
Safe Malware Analysis with VirusTotal

(EICAR Test File)

Project: Safe Malware Analysis with VirusTotal

Author: Mihira Seru

Description: Independent research on detecting safe test files (EICAR) using VirusTotal.

Date: November 2025

Step-by-Step Guide: Safe Malware Analysis Using the EICAR Test File and VirusTotal

This guide demonstrates how to safely perform a basic malware analysis using the EICAR test file inside a virtual machine (VM).
It walks through setting up a secure environment, uploading the file to VirusTotal, interpreting antivirus detections, and restoring your system to a clean state.
The project helps beginners understand how security analysts verify and analyze potential threats without handling real malware.

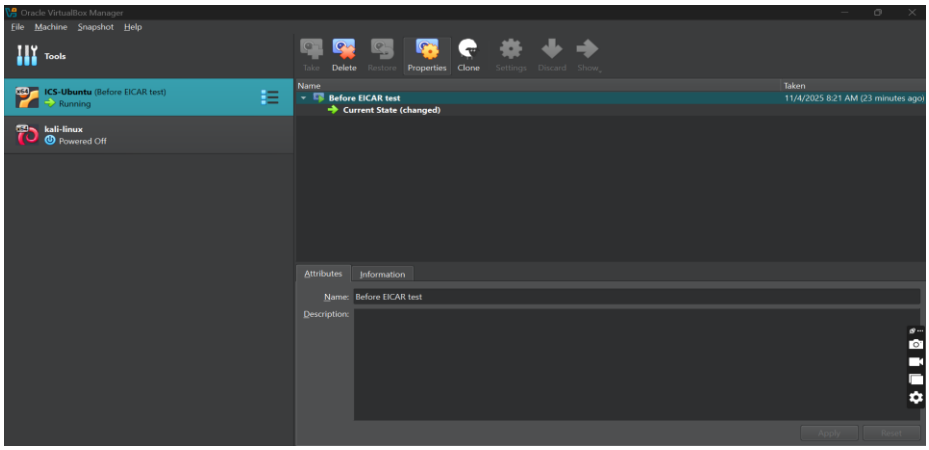
Setting up lab environment for testing

1. Open ubuntu VM
2. Take a snapshot as **Clean State**
   Machine → Take Snapshot…
   - A dialog appears:
   - Name: Clean State (or anything you like)
   - Description (optional): “Before EICAR test.”
   - Click OK
3. Restoring a Snapshot in VirtualBox - **use it only when something goes wrong**

- Restoring removes all changes made after the snapshot — useful for cleaning up experiments, undoing mistakes, or resetting before the next test.

Steps:

- Shut down the VM.
- In VirtualBox, open the **Snapshots** view.
- Select the snapshot you want to return to (e.g., *Clean State*).
- Click **Restore** → confirm.
- The VM will revert to exactly how it was when that snapshot was taken.

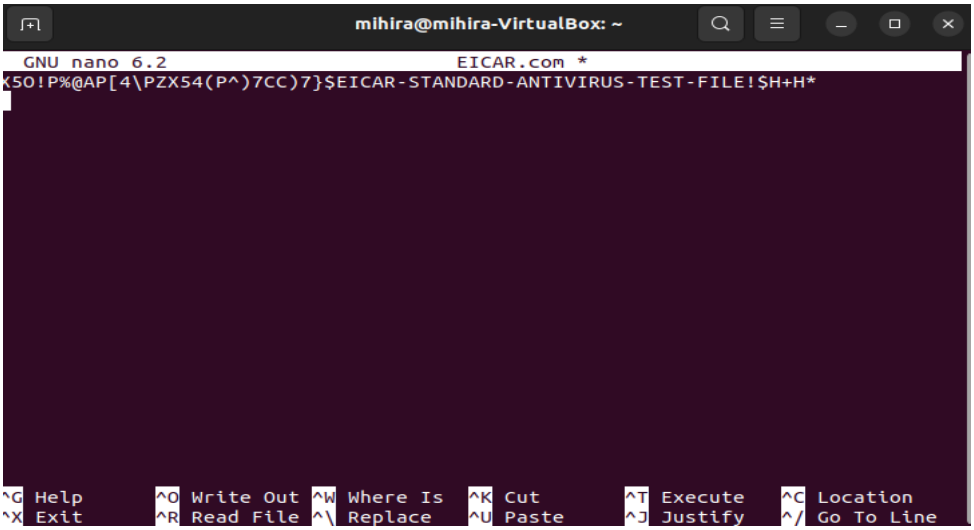


Creating & testing a sample Virus file

1. For this we use a website named eicar.org, to get the standard (trusted) virus files for testing. So that, they don't affect your system.

