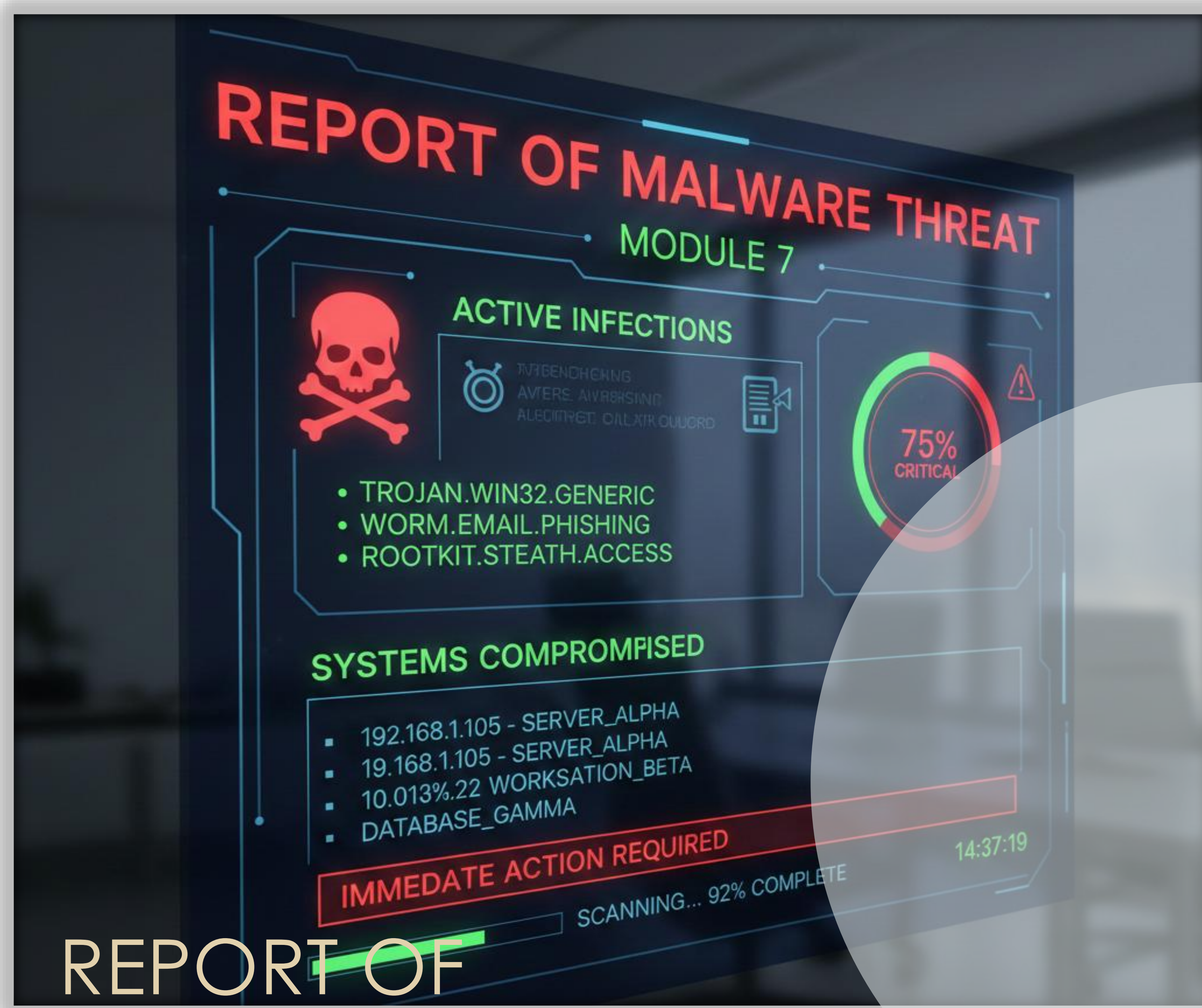


REPORT OF MALWARE THREAT

BY SACHCHITANAND YADAV

MALWARE THREAT MODULE - 7

Learning Objectives -

- Explain different malware threats and their categories concepts.
- Describe how njRAT Trojans operate.
- Perform static and dynamic malware analysis using common tools.
- Monitor system, process, and network activity for malicious behavior.
- Explain Malware Countermeasures

Table of Contents

5. Dynamic Malware Analysis

6. Infecting a Target System Using a virus

7. Malware Countermeasures

8. Module Summary

Malware Threat Concepts: -

Malware Threat

What is Malware?

Malware — short for *malicious software* — is any program created with harmful intent. Its mission? To break things, steal what isn't theirs, or quietly slip into systems where it has no business being. Attackers deploy malware to gain unauthorized access, extract sensitive data, disrupt operations, or simply cause chaos for fun or profit.

Types of Malwares

1. Virus

- **How it works:** Infects legitimate files or programs and spreads when those files are executed.
- **Impact:** Corrupts data, deletes files, slows systems, and causes crashes.
- **User action required:** Yes (opening the infected file).
- **Example:** ILOVEYOU virus.

2. Worm

- **How it works:** Spreads automatically across networks without user interaction.
- **Impact:** Consumes network resources, installs malicious payloads, or crashes systems.
- **Self-replication:** Yes.
- **Examples:** SQL Slammer, WannaCry.

3. Trojan Horse

- **How it works:** Pretends to be legitimate software to trick the user. After installation, it opens a hidden backdoor.
- **Impact:** Remote access for attackers, data theft, installation of secondary malware.
- **Example:** Zeus Trojan.

Common Ports Used by Trojans

Port Number	Trojan Name	Port Number	Trojan Name
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari

Port Number	Trojan Name	Port Number	Trojan Name
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	NetBus	12345	Valvoline

4. Ransomware

- **How it works:** Encrypts user data and demands payment for decryption.
- **Impact:** Data loss, financial damage, downtime in critical sectors.
- **Common victims:** Healthcare, finance, government, education.
- **Examples:** WannaCry, REvil.

5. Spyware

- **How it works:** Silently monitors user actions, such as keystrokes and browsing.
- **Impact:** Identity theft, financial fraud, stolen credentials.
- **Examples:** Keyloggers, banking trojans.

6. Adware

- **How it works:** Bombards the system with ads or redirects traffic to unsafe sites.
- **Impact:** System slowdown, tracking, and potential malware entry points.
- **Example:** Fireball.

7. Rootkit

- **How it works:** Hides deep inside the system to mask malicious activity and give attackers privileged access.
- **Impact:** Bypasses security tools, steals data, enables long-term espionage.
- **Detection difficulty:** Very high.

8. Botnet (Bot + Network)

- **How it works:** Turns infected devices into remotely controlled bots.
- **Impact:** Used for large-scale DDoS attacks, spam campaigns, and spreading malware.
- **Example:** Mirai Botnet.

9. Fileless Malware

- **How it works:** Lives in RAM instead of the hard drive, leaving almost no trace.
- **Impact:** Difficult for traditional antivirus to detect.
- **Example:** PowerShell-based attacks.

10. Scareware

- **How it works:** Shows fake security alerts to trick users into buying bogus software.
- **Impact:** Financial loss and risk of installing real malware.
- **Example:** Fake antivirus pop-ups.

Common Malware Delivery Methods

- Phishing emails and malicious attachments
- Infected USB drives / removable media
- Drive-by downloads from compromised websites
- Fake software updates
- Cracked software & illegal downloads
- Social engineering and fake apps
- Vulnerability exploitation

Attacking Phase.

Gaining Access to the Target System Using the njRAT Trojan

What Is a Trojan?

A computer Trojan is a malicious program disguised as legitimate software. Unlike viruses or worms, it does not self-replicate. Instead, it relies on user interaction to execute. Once activated, a Trojan can give an attacker unauthorized access to the target system, allowing them to steal data, manipulate files, monitor user activity, or completely compromise system integrity. Classic trick, modern damage.

Lab Scenario Overview

In this lab scenario, attackers leverage social engineering and digital deception to gain access to a target system using a Trojan. The attacker crafts a file that appears harmless—such as a movie, document, or utility—but secretly contains malicious code. When the victim downloads and executes the file, the Trojan activates and silently performs its predefined actions.

njRAT Trojan: -

njRAT (also known as **Bladabindi**) is a powerful **Remote Access Trojan (RAT)** designed to give attackers unauthorized remote control over Windows systems. Once installed on a victim machine, it allows the attacker to monitor activities, steal data, execute commands, and manipulate system resources—all without the user's knowledge.

