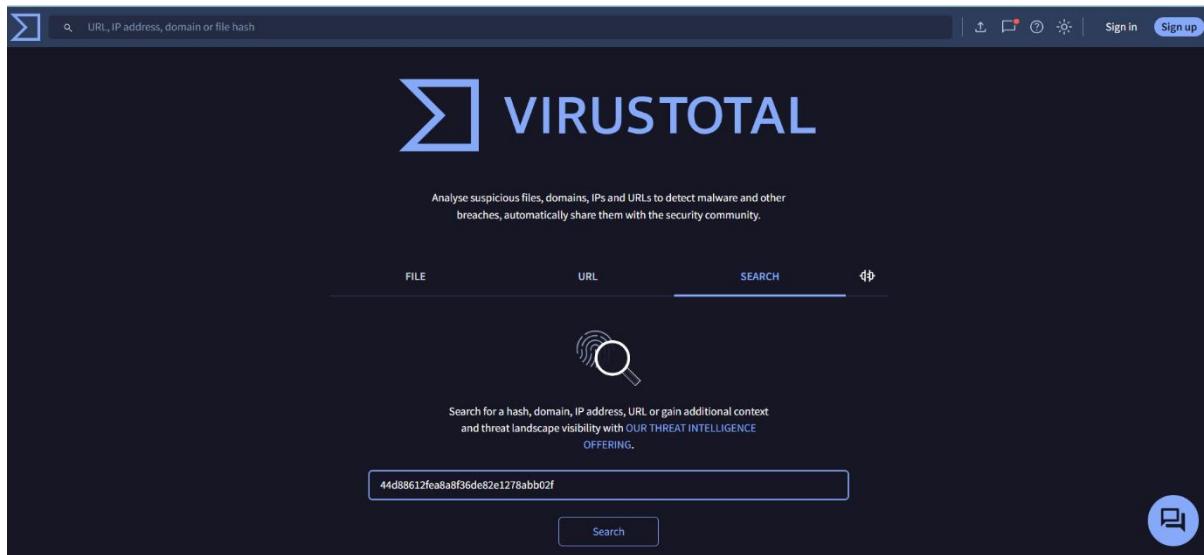
1 Objective

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.

2 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

The screenshot shows the VirusTotal analysis interface. At the top, there's a search bar with the placeholder "URL, IP address, domain or file hash". Below the search bar is a summary card with a large red circle containing the number "64 / 66" and the text "File distributed by Offensive Security". To the right of the card are buttons for "Reanalyze", "Similar", and "More". Further right are links for "Sign in" and "Sign up".

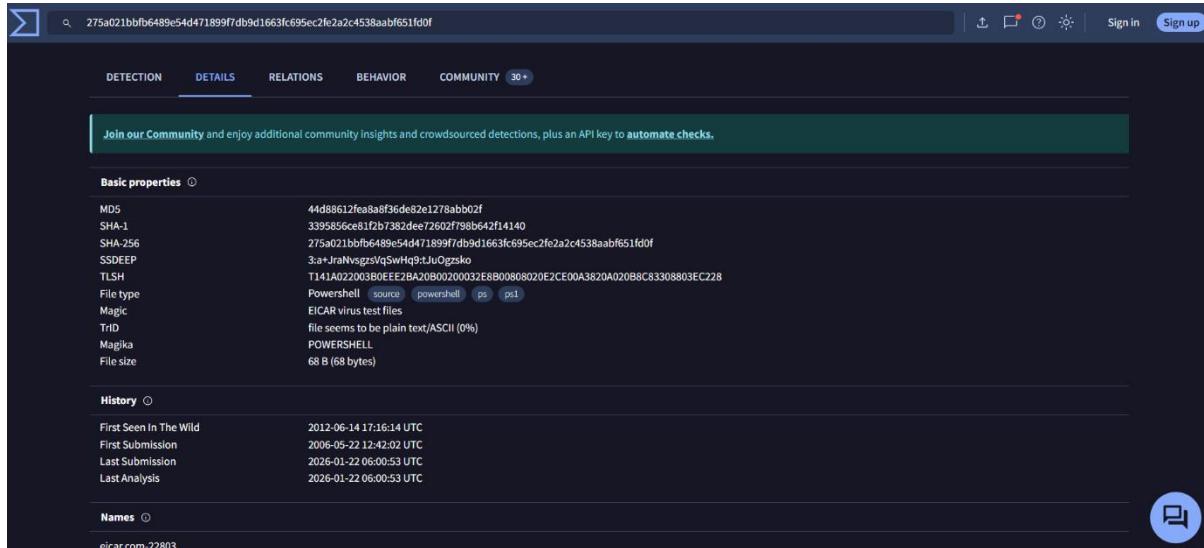
The main content area displays a file analysis result for the hash `275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f`, which is identified as `eicar.com-16557`. The file size is 68 B and was last analyzed 2 minutes ago. Below the file details are several tags: powershell, known-distributor, long-sleeps, direct-cpu-clock-access, idle, attachment, detect-debug-environment, and via-tor.

