
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.

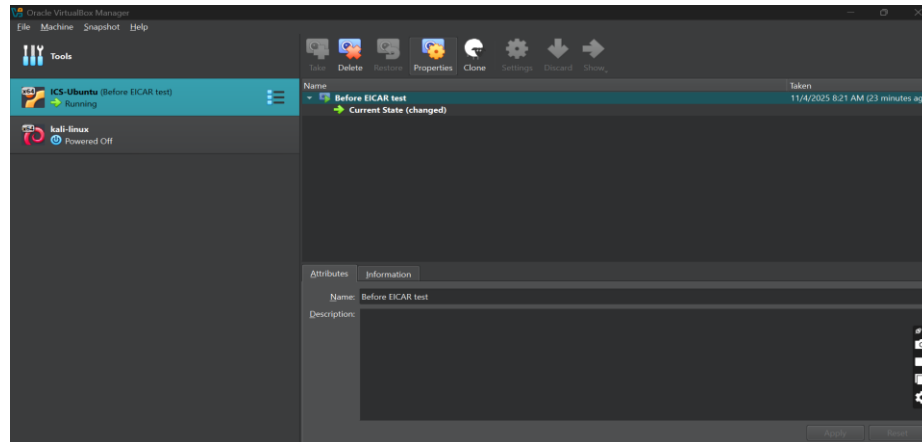
Setting up lab environment for testing

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.

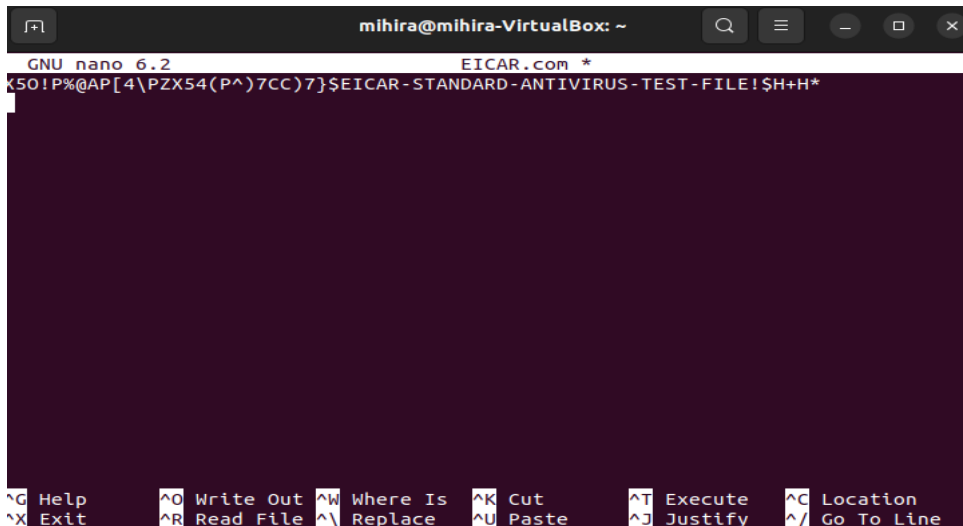


Creating & testing a sample Virus file

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 + 0** → **Enter** → **Ctrl + X**
- Use **ls** command to verify if the file got saved or not