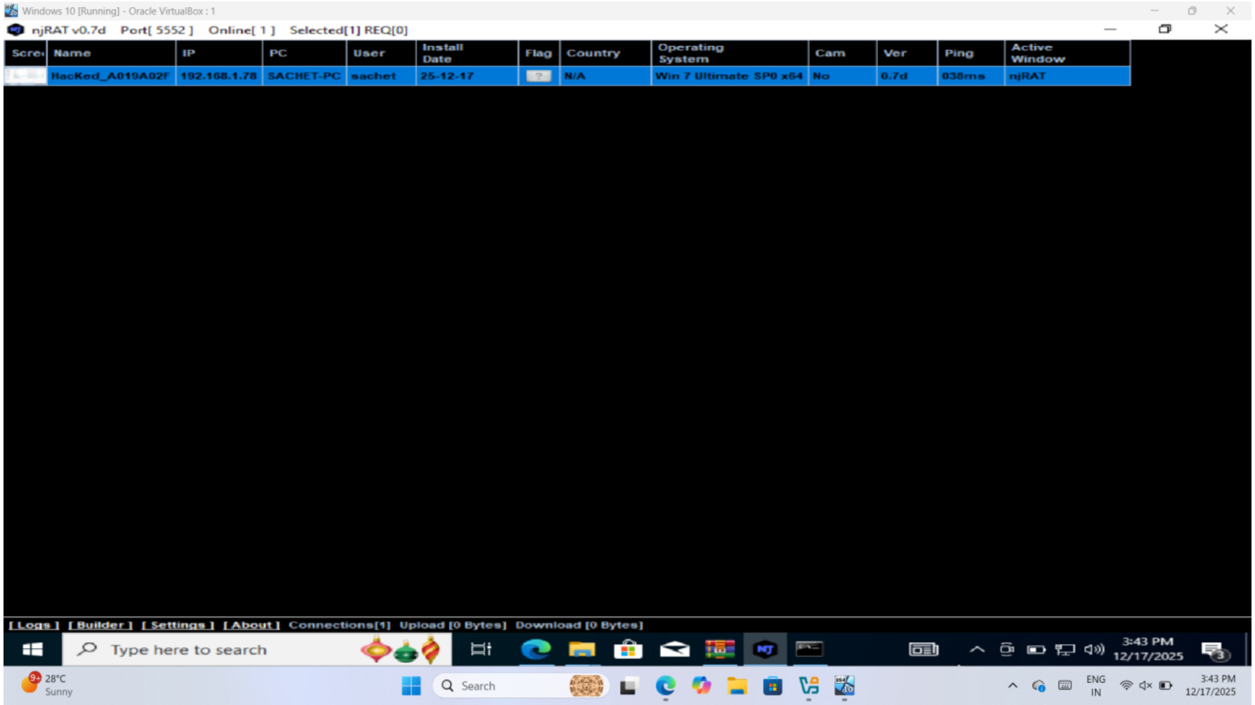
In this practical setup,

Attacker Machine: Windows 11

Target Machine: Windows 7

How to Download njRAT

1. Open a web browser on the attacker machine.
2. Search for: **“njRAT download GitHub”**
3. Download from the repository: **https://github.com/BlackAll9/NjRat.0.7D**
4. Open the main njRAT executable.
5. Start the program by selecting the “Start” option.
6. Proceed to the “Builder” section.
7. Now enter attacker machine (your machine ip) ip in host sections
8. Specify a name for the generated executable and click on build
9. Exe file created now share this folder or files to target machine
10. Return to the analyst machine to observe the connection within the evaluation setup.
11. Right-click inside the interface to access show options.
12. Open the manager panel to review the available controls.



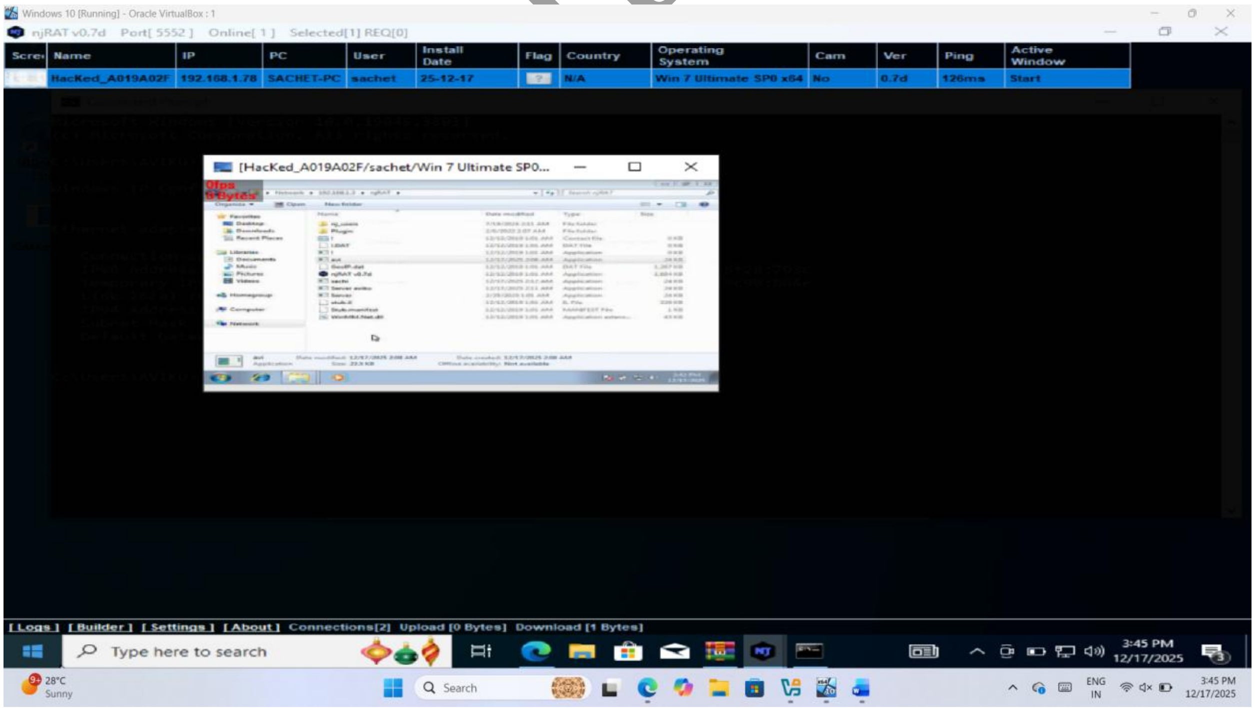
Windows 10 [Running] - Oracle VirtualBox : 1

njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]

Scre	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	HacKed_A019A02F	192.168.1.78	SACHET-PC	sachet	25-12-17	?	N/A	Win 7 Ultimate SP0 x64	No	0.7d	038ms	njRAT

[Logs] [Builder] [Settings] [About] Connections[1] Upload [0 Bytes] Download [0 Bytes]

13.Gaining Remote Access Done



Windows 10 [Running] - Oracle VirtualBox : 1

njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]

Scre	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	HacKed_A019A02F	192.168.1.78	SACHET-PC	sachet	25-12-17	?	N/A	Win 7 Ultimate SP0 x64	No	0.7d	126ms	Start

[HacKed_A019A02F/sachet/Win 7 Ultimate SP0...

[Logs] [Builder] [Settings] [About] Connections[2] Upload [0 Bytes] Download [1 Bytes]

Malware Analysis

Malware analysis refers to the detailed investigation of malicious software to understand how it works, where it came from, and what damage it can cause. The purpose is to uncover its functionality, identify its techniques, and determine how to detect, mitigate, or eliminate the threat effectively.

Types of Malware Analysis

1. **Static Malware Analysis**
2. **Dynamic Malware Analysis**

Static Malware Analysis

Static analysis focuses on studying the malware file *without actually running it*. In this method, an analyst reviews the file's internal structure—such as its code, embedded strings, headers, and metadata—to predict what the malware is designed to do.

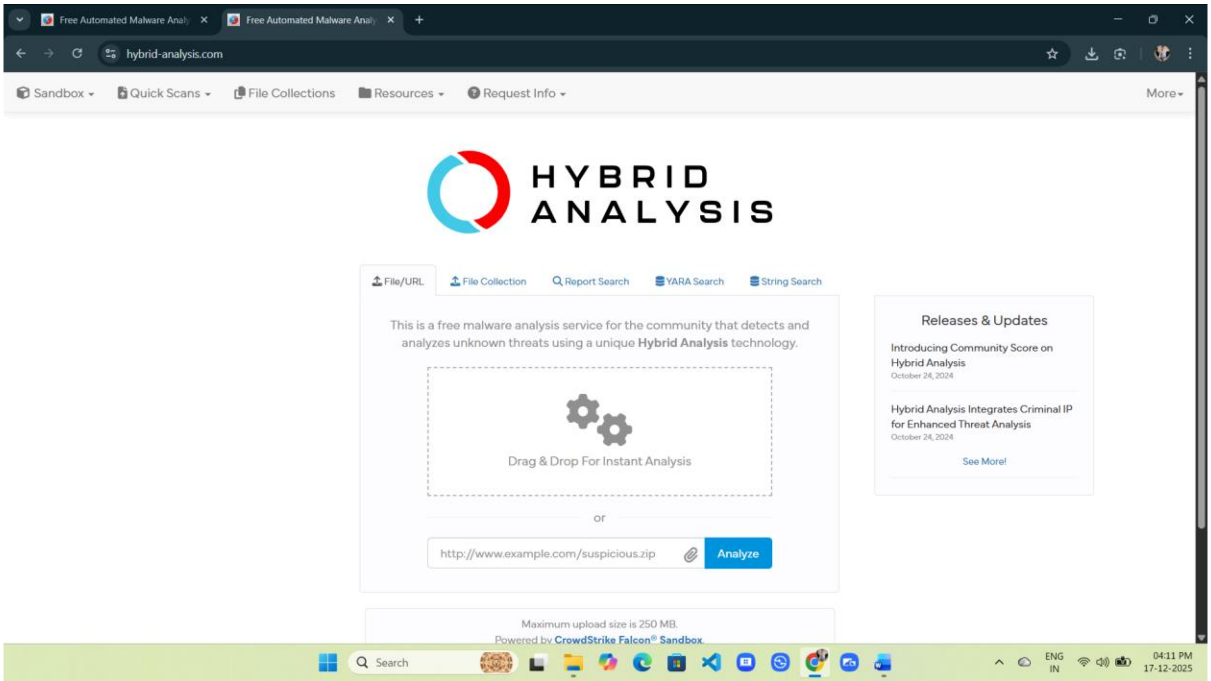
1. Static Analysis Using Hybrid Analysis Online Platform