   Steps:

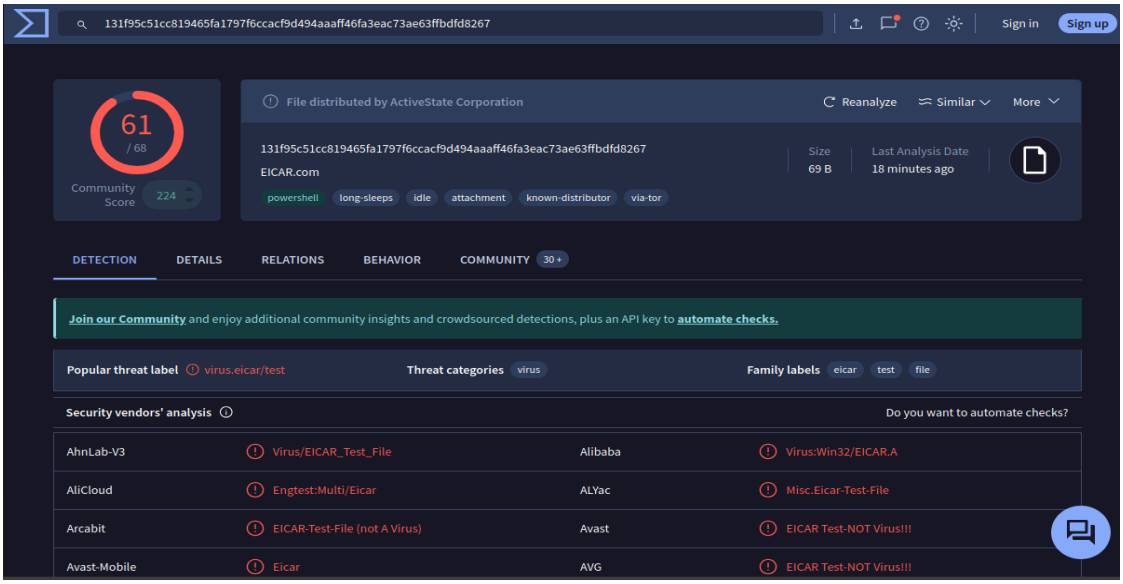
   - Open nano editor with filename as : EICAR.org
     $nano EICAR.com
   - Enter the string as shown, then press **`Ctrl + O`** → **`Enter`** → **`Ctrl + X`**
   - Use **`ls`** command to verify if the file got saved or not



- Now we have created our sample antivirus file for testing.

2. Open your browser (inside the VM) and go to: https://www.virustotal.com

- **VirusTotal** is a free site that scans files with many antivirus engines to check for threats. Uploading our EICAR file shows how antivirus detections work in real time.
- Uploading EICAR.com to VirusTotal



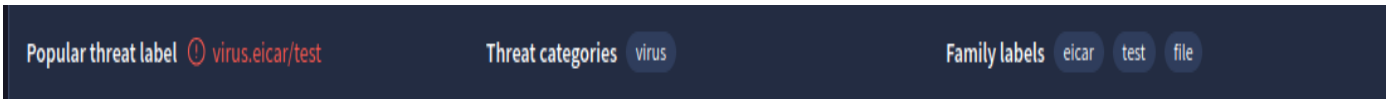
- These are the detections from various antivirus (AV) engines.

Note: Do **not** perform this on your host system.
The EICAR test file may still trigger alerts even though it's harmless.
Always use an isolated VM for safe handling.