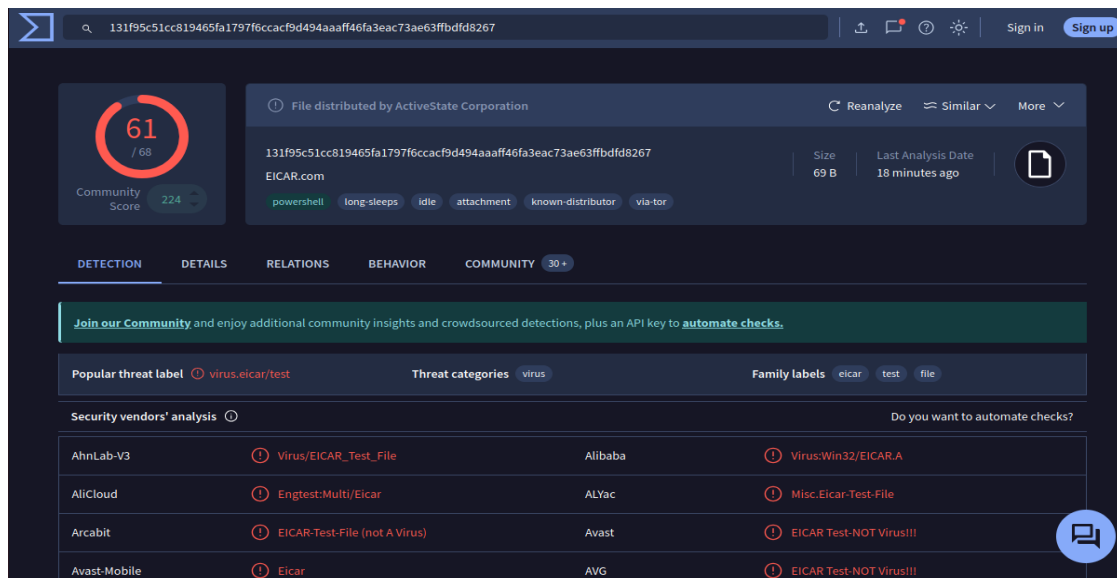
The screenshot shows a terminal window titled 'mihira@mihira-VirtualBox: ~'. Inside, the GNU nano 6.2 editor is open, editing a file named 'EICAR.com'. The file contains the standard EICAR test string: 'X5O!P%@AP[4\PZX54(P^7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*'. The bottom of the terminal shows the nano editor's command shortcuts: ^G Help, ^O Write Out, ^W Where Is, ^K Cut, ^T Execute, ^C Location, ^X Exit, ^R Read File, ^_ Replace, ^U Paste, ^J Justify, and ^_/ Go To Line.

- 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](https://www.virustotal.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:

























Popular threat label  virus.eicar/test

Threat categories  virus



Family labels  eicar  test  file

- 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:

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
Arcabit	 EICAR-Test-File (not A Virus)	Avast	 EICAR Test-NOT Virus!!!
Avast-Mobile	 Eicar	AVG	 EICAR Test-NOT Virus!!!
Avira (no cloud)	 Eicar-Test-Signature	Baidu	 Win32.Test.Eicar.a
BitDefender	 EICAR-Test-File (not A Virus)	ClamAV	 Eicar-Signature
CTX	 Txt.virus.eicar	Cynet	 Malicious (score: 99)
DrWeb	 EICAR Test File (NOT A Virus!)	Elastic	 Eicar
Emsisoft	 EICAR-Test-File (not A Virus) (B)	eScan	 EICAR-Test-File
ESET-NOD32	 Eicar Test File	Fortinet	 EICAR_TEST_FILE
GData	 EICAR_TEST_FILE	Google	 Detected
Huorong	 TEST/AVEngTestFileEICAR	Ikarus	 EICAR-Test-File

- 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., <i>EICAR-Test-File</i> , <i>Trojan.Win32</i>).
Severity Icon	Shows if the file is malicious  or clean  .
Category / Family Label	Type or family of threat (e.g., <i>EICAR</i> , <i>Trojan</i> , <i>Worm</i>).
Community Tags	Keywords describing file behavior or context (e.g., <i>powershell</i> , <i>attachment</i>).

4. Details tab

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 30+

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

Basic properties

MD5	69630e4574ec6798239b091cda43dca0
SHA-1	cf8bd9dfddff007f75adf4c2be48005cea317c62
SHA-256	131f95c51cc819465fa1797f6ccacf9d494aaaff46fa3eac73ae63ffbfdd8267
SSDEEP	3:a+JraNvsqzVqSwHqNtLJuOgzsky
TLSH	T1E6A022003B0EEE2BA20B00200032E8B00808020F2CE00A3820A020B8C83308803EC228
File type	Powershell source powershell ps ps1
Magic	EICAR virus test files
TrID	EICAR antivirus test file (100%)
Magika	POWERSHELL
File size	69 B (69 bytes)

History

First Seen In The Wild	2020-02-18 13:15:46 UTC
First Submission	2006-05-23 17:26:21 UTC
Last Submission	2025-11-04 03:52:46 UTC
Last Analysis	2025-11-04 03:33:55 UTC

Names

eicar.txt

EICAR.com

- 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

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 30+

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

Contacted Domains (1)

Domain	Detections	Created	Registrar
ctldl.windowsupdate.com	0 / 95	1997-07-22	CSC Corporate Domains, Inc.