To perform basic static checks, you can use online malware-analysis tools that automatically examine the file and generate reports.

How to use the Hybrid Analysis platform:

- Open any web browser and search for **"Hybrid Analysis"**.
- Go to the official site: https://www.hybrid-analysis.com/
- Upload the suspicious file for automatic static and behavioral inspection.

- Add file that you want to analys



This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

Drag & Drop For Instant Analysis

or

http://www.example.com/suspicious.zip | Analyze

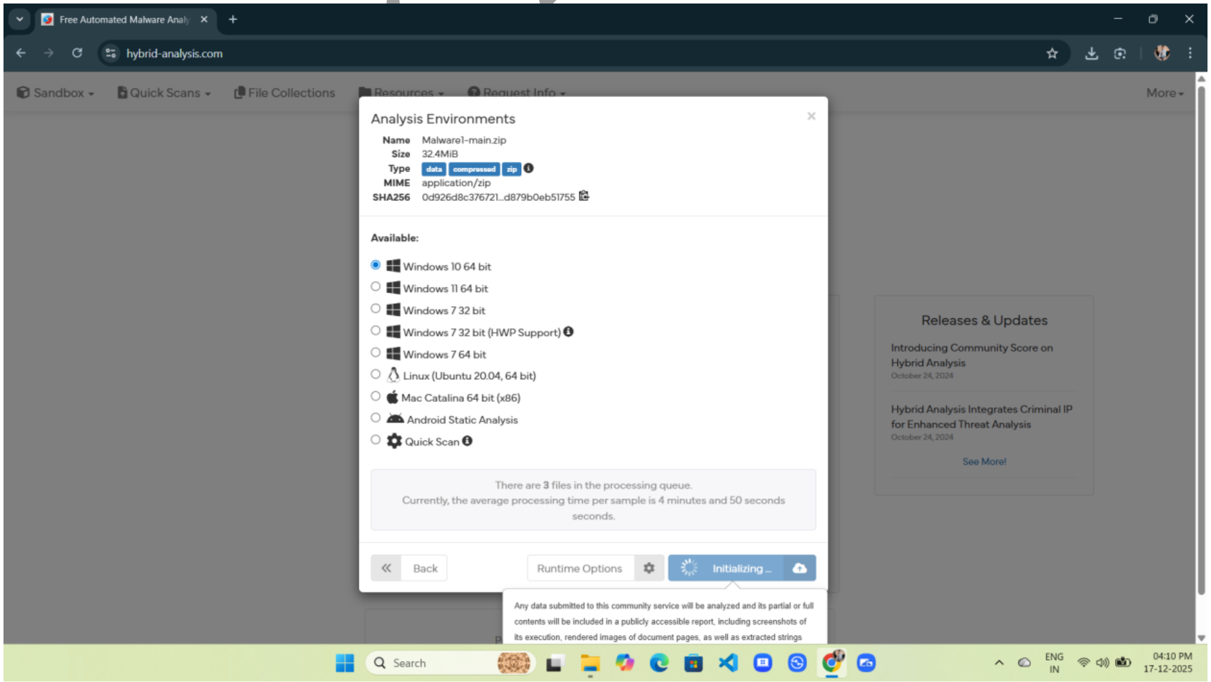
Maximum upload size is 250 MB.
Powered by CrowdStrike Falcon® Sandbox

Releases & Updates

Introducing Community Score on Hybrid Analysis
October 24, 2024

Hybrid Analysis Integrates Criminal IP for Enhanced Threat Analysis
October 24, 2024

See More!



Analysis Environments

Name	Malware1-main.zip
Size	32.4MiB
Type	data compressed zip
MIME	application/zip
SHA256	0d926d8c376721...d879b0eb51755

Available:

- ● Windows 10 64 bit
- ○ Windows 11 64 bit
- ○ Windows 7 32 bit
- ○ Windows 7 32 bit (HWP Support)
- ○ Windows 7 64 bit
- ○ Linux (Ubuntu 20.04, 64 bit)
- ○ Mac Catalina 64 bit (x86)
- ○ Android Static Analysis
- ○ Quick Scan

There are **3** files in the processing queue.
Currently, the average processing time per sample is 4 minutes and 50 seconds seconds.

Any data submitted to this community service will be analyzed and its partial or full contents will be included in a publicly accessible report, including screenshots of its execution, rendered images of document pages, as well as extracted strings

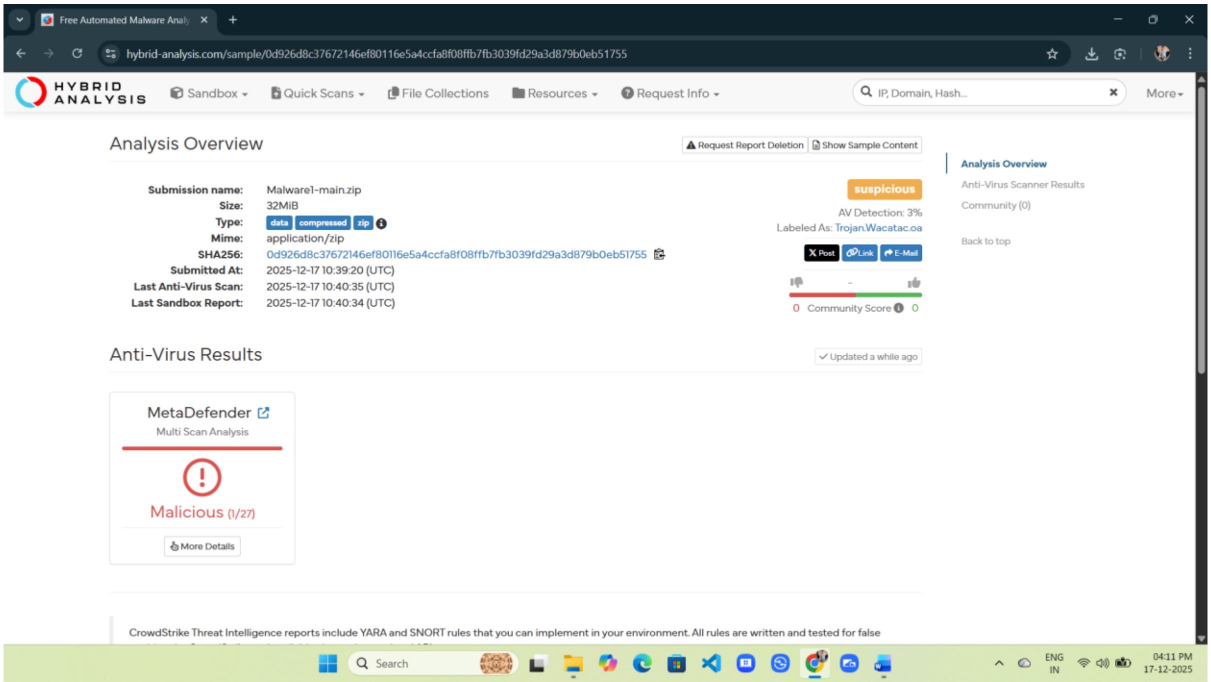
Releases & Updates

Introducing Community Score on Hybrid Analysis
October 24, 2024

Hybrid Analysis Integrates Criminal IP for Enhanced Threat Analysis
October 24, 2024

See More!

