Malware Types & Behaviour Analysis

Malware:

A malicious file or software which is designed to harm a system or steal data or spy on users or disrupt services.

Types of Malwares:

1. Virus
2. Worm
3. Trojan
4. Ransomware
5. Spyware
6. Adware
7. Backdoor
8. Rootkit
9. Botnet Malware
10. Fileless Malware

Virus:

Attached with legitimate files and spreads when the file runs. It needs user action for do this work.

WORM:

It spreads automatically. It spread with the entire network without user action.

Trojan:

It looks legitimate but it has malicious inside it. It does not self-replicate.

Ransomware:

It encrypts files and demands payment for decrypt it.

Spyware:

It is a malicious file used for secretly monitors user activities like keystroke logging, screenshot capturing.

Adware:

It used to display unwanted ads like browser Pop-ups, Redirects.

Backdoor:

It creates a secret access to the system. It gives remote access for the attackers.

Rootkit:

It used to hide malware from the system. It needs deep system access to do its work.

Botnet Malware:

It turns the affected system into bot. It communicates with C2 server.

File less Malware:

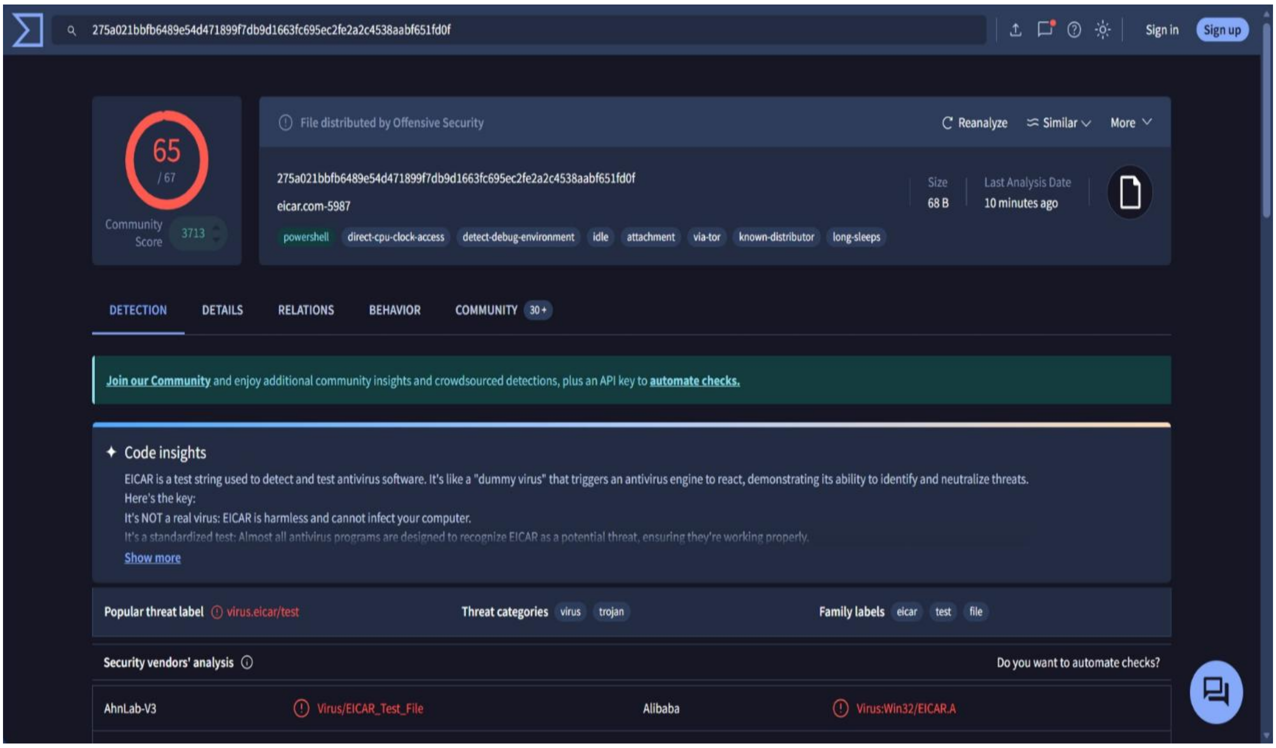
It runs in memory, not as a file. It uses PowerShell or scripts.

Malware Research:

Tool: Virustotal.com

Hash:

275a021bbfb6489e54d4718899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f



275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

65 / 67

Community Score 3713

File distributed by Offensive Security

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

eicar.com-5987

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

Size 68 B

Last Analysis Date 10 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.

Show more

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

This report shows that the hash has 65/67 detection ratio. So, it is a high-risk threat. It is a fileless malware and it works on PowerShell. The high detection ratio clearly confirms that the analysed hash represents a known and confirmed malicious threat, despite the absence of a traditional executable file.