Execution Parents (3.0 K)

Scanned	Detections	Type	Name
2025-10-28	57 / 72	Win32 EXE	0020c5419a3e578707fa67d365b8de1cbc40c526edc967d026552d1929c3e1e8
2025-10-16	49 / 72	Win32 EXE	m9m1jutt.exe
2025-11-04	15 / 38	ZIP	awslabs_service-workbench-on-aws.zip
2025-10-28	55 / 72	Win32 EXE	fsa_downloader_98a91c.exe
2025-10-28	56 / 72	Win32 EXE	9f9bc9150a86d8c833fa52e12755ad77.virus
2024-10-23	53 / 68	ZIP	ThundralImageLinkExtractor.zip
2023-10-02	56 / 72	Win32 EXE	00533a84a3cc5442762c8402652408b86cc8ff2fecb18aae4f906a00c64de029
2025-04-22	55 / 72	Win32 EXE	0.49391562435309044
2025-10-28	47 / 68	ZIP	JensWalter_jens.dev.zip
2025-10-28	56 / 72	Win32 EXE	227227944

Dropped Files (10)

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

6. Behaviour tab

DETECTION DETAILS RELATIONS **BEHAVIOR** COMMUNITY (30+)

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

☒ Display grouped sandbox reports

<input checked="" type="checkbox"/> CAPE Linux	△ 0	👤 1	🔒 1	🔍 0	🔗 0	📄 0	<input checked="" type="checkbox"/> CAPE Sandbox	△ 0	👤 5	🔒 0	🔍 0	🔗 9	📄 0
<input checked="" type="checkbox"/> Lastline	△ 2	👤 0	🔒 0	🔍 0	🔗 0	📄 0	<input checked="" type="checkbox"/> VirusTotal Jujubox	△ 0	👤 0	🔒 0	🔍 0	🔗 1	📄 0
<input checked="" type="checkbox"/> VirusTotal Observer	△ 0	👤 0	🔒 0	🔍 0	🔗 0	📄 0	<input checked="" type="checkbox"/> Zenbox	△ 2	👤 3	🔒 0	🔍 0	🔗 0	📄 0

Activity Summary Download Artifacts ▾ Full Reports ▾ Help ▾

△ 2 Detections 2 MALWARE 2 TROJAN	👤 Mitre Signatures 4 MEDIUM 10 LOW 8 INFO	🔒 IDS Rules 1 LOW	🔍 Sigma Rules NOT FOUND	🔗 Dropped Files 8 OTHER 1 TEXT 1 PE_EXE	📄 Network comms NOT FOUND
---	--	-----------------------------	-----------------------------------	--	-------------------------------------

Behavior Tags ○ 🗨️

- 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

DETECTION DETAILS RELATIONS **BEHAVIOR** **COMMUNITY** (30+)

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Contained in Graphs (28) ○

NC_1	Copy of Process Hacker Lookup	2025-08-14 15:14:34	🗨️
miniuser	Cyber_Folks S.A. entrance gate s3[.]tld[.]pl to Canada via SQLi Dumper.exe	2025-06-21 19:52:04	🗨️
Marla.Naples	delete app	2025-06-13 18:00:20	🗨️
bigosys	Telco Related	2025-04-27 04:27:03	🗨️
jwanihad	Evidence of ongoing #DataBreach at the University of Alberta - #UALberta #UALbertaHacked #youralberta - 04.17....	2025-04-17 22:05:25	🗨️
Silver9x9x	gentlent.com	2025-04-16 04:56:05	🗨️
miniuser	Copy of Still Not Fixed - 04.08.25>>SPREADER 0072ba58a039602494a7a40139142d0b0379c1c36f3a71b25d8426f9...	2025-04-15 18:49:47	🗨️
miniuser	stolen credentials by karanPC dot com	2025-02-22 15:58:24	🗨️
jwanihad	Copy of basic principle of valid certs & a nice bussiness plan with leaked credentials	2025-02-18 22:55:27	🗨️
miniuser	basic principle of valid certs & a nice bussiness plan with leaked credentials	2025-02-17 21:05:35	🗨️

... 🗨️

- 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