- Here scan completed and it is a malicious file


hybrid-analysis.com/sample/0d926d8c37672146ef80116e5a4ccfa8f08ffb7fb3039fd29a3d879b0eb51755

Analysis Overview

Submission name:	Malware1-main.zip
Size:	32MiB
Type:	data compressed zip
Mime:	application/zip
SHA256:	0d926d8c37672146ef80116e5a4ccfa8f08ffb7fb3039fd29a3d879b0eb51755
Submitted At:	2025-12-17 10:39:20 (UTC)
Last Anti-Virus Scan:	2025-12-17 10:40:35 (UTC)
Last Sandbox Report:	2025-12-17 10:40:34 (UTC)

suspicious

AV Detection: 3%

Labeled As: Trojan.Wacatac.oa

0 Community Score 0

Anti-Virus Results

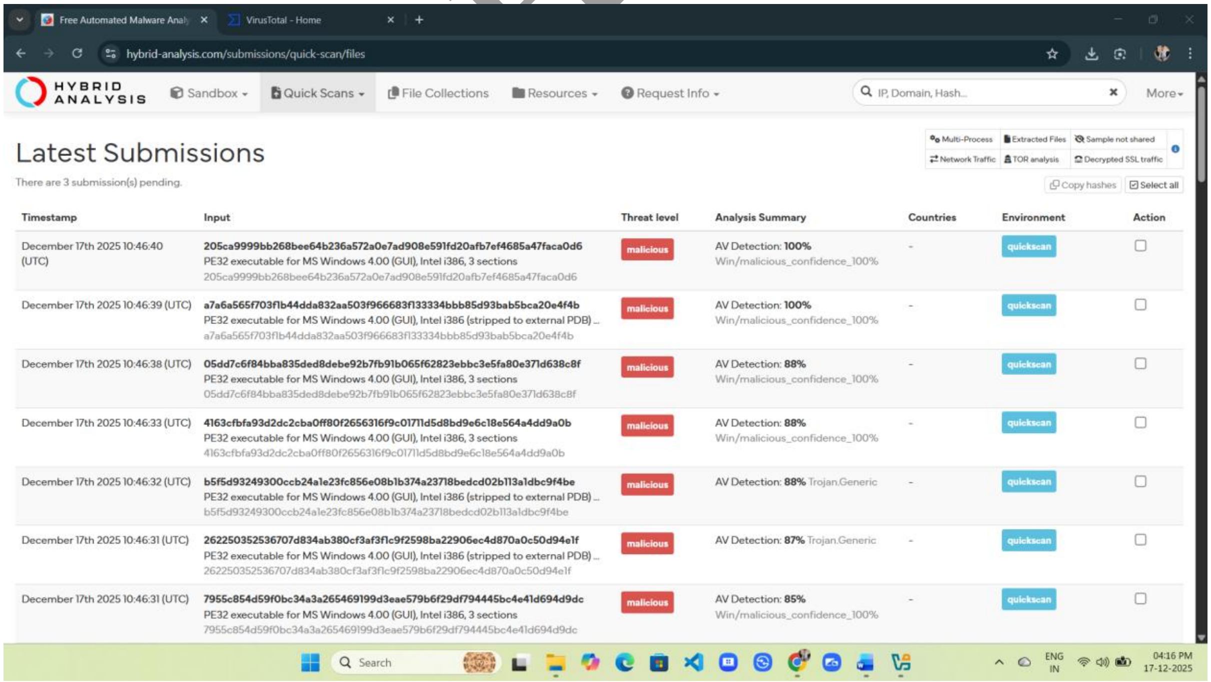
✓ Updated a while ago

MetaDefender

Multi Scan Analysis

Malicious (1/27)

CrowdStrike Threat Intelligence reports include YARA and SNORT rules that you can implement in your environment. All rules are written and tested for false


hybrid-analysis.com/submissions/quick-scan/files

Latest Submissions

There are 3 submission(s) pending.

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
December 17th 2025 10:46:40 (UTC)	**205ca9999bb268bee64b236a572a0e7ad908e591fd20afb7ef4685a47faca0d6** PE32 executable for MS Windows 4.00 (GUI), Intel i386, 3 sections 205ca9999bb268bee64b236a572a0e7ad908e591fd20afb7ef4685a47faca0d6	malicious	AV Detection: **100%** Win/malicious_confidence_100%	-	quickscan	□
December 17th 2025 10:46:39 (UTC)	**a7a6a565f703f1b44dda832aa503f966683f133334bbb85d93bab5bca20e4f4b** PE32 executable for MS Windows 4.00 (GUI), Intel i386 (stripped to external PDB) ... a7a6a565f703f1b44dda832aa503f966683f133334bbb85d93bab5bca20e4f4b	malicious	AV Detection: **100%** Win/malicious_confidence_100%	-	quickscan	□
December 17th 2025 10:46:38 (UTC)	**05dd7c6f84bba835ded8debe92b7fb91b065f62823ebbc3e5fa80e371d638c8f** PE32 executable for MS Windows 4.00 (GUI), Intel i386, 3 sections 05dd7c6f84bba835ded8debe92b7fb91b065f62823ebbc3e5fa80e371d638c8f	malicious	AV Detection: **88%** Win/malicious_confidence_100%	-	quickscan	□
December 17th 2025 10:46:33 (UTC)	**4163cfbfa93d2dc2cba0ff80f2656316f9c01711d5d8bd9e6c18e564a4dd9a0b** PE32 executable for MS Windows 4.00 (GUI), Intel i386, 3 sections 4163cfbfa93d2dc2cba0ff80f2656316f9c01711d5d8bd9e6c18e564a4dd9a0b	malicious	AV Detection: **88%** Win/malicious_confidence_100%	-	quickscan	□
December 17th 2025 10:46:32 (UTC)	**b5f5d93249300ccb24a1e23fc856e08b1b374a23718bedcd02b113a1dbc9f4be** PE32 executable for MS Windows 4.00 (GUI), Intel i386 (stripped to external PDB) ... b5f5d93249300ccb24a1e23fc856e08b1b374a23718bedcd02b113a1dbc9f4be	malicious	AV Detection: **88%** Trojan.Generic	-	quickscan	□
December 17th 2025 10:46:31 (UTC)	**262250352536707d834ab380cf3af3f1c9f2598ba22906ec4d870a0c50d94e1f** PE32 executable for MS Windows 4.00 (GUI), Intel i386 (stripped to external PDB) ... 262250352536707d834ab380cf3af3f1c9f2598ba22906ec4d870a0c50d94e1f	malicious	AV Detection: **87%** Trojan.Generic	-	quickscan	□
December 17th 2025 10:46:31 (UTC)	**7955c854d59f0bc34a3a265469199d3eae579b6f29df794445bc4e41d694d9dc** PE32 executable for MS Windows 4.00 (GUI), Intel i386, 3 sections 7955c854d59f0bc34a3a265469199d3eae579b6f29df794445bc4e41d694d9dc	malicious	AV Detection: **85%** Win/malicious_confidence_100%	-	quickscan	□

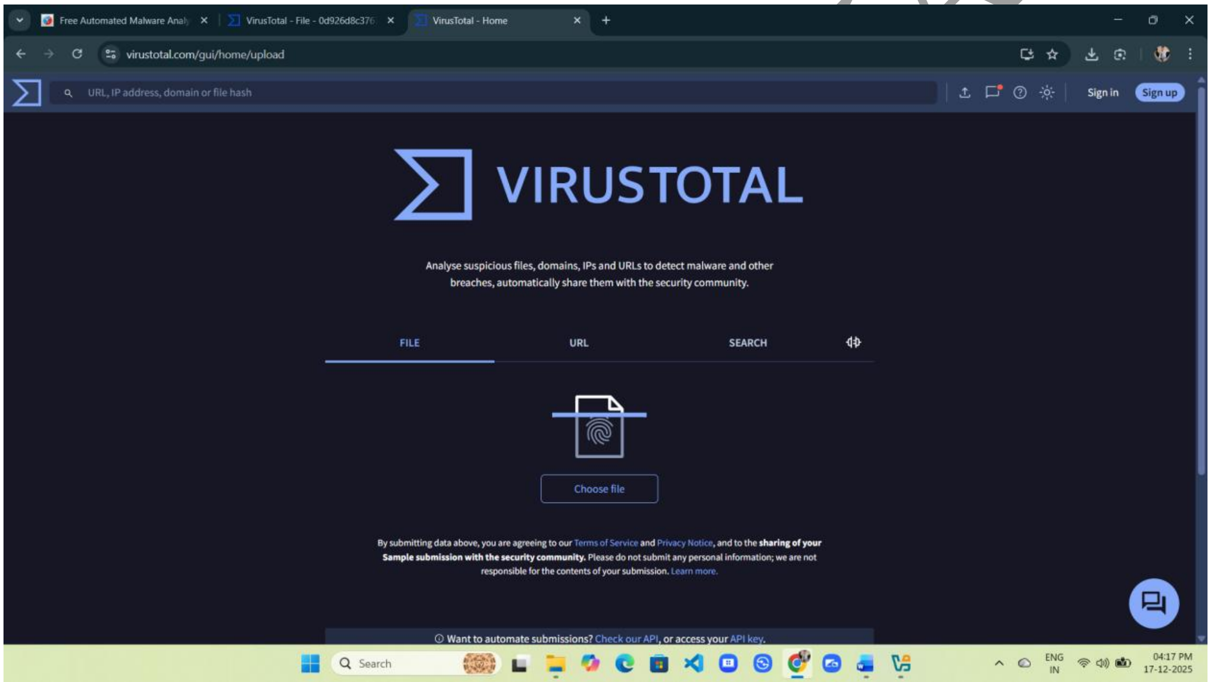
2.Static Malware Analysis Using Virus Total (Website)