Below the file details, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with 30+ items). A green banner at the bottom of the main content area encourages users to "Join our Community" and provides an API key for "automate checks".

The bottom section of the interface shows a table of security vendor analysis results. The columns include the vendor name, detection status, and a link to the vendor's report. The table lists 16 vendors, all of whom detected the file as malicious (indicated by a red circle icon). The vendors listed are: SUPERAntiSpyware, NotAThreat.EICAR[TestFile], TACHYON, EICAR-Test-File; Tencent, EICAR.TEST.NOT-A-VIRUS, Trellix ENS, EICAR Test File; TrendMicro, Eicar_test_file, TrendMicro-HouseCall, Eicar_test_file; Varist, EICAR_Test_File, VBA32, EICAR-Test-File; VIPRE, EICAR-Test-File (not a Virus), ViriT, EICAR-Test-File; ViRobot, EICAR-test, Webroot, W32.Eicar.Testvirus.Gen; WithSecure, EICAR_Test_File, Xcitium, Malware@#2975xfk8s2pq1; Yandex, EICAR_test_file, Zillya, EICAR.TestFile; ZoneAlarm by Check Point, EICAR-AV-Test, Zoner, EICAR.Test.File-NoVirus.250; Acronis (Static ML), Undetected, CrowdStrike Falcon, Undetected; Arctic Wolf, Unable to process file type, BitDefenderFalk, Unable to process file type; DeepInstinct, Unable to process file type, Palo Alto Networks, Unable to process file type; TEHTRIS, Unable to process file type, Trapmine, Unable to process file type; Trustlook, Unable to process file type, Symantec, —.

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

3. Malware Classification Details

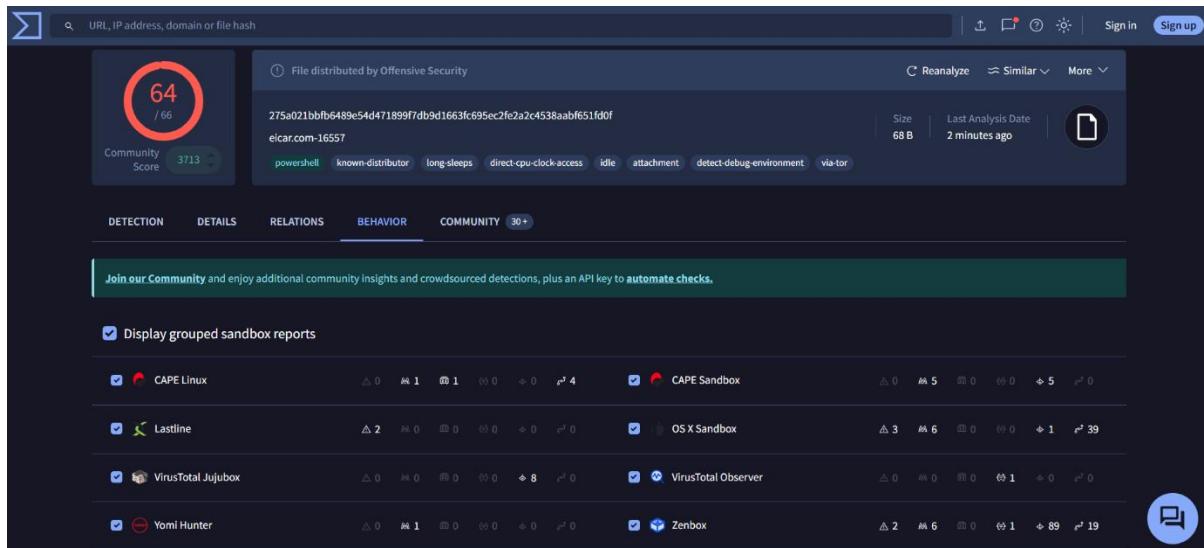


This screenshot shows the 'Details' tab of a VirusTotal analysis page for a specific file hash. The page displays various metadata and threat intelligence. Key sections include:

- Basic properties:** Includes MD5, SHA-1, SHA-256, SSDeep, TLSH, File type (Powershell), Magic, TrID, Magika, and File size (68 B).
- History:** Shows First Seen In The Wild (2012-06-14 17:16:14 UTC), First Submission (2006-05-22 12:42:02 UTC), Last Submission (2026-01-22 06:00:53 UTC), and Last Analysis (2026-01-22 06:00:53 UTC).
- Names:** Lists the domain eicar.com-22803.

