Malware Types Behavior Analysis (Basic)

January 22, 2026

Introduction

Malware is malicious software designed to disrupt systems, steal sensitive information, or gain unauthorized access. Understanding different malware types and their behavior is essential in cybersecurity. VirusTotal provides a safe platform for analyzing malware using hash-based detection. This practical focuses on malware analysis, lifecycle, spread methods, and prevention techniques.

—

1 Different Types of Malware

1.1 Virus

- Attaches to legitimate files
- Requires user action to execute
- Spreads through file sharing

1.2 Worm

- Self-replicating malware
- Spreads automatically over networks
- No user interaction required

1.3 Trojan

- Disguised as legitimate software
- Creates backdoors or steals sensitive data
- Does not self-replicate

1.4 Ransomware

- Encrypts user data
- Demands ransom payment
- Often spreads via phishing emails or software exploits

—

2 Uploading Malware Hashes to VirusTotal

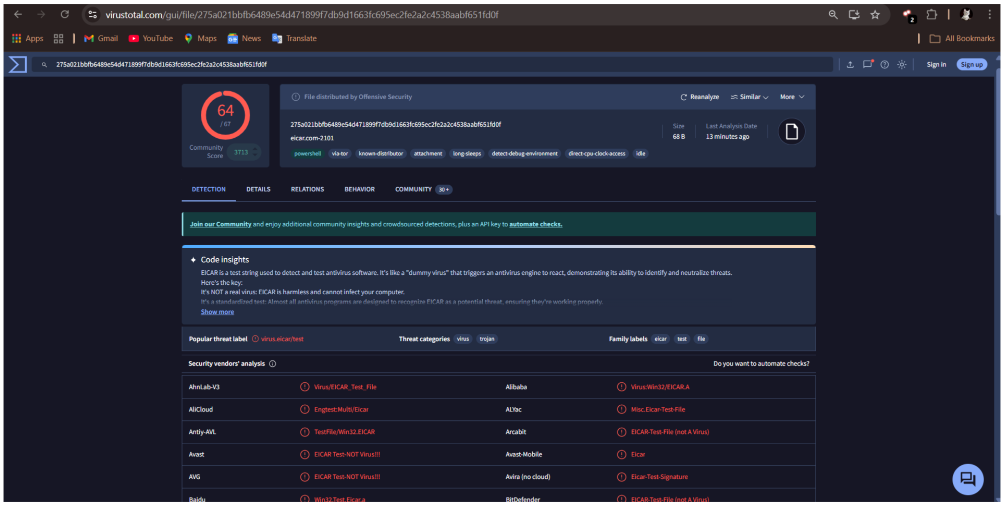
Only malware hash values are uploaded to VirusTotal to ensure safety and legality.

Procedure:

1. Open `https://www.virustotal.com`
2. Click on the **Search** option
3. Paste the malware hash value
4. Press Enter to analyze

Example Hash:

```
44d88612fea8a8f36de82e1278abb02f
```



virustotal.com/gui/file/275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

64 / 67

Community Score 3713

File distributed by Offensive Security

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
eicar.com-2101

powershell via-tor known-distributor attachment long-sleeps detect-debug-environment direct-cpu-clock-access idle

Size 68 B

Last Analysis Date 13 minutes ago

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

✦ Code insights

EICAR is a test string used to detect and test antivirus software. It's like a "dummy virus" that triggers an antivirus engine to react, demonstrating its ability to identify and neutralize threats.
Here's the key:
It's NOT a real virus: EICAR is harmless and cannot infect your computer.
It's a standardized test: Almost all antivirus programs are designed to recognize EICAR as a potential threat, ensuring they're working properly.

Popular threat label virus.eicar/test

Threat categories virus trojan

Family labels eicar test file

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
Antiy-AVL	TestFile/Win32.EICAR	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)