How to use it -:

- Open Browser and search Virus Total

  Website -: https://www.virustotal.com/gui/home/upload

- Now, choose a file that want to scan



virustotal.com/gui/home/upload

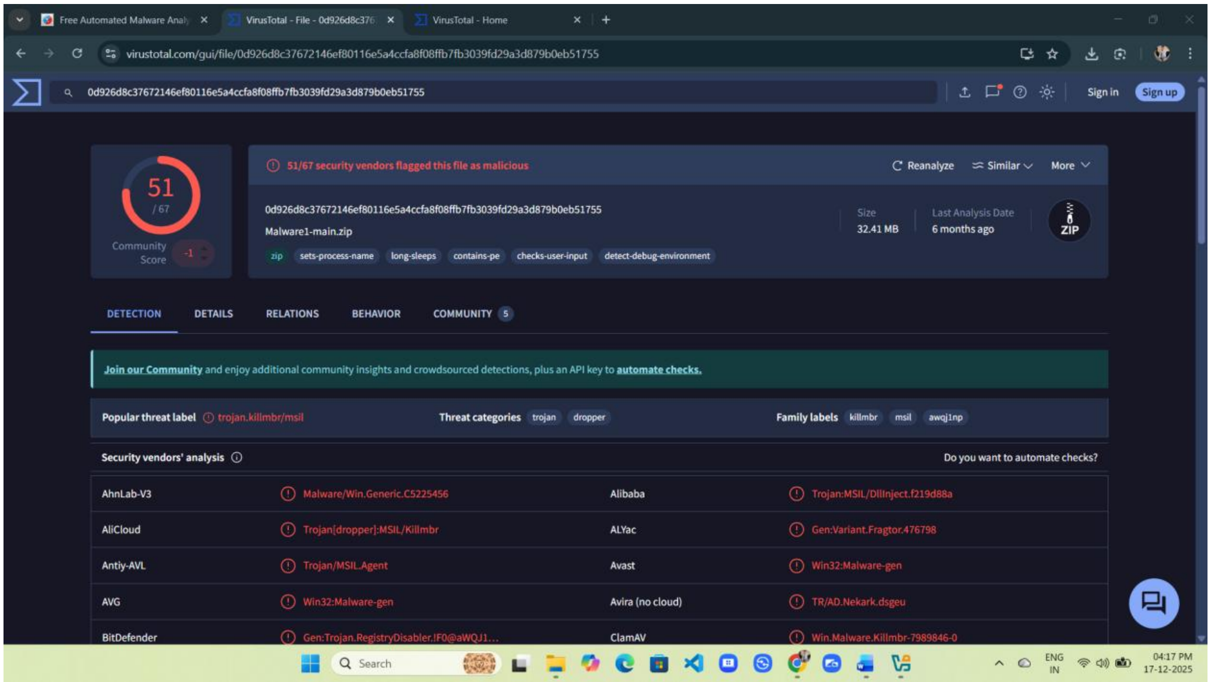
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, or access your API key.

Free Automated Malware Analy
VirusTotal - File - 0d926d8c376
VirusTotal - Home
URL, IP address, domain or file hash
Sign in
Sign up
VIRUSTOTAL
FILE
URL
SEARCH
Choose file
Search
ENG
IN
04:17 PM
17-12-2025

- Here scan completed and it is a malicious file



Free Automated Malware Analy
VirusTotal - File - 0d926d8c376
VirusTotal - Home
virustotal.com/gui/file/0d926d8c37672146ef80116e5a4ccfa8f08ffb7fb3039fd29a3d879b0eb51755
0d926d8c37672146ef80116e5a4ccfa8f08ffb7fb3039fd29a3d879b0eb51755
Sign in
Sign up

51 / 67

Community Score -1

51/67 security vendors flagged this file as malicious

0d926d8c37672146ef80116e5a4ccfa8f08ffb7fb3039fd29a3d879b0eb51755

Malware1-main.zip

zip sets-process-name long-sleeps contains-pe checks-user-input detect-debug-environment

Size 32.41 MB

Last Analysis Date 6 months ago

ZIP
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 5

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

Popular threat label trojan.killmbr/msil

Threat categories trojan dropper

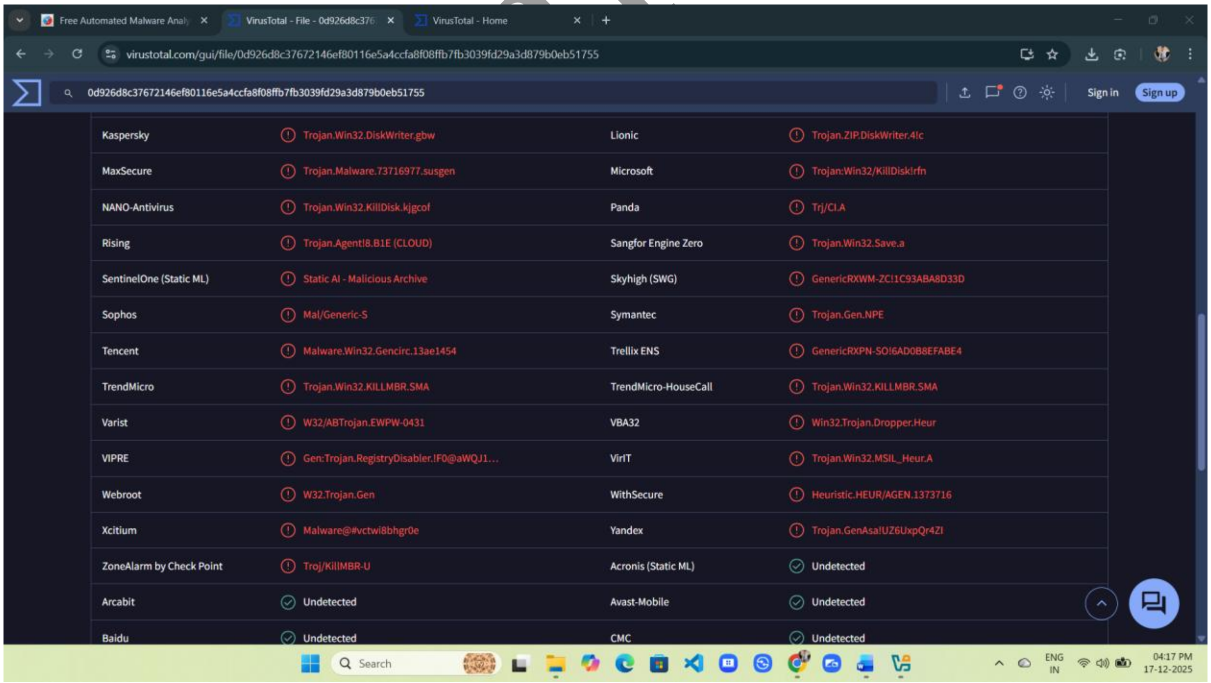
Family labels killmbr msil awqj1np

Security vendors' analysis

Do you want to automate checks?