Analysing results on VirusTotal

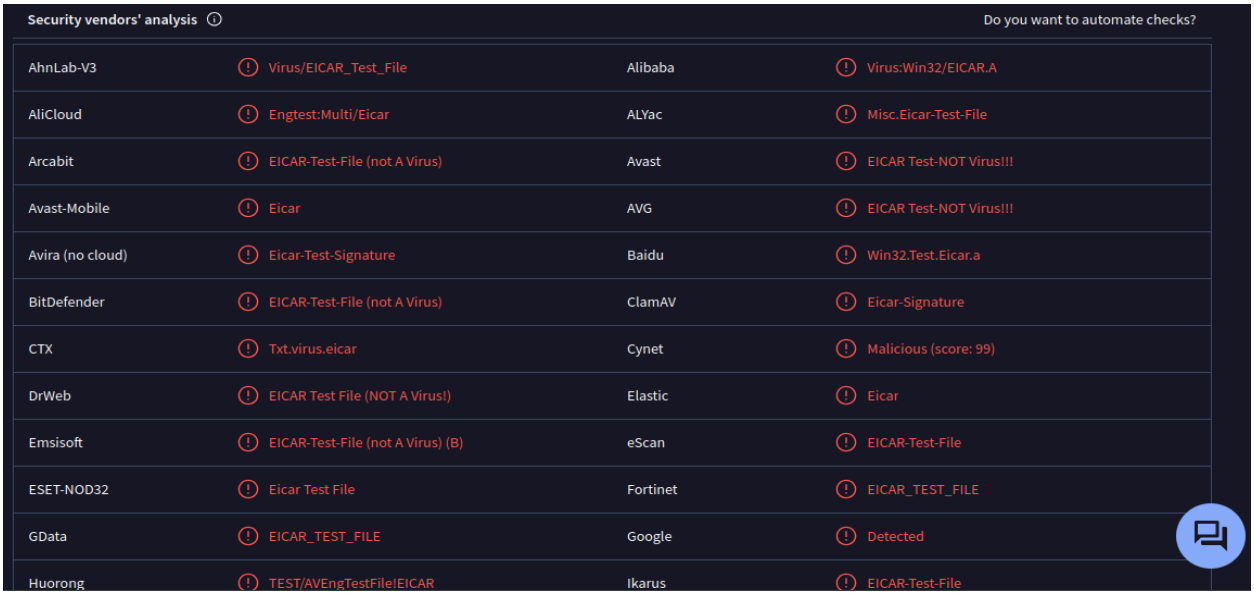
1. **Detection Overview:**
   - The file has **61/68 detections**, meaning 61 antivirus engines identified it as malicious.
   - The **Community Score 224** shows that VirusTotal users also recognized it as a known test file.

2. **Popular Threat Label:**



- It's labeled as **virus.eicar/test**, which means this is the **EICAR test file**, a *non-malicious* file used to check antivirus detection.
- Many AVs tag it as "Test File" or "EICAR-Test-NOT Virus," confirming it's safe.

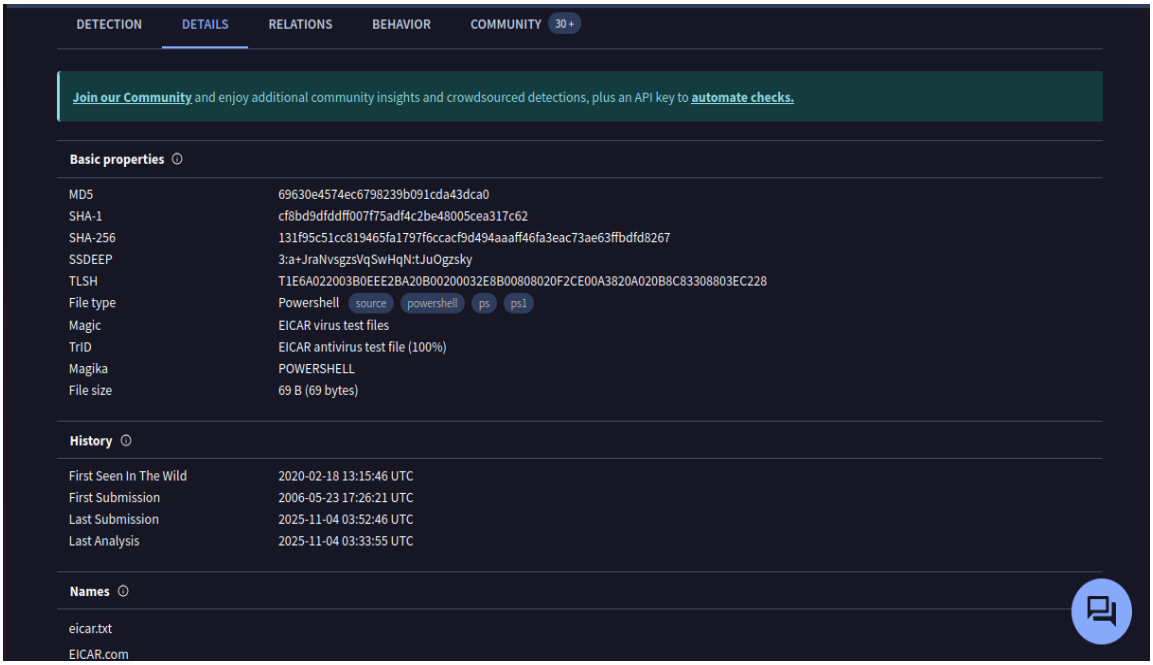
3. Vendor Analysis Table:



- Each antivirus engine's result is listed.
- For example, **Avast → "EICAR Test-NOT Virus!!!"** and **Arcabit → "EICAR-Test-File (not A Virus)"** clearly indicate it's not real malware.

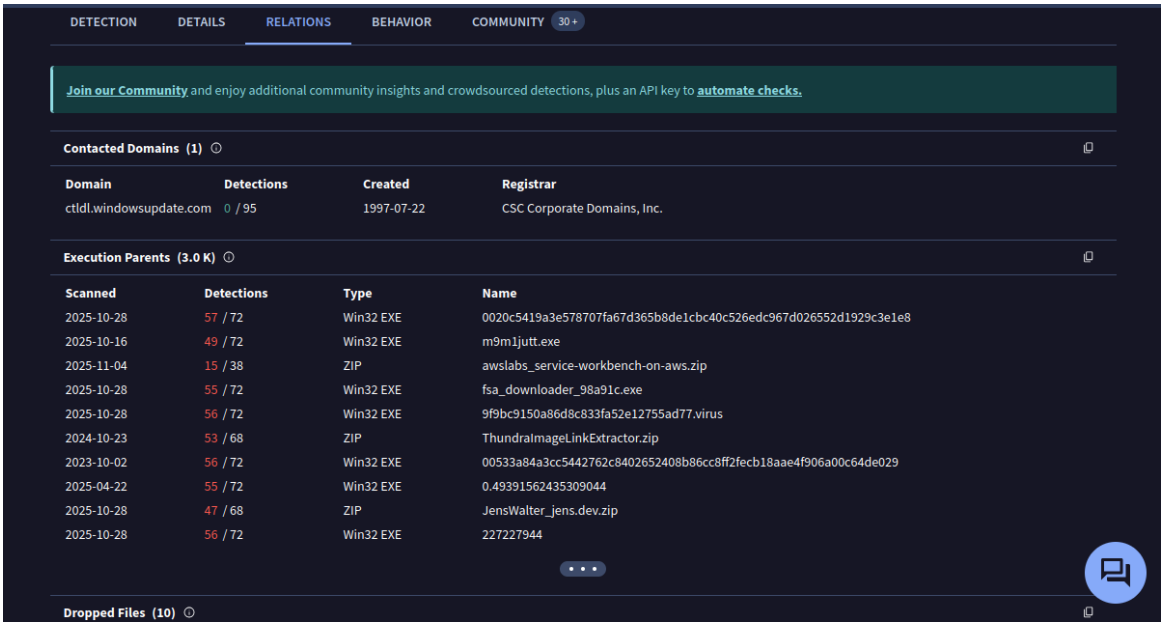
Field	Description
Security Vendor	**Name of the antivirus engine (e.g., Avast, Kaspersky).**
Detection Name / Result	**What the engine labeled the file as (e.g., *EICAR-Test-File*, *Trojan.Win32*).**
Severity Icon	**Shows if the file is malicious or clean .**
Category / Family Label	**Type or family of threat (e.g., *EICAR*, *Trojan*, *Worm*).**
Community Tags	**Keywords describing file behavior or context (e.g., *powershell*, *attachment*).**