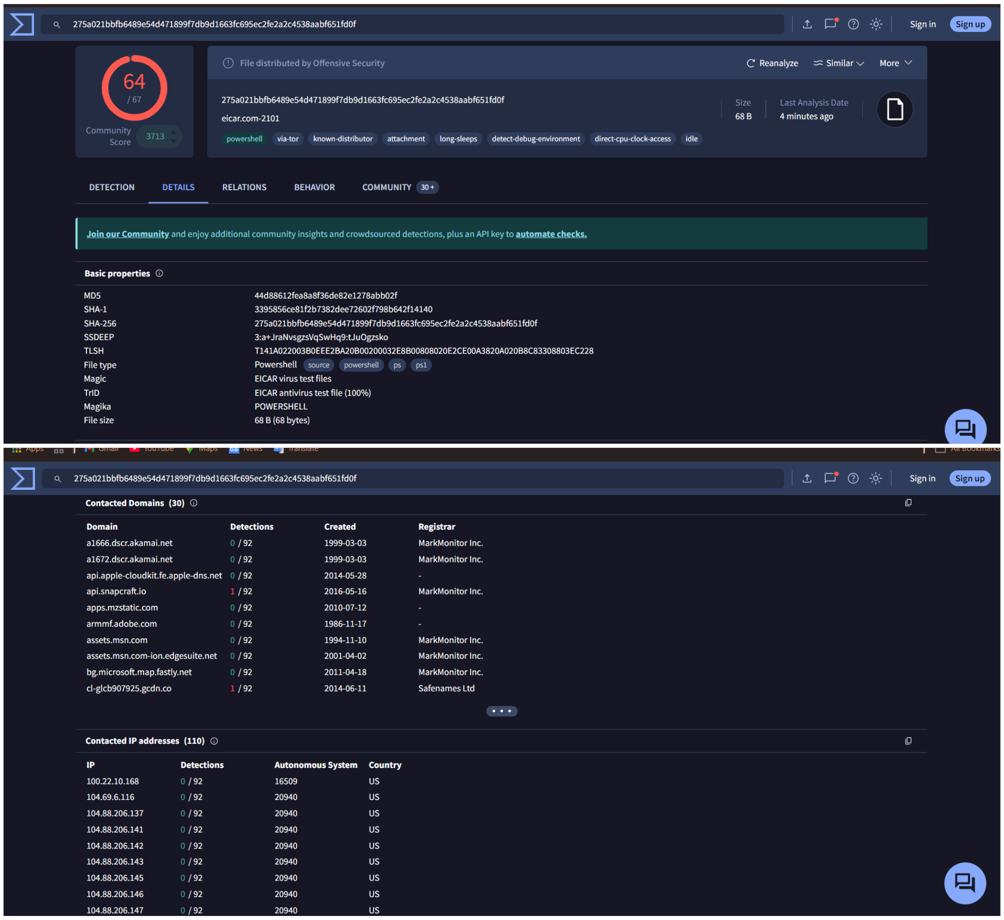
Figure 1: VirusTotal Homepage Showing Hash Search

—

3 Detection Report Analysis

The detection report provides information about malware severity and classification.

- Detection Ratio (e.g., 50/70)
- Malware Family Name
- File Type
- First Seen and Last Seen Details



275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

eicar.com-2101

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

Basic properties

MD5	44d88612fea8a8f36de82e1278abb02f
SHA-1	3395856ce81f2b7382dee72602f798b642f14140
SHA-256	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
SSDEEP	3:a+JraNvsgzsVqSwHq9:tJuOgzsko
TLSH	T141A022003B0EEE2BA20B00200032E8B00808020E2CE00A3820A020B8C83308803EC228
File type	Powershell source powershell ps ps1
Magic	EICAR virus test files
TrID	EICAR antivirus test file (100%)
Magika	POWERSHELL
File size	68 B (68 bytes)

Contacted Domains (30)

Domain	Detections	Created	Registrar
a1666.dscr.akamai.net	0 / 92	1999-03-03	MarkMonitor Inc.
a1672.dscr.akamai.net	0 / 92	1999-03-03	MarkMonitor Inc.
api.apple-cloudkit.fe.apple-dns.net	0 / 92	2014-05-28	-
api.snapcraft.io	1 / 92	2016-05-16	MarkMonitor Inc.
apps.mzstatic.com	0 / 92	2010-07-12	-
armmf.adobe.com	0 / 92	1986-11-17	-
assets.msn.com	0 / 92	1994-11-10	MarkMonitor Inc.
assets.msn.com-ion.edgesuite.net	0 / 92	2001-04-02	MarkMonitor Inc.
bg.microsoft.map.fastly.net	0 / 92	2011-04-18	MarkMonitor Inc.
cl-glcb907925.gcdn.co	1 / 92	2014-06-11	Safenames Ltd

Contacted IP addresses (110)