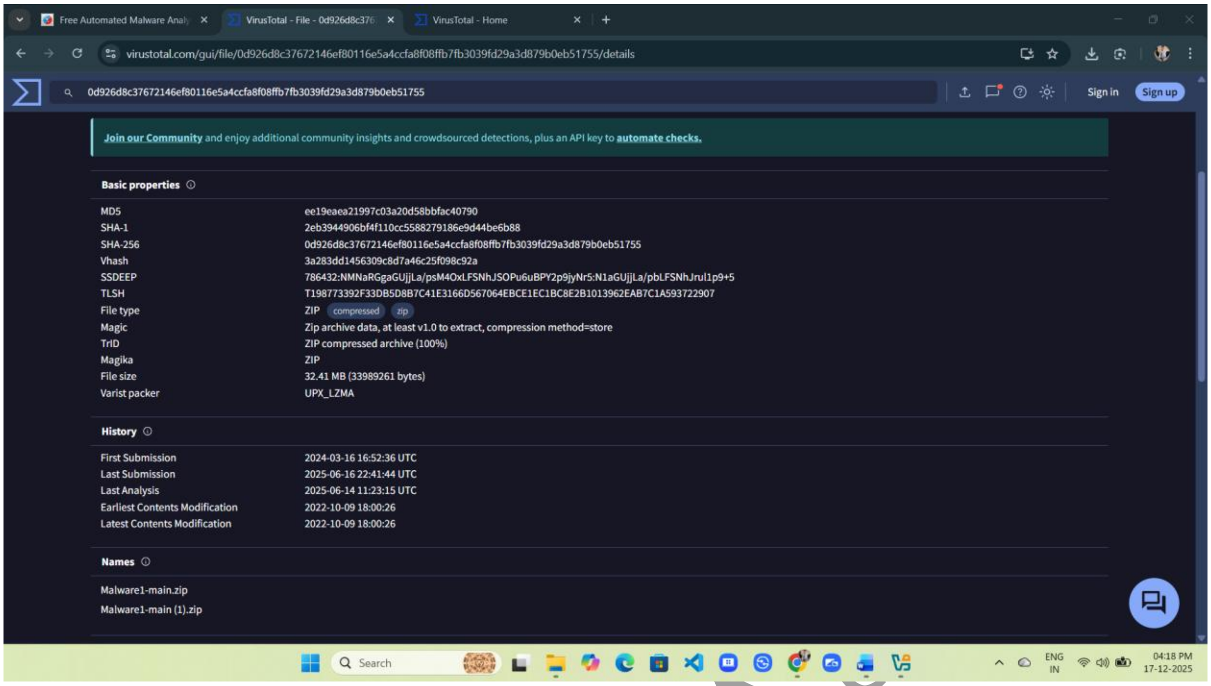
AhnLab-V3	Malware/Win.Generic.C5225456	Alibaba	Trojan:MSIL/DllInject.f219d88a
AliCloud	Trojan[dropper]:MSIL/Killmbr	ALYac	Gen:Variant.Fragtor.476798
Antiy-AVL	Trojan/MSIL.Agent	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/AD.Nekark.dsgeu
BitDefender	Gen:Trojan.RegistryDisabler.!F0@aWQJ1…	ClamAV	Win.Malware.Killmbr-7989846-0

Search
ENG
IN
04:17 PM
17-12-2025



Free Automated Malware Analy
VirusTotal - File - 0d926d8c376
VirusTotal - Home
virustotal.com/gui/file/0d926d8c37672146ef80116e5a4ccfa8f08ffb7fb3039fd29a3d879b0eb51755
0d926d8c37672146ef80116e5a4ccfa8f08ffb7fb3039fd29a3d879b0eb51755
Sign in
Sign up

Kaspersky	Trojan.Win32.DiskWriter.gbw	Lionic	Trojan.ZIP.DiskWriter.4!c
MaxSecure	Trojan.Malware.73716977.susgen	Microsoft	Trojan:Win32/KillDisk!rfn
NANO-Antivirus	Trojan.Win32.KillDisk.kjgcof	Panda	Trj/CI.A
Rising	Trojan.Agent!8.B1E (CLOUD)	Sangfor Engine Zero	Trojan.Win32.Save.a
SentinelOne (Static ML)	Static AI - Malicious Archive	Skyhigh (SWG)	GenericRXWM-ZC!1C93ABA8D33D
Sophos	Mal/Generic-S	Symantec	Trojan.Gen.NPE
Tencent	Malware.Win32.Gencirc.13ae1454	Trellix ENS	GenericRXPN-SO!6AD0B8EFABE4
TrendMicro	Trojan.Win32.KILLMBR.SMA	TrendMicro-HouseCall	Trojan.Win32.KILLMBR.SMA
Varist	W32/ABTrojan.EWPW-0431	VBA32	Win32.Trojan.Dropper.Heur
VIPRE	Gen:Trojan.RegistryDisabler.!F0@aWQJ1…	VirIT	Trojan.Win32.MSIL_Heur.A
Webroot	W32.Trojan.Gen	WithSecure	Heuristic.HEUR/AGEN.1373716
Xcitium	Malware@#vctwi8bhgr0e	Yandex	Trojan.GenAsa!UZ6UxpQr4ZI
ZoneAlarm by Check Point	Troj/KillMBR-U	Acronis (Static ML)	Undetected
Arcabit	Undetected	Avast-Mobile	Undetected
Baidu	Undetected	CMC	Undetected



Free Automated Malware Analy
VirusTotal - File - 0d926d8c376
VirusTotal - Home
virustotal.com/gui/file/0d926d8c37672146ef80116e5a4ccfa8f08ffb7fb3039fd29a3d879b0eb51755/details
0d926d8c37672146ef80116e5a4ccfa8f08ffb7fb3039fd29a3d879b0eb51755
Sign in
Sign up

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

Basic properties

MD5	ee19eaea21997c03a20d58bbfac40790
SHA-1	2eb3944906bf4f110cc5588279186e9d44be6b88
SHA-256	0d926d8c37672146ef80116e5a4ccfa8f08ffb7fb3039fd29a3d879b0eb51755
Vhash	3a283dd1456309c8d7a46c25f098c92a
SSDEEP	786432:NMNaRGgaGUjjLa/psM4OxLFSNhJSOPu6uBPY2p9jyNr5:N1aGUjjLa/pbLFSNhJrul1p9+5
TLSH	T198773392F33DB5D8B7C41E3166D567064EBCE1EC1BC8E2B1013962EAB7C1A593722907
File type	ZIP compressed zip
Magic	Zip archive data, at least v1.0 to extract, compression method=store
TrID	ZIP compressed archive (100%)
Magika	ZIP
File size	32.41 MB (33989261 bytes)
Varist packer	UPX_LZMA

History

First Submission	2024-03-16 16:52:36 UTC
Last Submission	2025-06-16 22:41:44 UTC
Last Analysis	2025-06-14 11:23:15 UTC
Earliest Contents Modification	2022-10-09 18:00:26
Latest Contents Modification	2022-10-09 18:00:26

Names

Malware1-main.zip

Malware1-main (1).zip

3.Static Malware Analysis Using Detect It Easy (DIE)

Definition

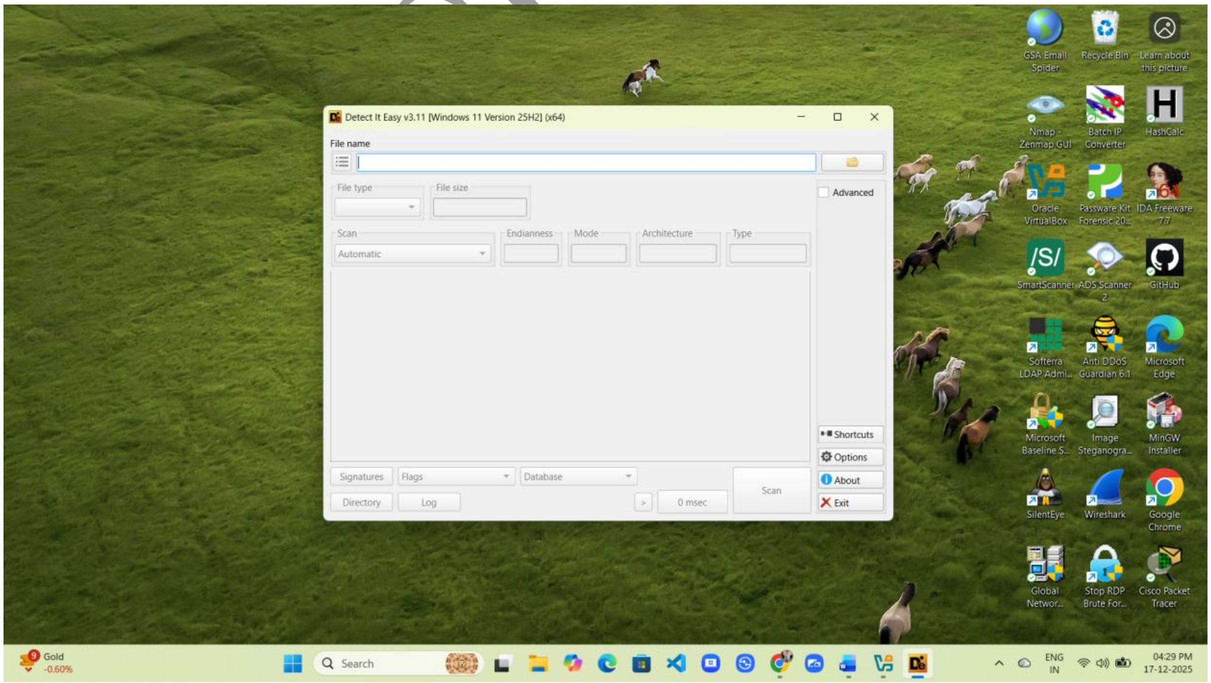
Static malware analysis is the art of understanding a suspicious file **without executing it**. No running, no detonating—just observation. Detect It Easy (DIE) is a lightweight analysis tool used to identify file type, compiler, packer, and basic characteristics of malware samples. Think of it as reading the enemy's diary without waking them up.