4. Details tab



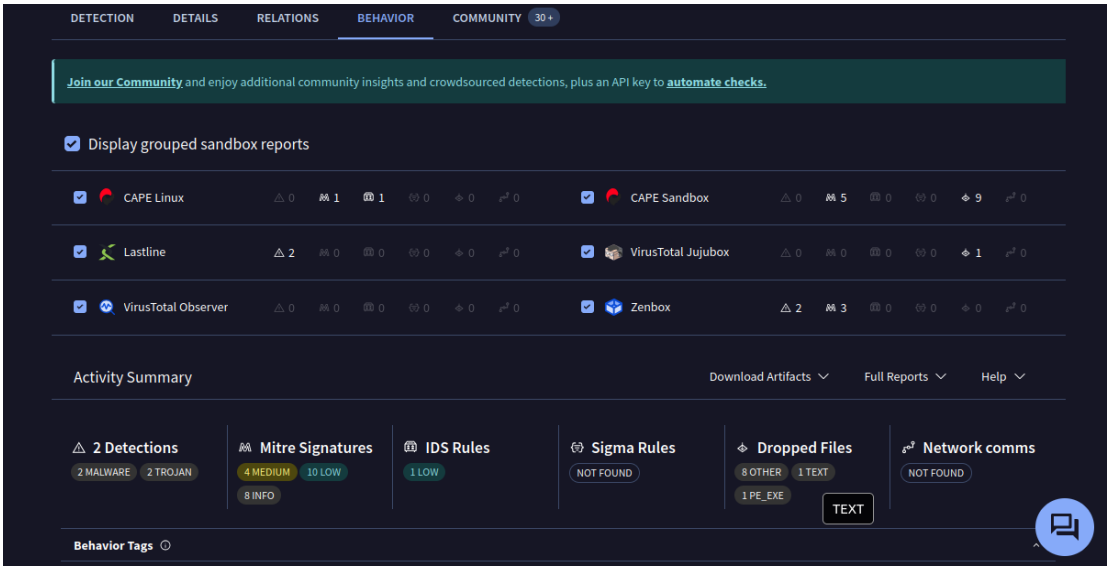
- File info like hash values (MD5, SHA-1, SHA-256), size, file type, creation time, and signatures. Used to verify integrity and identify file type.

5. Relations tab



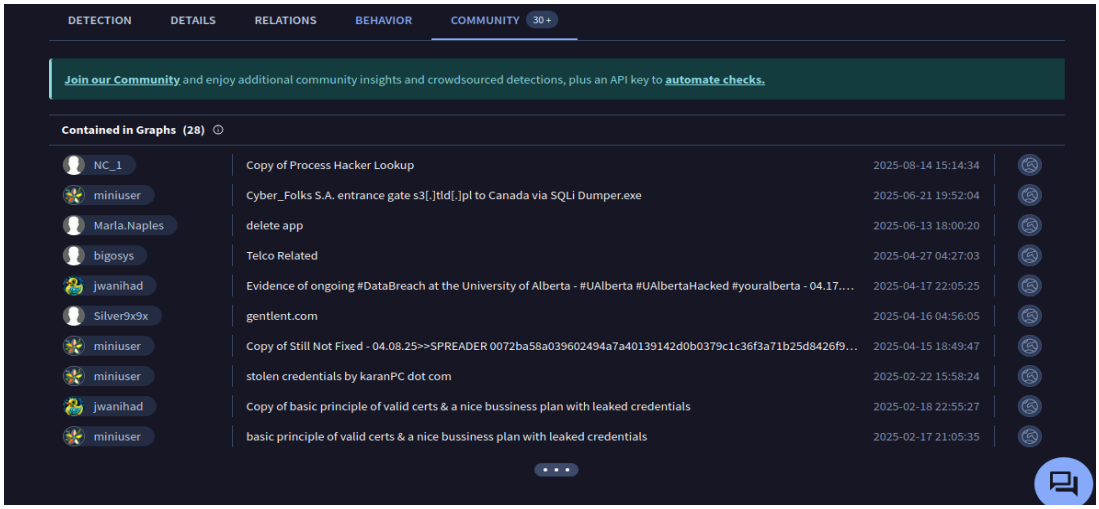
- Shows links between this file and other items (e.g., URLs or IPs it contacted).

6. Behaviour tab



- Shows what the file *does* when executed in VirusTotal's sandbox (e.g., creates files, modifies registry, connects to IPs). For EICAR, this will be empty since it's harmless.

7. Community tab



- Comments and votes from other analysts about the file.

After the Test

1. **Delete** the `EICAR.com` file from your VM (optional, since it's harmless).
2. **Restore your snapshot** to return the VM to a clean state — this removes all test activity and keeps your analysis environment safe for future labs.

Key Takeaways

- Learned how antivirus engines identify known signatures
- Understood VirusTotal's behaviour and metadata analysis tabs
- Practiced safe malware handling inside an isolated VM