IP	Detections	Autonomous System	Country
100.22.10.168	0 / 92	16509	US
104.69.6.116	0 / 92	20940	US
104.88.206.137	0 / 92	20940	US
104.88.206.141	0 / 92	20940	US
104.88.206.142	0 / 92	20940	US
104.88.206.143	0 / 92	20940	US
104.88.206.145	0 / 92	20940	US
104.88.206.146	0 / 92	20940	US
104.88.206.147	0 / 92	20940	US

Figure 2: VirusTotal Detection Report

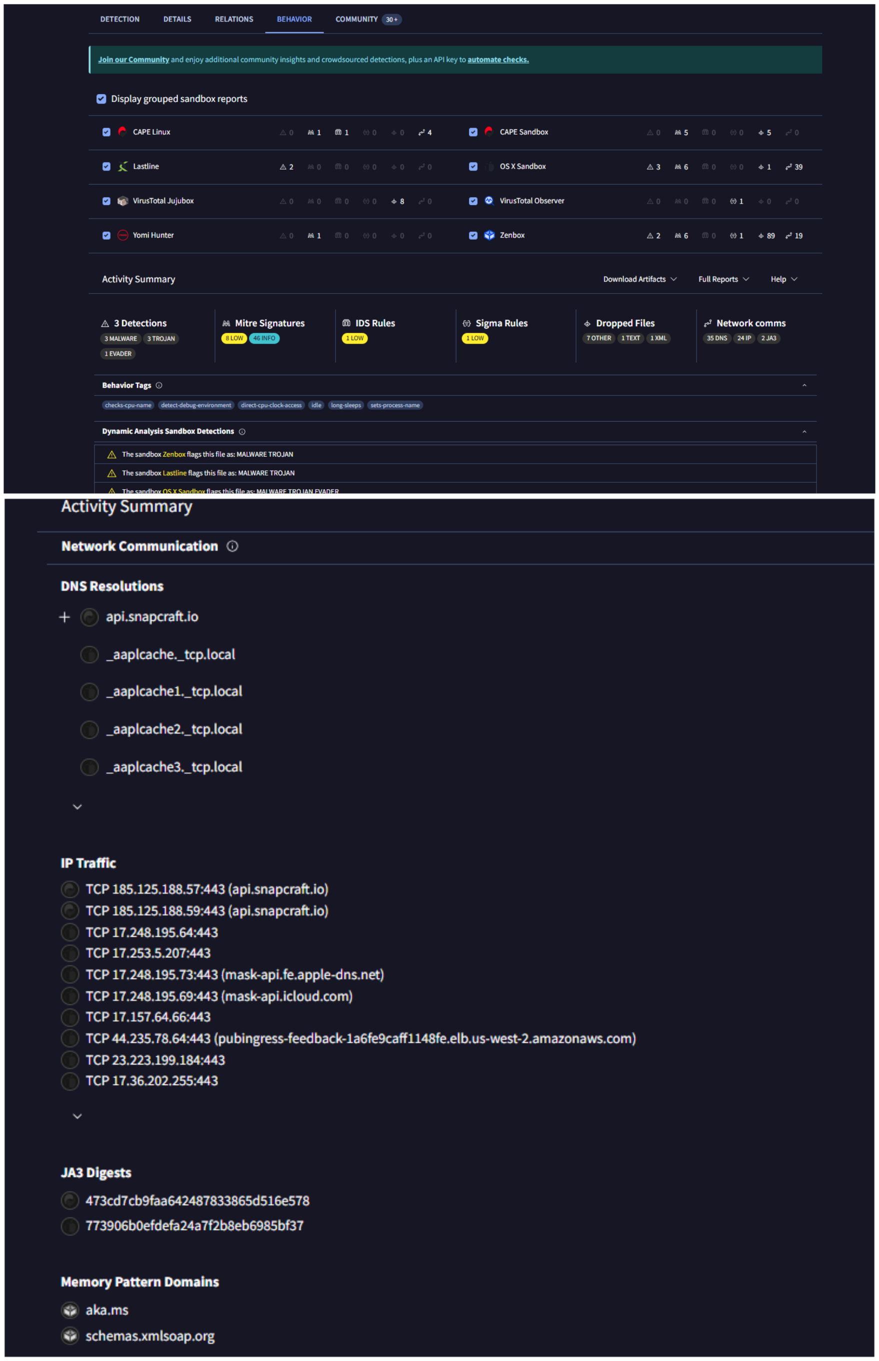
—

4 Behavior Indicators

Behavior analysis helps understand real-time malware activity.