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



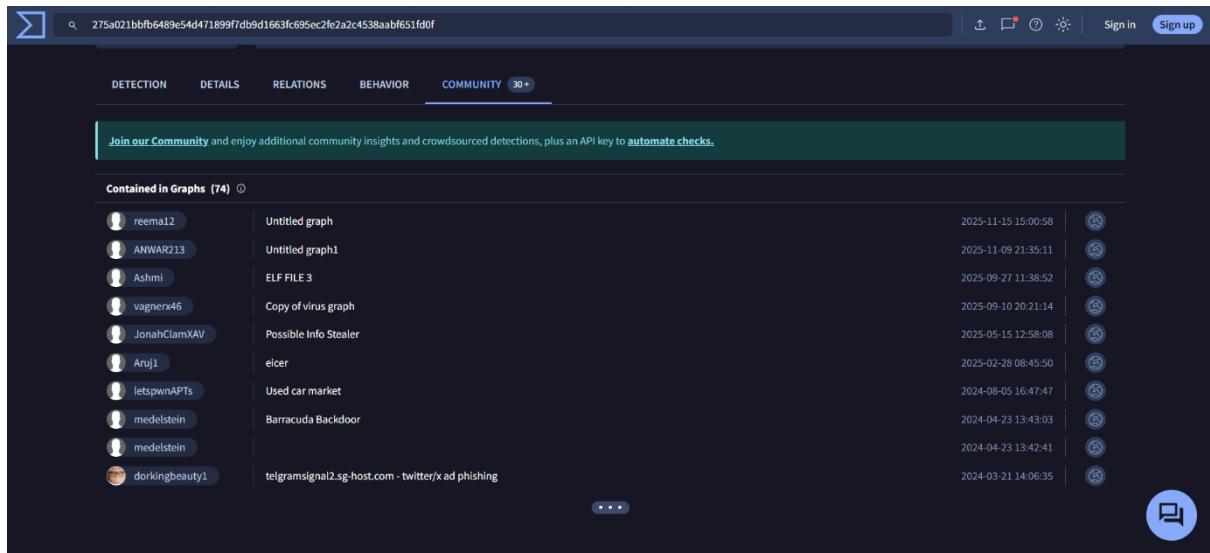
This screenshot shows the 'Behavior' tab of a VirusTotal analysis page. It highlights various suspicious activities observed during the analysis. Key findings include:

- A large red circle highlights a "Community Score" of 64 / 66.
- The file was distributed by Offensive Security.
- File details: Hash (275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c453aabf651fd0f), Size (68 B), and Last Analysis Date (2 minutes ago).
- Threat labels: powershell, known-distributor, long-sleeps, direct-cpu-clock-access, idle, attachment, detect-debug-environment, via-tor.
- Behavior indicators from various sandboxes and tools:

 - CAPE Linux: △ 0, ▲ 1, ⚡ 1, ⚡ 0, ⚡ 0, ⚡ 4, ⚡ 5, ⚡ 0.
 - CAPE Sandbox: △ 0, ⚡ 5, ⚡ 0, ⚡ 0, ⚡ 0, ⚡ 5, ⚡ 0.
 - Lastline: △ 2, ⚡ 0, ⚡ 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.

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

5. Community and Security Vendor Analysis



The screenshot shows a dark-themed user interface for a security analysis platform. At the top, there's a search bar with the ID '275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0'. Below the search bar is a navigation menu with tabs: DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with a '30+' badge). A green banner below the tabs encourages users to 'Join our Community' for additional insights and API access. The main content area is titled 'Contained in Graphs (74)' and lists 10 entries, each with a small profile icon, the graph name, and a timestamp. The entries are:

User	Graph Name	Timestamp
reema12	Untitled graph	2025-11-15 15:00:58
ANWAR213	Untitled graph1	2025-11-09 21:35:11
Ashmi	ELF FILE 3	2025-09-27 11:38:52
vagnerx46	Copy of virus graph	2025-09-10 20:21:14
JonahClamXAV	Possible Info Stealer	2025-05-15 12:58:08
Aruj1	eicer	2025-02-28 08:45:50
letsppwnAPTs	Used car market	2024-08-05 16:47:47
medelstein	Barracuda Backdoor	2024-04-23 13:43:03
medelstein	telegramsignal2.sg-host.com - twitter/x ad phishing	2024-04-23 13:42:41
dorkingbeauty1		2024-03-21 14:06:35

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.
-

4 **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.)

5 **Behavior Indicators Observed**

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

6 **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
-

7 Malware Spread Methods

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

8 Prevention Methods

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

9 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.