Working

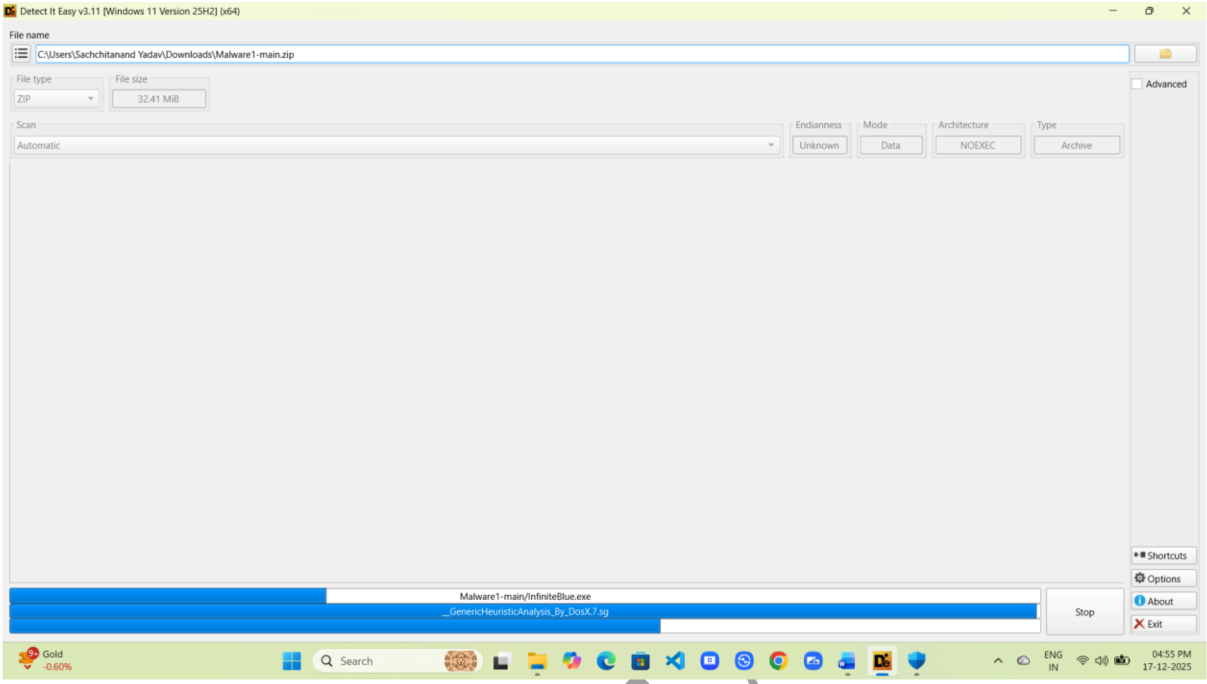
DIE scans the malware sample and analyzes its internal structure. It looks for signatures, entropy levels, and known packers to determine how the file was built and whether it's obfuscated or compressed. Since the file is never executed, the system stays safe—old-school caution, modern efficiency.

Steps

1. Launch Detect It Easy (DIE) on the analysis system.



2. Load the suspicious executable file into the tool.



Detect It Easy v3.11 [Windows 11 Version 25H2] (x64)

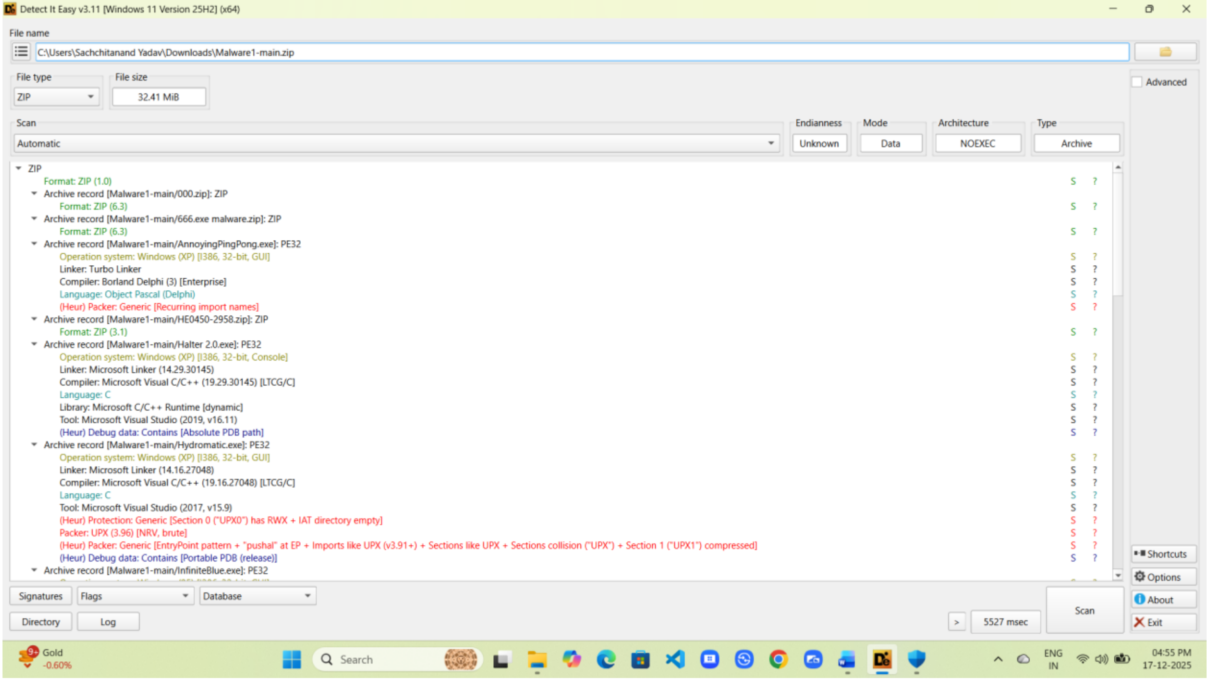
File name: C:\Users\Sachchitanand Yadav\Downloads\Malware1-main.zip

File type: ZIP | File size: 32.41 MiB

Scan: Automatic | Endianness: Unknown | Mode: Data | Architecture: NOEXEC | Type: Archive

```
Malware1-main/InfiniteBlue.exe
_GenericHeuristicAnalysis_By_DosX.7.sg
```

3. Examine detected information such as file format, compiler, packer, and entropy.



Detect It Easy v3.11 [Windows 11 Version 25H2] (x64)