- File creation and modification

- Registry changes
- Network communication
- Process injection



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

☑ Display grouped sandbox reports

	⚠					
☑ CAPE Linux	0	1	1	0	0	4
☑ Lastline	2	0	0	0	0	0
☑ VirusTotal Jujubox	0	0	0	0	8	0
☑ Yomi Hunter	0	1	0	0	0	0
☑ CAPE Sandbox	0	5	0	0	5	0
☑ OS X Sandbox	3	6	0	0	1	39
☑ VirusTotal Observer	0	0	0	1	0	0
☑ Zenbox	2	6	0	1	89	19

Activity Summary

⚠ 3 Detections	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
3 MALWARE 3 TROJAN 1 EVADER	8 LOW 46 INFO	1 LOW	1 LOW	7 OTHER 1 TEXT 1 XML	35 DNS 24 IP 2 JA3

Behavior Tags

checks-cpu-name, detect-debug-environment, direct-cpu-clock-access, idle, long-sleeps, sets-process-name

Dynamic Analysis Sandbox Detections

⚠ The sandbox Zenbox flags this file as: MALWARE TROJAN

⚠ The sandbox Lastline flags this file as: MALWARE TROJAN

⚠ The sandbox OS X Sandbox flags this file as: MALWARE TROJAN EVADER

Activity Summary

Network Communication

DNS Resolutions

- api.snapcraft.io
- _aaplcache._tcp.local
- _aaplcache1._tcp.local
- _aaplcache2._tcp.local
- _aaplcache3._tcp.local

IP Traffic

- TCP 185.125.188.57:443 (api.snapcraft.io)
- TCP 185.125.188.59:443 (api.snapcraft.io)
- TCP 17.248.195.64:443
- TCP 17.253.5.207:443
- TCP 17.248.195.73:443 (mask-api.fe.apple-dns.net)
- TCP 17.248.195.69:443 (mask-api.icloud.com)
- TCP 17.157.64.66:443
- TCP 44.235.78.64:443 (pubingress-feedback-1a6fe9caff1148fe.elb.us-west-2.amazonaws.com)
- TCP 23.223.199.184:443
- TCP 17.36.202.255:443

JA3 Digests

- 473cd7cb9faa642487833865d516e578
- 773906b0efdefa24a7f2b8eb6985bf37

Memory Pattern Domains

- aka.ms
- schemas.xmlsoap.org

Figure 3: Behavior Indicators Observed in VirusTotal

5 Malware Lifecycle

The typical lifecycle of malware consists of the following stages:

1. **Creation**: The attacker develops or writes the malware code.
2. **Distribution**: Malware is distributed through emails, USB devices, or exploit kits.
3. **Execution**: The malware executes when a user runs the infected file or when an exploit is triggered.
4. **Persistence**: Malware establishes mechanisms to survive system reboots.
5. **Command and Control (C2)**: The malware communicates with the attacker's server to receive instructions.
6. **Payload Action**: Malicious activities such as data theft, file encryption, or spying are performed.
7. **Cleanup / Spread**: The malware deletes traces to avoid detection or spreads to other systems.

6 How Malware Spreads

Malware can spread through various vectors as listed below:

- Phishing emails
- Malicious downloads from untrusted sources
- Infected USB devices
- Exploitation of network vulnerabilities
- Fake or malicious software updates
- Cracked or pirated software

—

7 Prevention Methods

Effective prevention techniques help reduce the risk of malware infections:

- Use updated antivirus software
- Enable and properly configure firewall
- Perform regular operating system and software updates

- Avoid opening unknown or suspicious email attachments
- Use strong passwords and enable Multi-Factor Authentication (MFA)
- Disable autorun feature for USB devices
- Conduct user awareness and cybersecurity training

8 Summary of Findings

- Malware exists in many forms, each exhibiting different behaviors.
- VirusTotal is an effective tool for hash-based malware analysis.
- Detection reports assist in identifying malware type and severity.
- Behavior indicators reveal the real-world impact of malware.
- Understanding the malware lifecycle supports better defense planning.
- Most malware infections occur due to human error.
- Effective prevention depends on a combination of technology and user awareness.