File name: C:\Users\Sachchitanand Yadav\Downloads\Malware1-main.zip

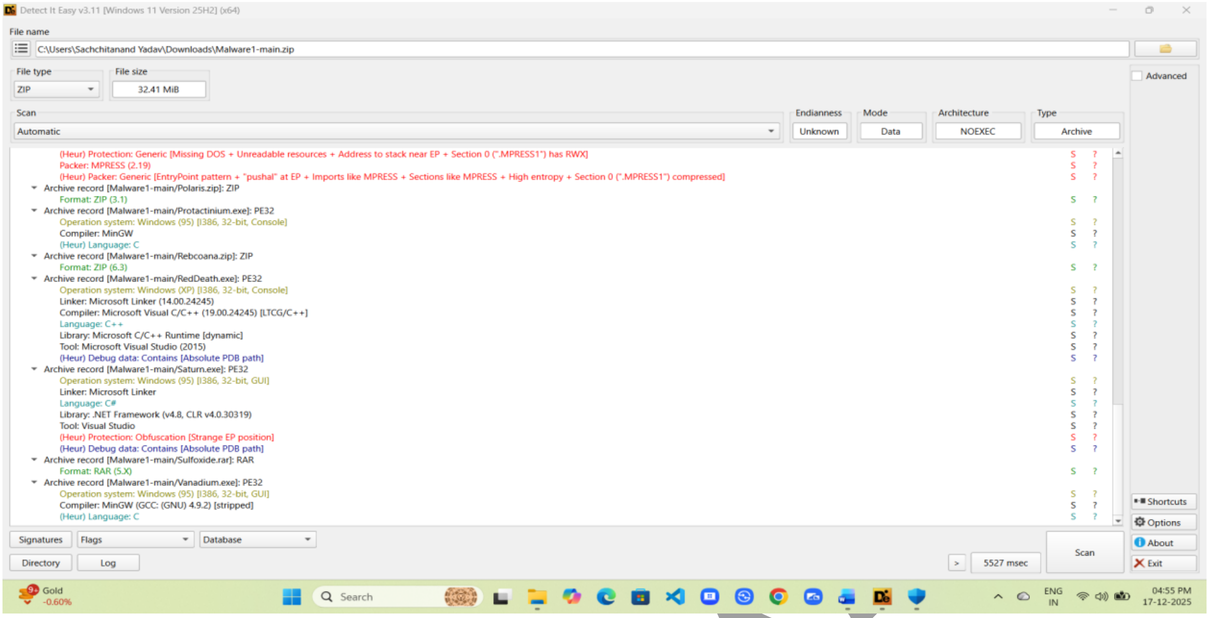
File type: ZIP | File size: 32.41 MiB

Scan: Automatic | Endianness: Unknown | Mode: Data | Architecture: NOEXEC | Type: Archive

```
ZIP
    Format: ZIP (1.0)
  Archive record [Malware1-main/000.zip]: ZIP
      Format: ZIP (6.3)
  Archive record [Malware1-main/666.exe malware.zip]: ZIP
      Format: ZIP (6.3)
  Archive record [Malware1-main/AnnoyingPingPong.exe]: PE32
      Operation system: Windows (XP) [I386, 32-bit, GUI]
      Linker: Turbo Linker
      Compiler: Borland Delphi (3) [Enterprise]
      Language: Object Pascal (Delphi)
      (Heur) Packer: Generic [Recurring import names]
  Archive record [Malware1-main/HE0450-2958.zip]: ZIP
      Format: ZIP (3.1)
  Archive record [Malware1-main/Halter 2.0.exe]: PE32
      Operation system: Windows (XP) [I386, 32-bit, Console]
      Linker: Microsoft Linker (14.29.30145)
      Compiler: Microsoft Visual C/C++ (19.29.30145) [LTCG/C]
      Language: C
      Library: Microsoft C/C++ Runtime [dynamic]
      Tool: Microsoft Visual Studio (2019, v16.11)
      (Heur) Debug data: Contains [Absolute PDB path]
  Archive record [Malware1-main/Hydromatic.exe]: PE32
      Operation system: Windows (XP) [I386, 32-bit, GUI]
      Linker: Microsoft Linker (14.16.27048)
      Compiler: Microsoft Visual C/C++ (19.16.27048) [LTCG/C]
      Language: C
      Tool: Microsoft Visual Studio (2017, v15.9)
      (Heur) Protection: Generic [Section 0 ("UPX0") has RWX + IAT directory empty]
      Packer: UPX (3.96) [NRV, brute]
      (Heur) Packer: Generic [EntryPoint pattern + "pushal" at EP + Imports like UPX (v3.91+) + Sections like UPX + Sections collision ("UPX") + Section 1 ("UPX1") compressed]
      (Heur) Debug data: Contains [Portable PDB (release)]
  Archive record [Malware1-main/InfiniteBlue.exe]: PE32
```

5527 msec

4. Analyze results to understand whether the file is packed or potentially malicious.



Detect It Easy v3.11 [Windows 11 Version 25H2] (x64)

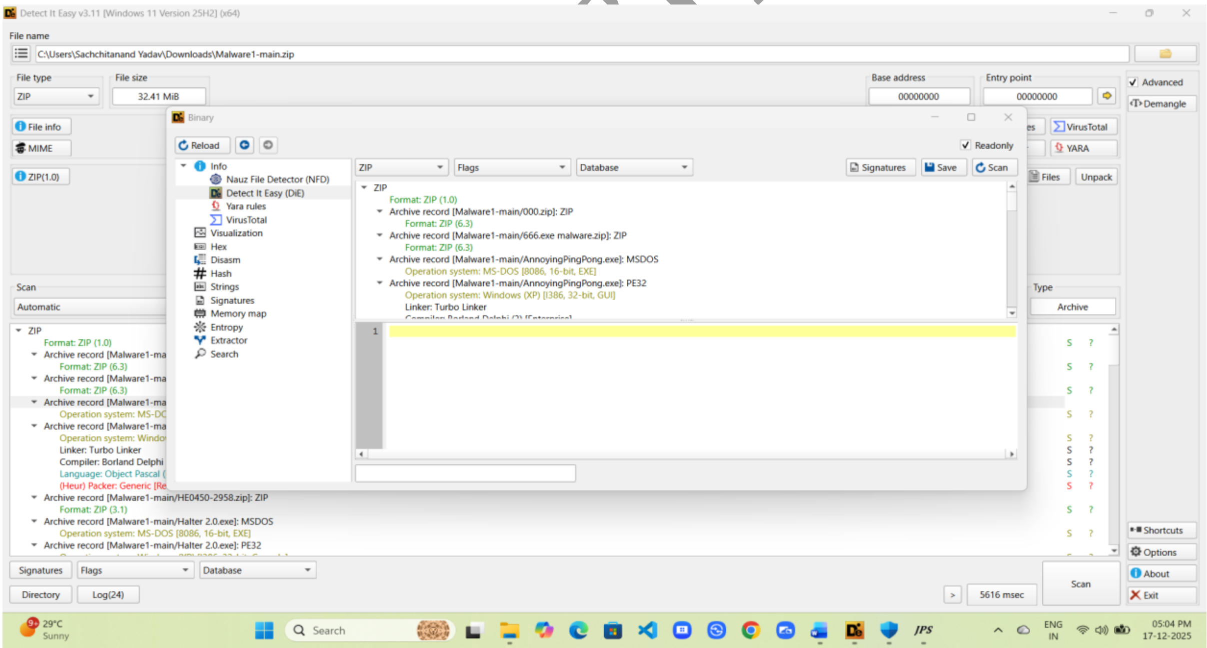
File name: C:\Users\Sachchitanand Yadav\Downloads\Malware1-main.zip

File type: ZIP | File size: 32.41 MiB

Scan: Automatic | Endianness: Unknown | Mode: Data | Architecture: NOEXEC | Type: Archive

```
        (Heur) Protection: Generic [Missing DOS + Unreadable resources + Address to stack near EP + Section 0 (".MPRESS1") has RWX]
        Packer: MPRESS (2.19)
        (Heur) Packer: Generic [EntryPoint pattern + "pushal" at EP + Imports like MPRESS + Sections like MPRESS + High entropy + Section 0 (".MPRESS1") compressed]
    Archive record [Malware1-main/Polaris.zip]: ZIP
        Format: ZIP (3.1)
    Archive record [Malware1-main/Protactinium.exe]: PE32
        Operation system: Windows (95) [I386, 32-bit, Console]
        Compiler: MinGW
        (Heur) Language: C
    Archive record [Malware1-main/Rebcoana.zip]: ZIP
        Format: ZIP (6.3)
    Archive record [Malware1-main/RedDeath.exe]: PE32
        Operation system: Windows (XP) [I386, 32-bit, Console]
        Linker: Microsoft Linker (14.00.24245)
        Compiler: Microsoft Visual C/C++ (19.00.24245) [LTCG/C++]
        Language: C++
        Library: Microsoft C/C++ Runtime [dynamic]
        Tool: Microsoft Visual Studio (2015)
        (Heur) Debug data: Contains [Absolute PDB path]
    Archive record [Malware1-main/Saturn.exe]: PE32
        Operation system: Windows (95) [I386, 32-bit, GUI]
        Linker: Microsoft Linker
        Language: C#
        Library: .NET Framework (v4.8, CLR v4.0.30319)
        Tool: Visual Studio
        (Heur) Protection: Obfuscation [Strange EP position]
        (Heur) Debug data: Contains [Absolute PDB path]
    Archive record [Malware1-main/Sulfoxide.rar]: RAR
        Format: RAR (5.X)
    Archive record [Malware1-main/Vanadium.exe]: PE32
        Operation system: Windows (95) [I386, 32-bit, GUI]
        Compiler: MinGW (GCC: (GNU) 4.9.2) [stripped]
        (Heur) Language: C
```

5. Document findings for further investigation or reporting.



Detect It Easy v3.11 [Windows 11 Version 25H2] (x64)

File name: C:\Users\Sachchitanand Yadav\Downloads\Malware1-main.zip

File type: ZIP | File size: 32.41 MiB | Base address: 00000000 | Entry point: 00000000

☑ Advanced

Binary

☑ Readonly

```
ZIP
    Format: ZIP (1.0)
    Archive record [Malware1-main/000.zip]: ZIP
        Format: ZIP (6.3)
    Archive record [Malware1-main/666.exe malware.zip]: ZIP
        Format: ZIP (6.3)
    Archive record [Malware1-main/AnnoyingPingPong.exe]: MSDOS
        Operation system: MS-DOS [8086, 16-bit, EXE]
    Archive record [Malware1-main/AnnoyingPingPong.exe]: PE32
        Operation system: Windows (XP) [I386, 32-bit, GUI]
        Linker: Turbo Linker
```

```
ZIP
    Format: ZIP (1.0)
    Archive record [Malware1-ma
        Format: ZIP (6.3)
    Archive record [Malware1-ma
        Format: ZIP (6.3)
    Archive record [Malware1-ma
        Operation system: MS-DC
    Archive record [Malware1-ma
        Operation system: Windo
        Linker: Turbo Linker
        Compiler: Borland Delphi
        Language: Object Pascal (
        (Heur) Packer: Generic [Re
    Archive record [Malware1-main/HE0450-2958.zip]: ZIP
        Format: ZIP (3.1)
    Archive record [Malware1-main/Halter 2.0.exe]: MSDOS
        Operation system: MS-DOS [8086, 16-bit, EXE]
    Archive record [Malware1-main/Halter 2.0.exe]: PE32
```

Conclusion

Static analysis using DIE provides a safe and effective first look into malware behavior. It helps analysts identify threats early without risking system infection. The lesson is simple and timeless: observe before you act—because smart defense always starts with understanding.

4. Perform Malware Disassembly Using IDA

Definition

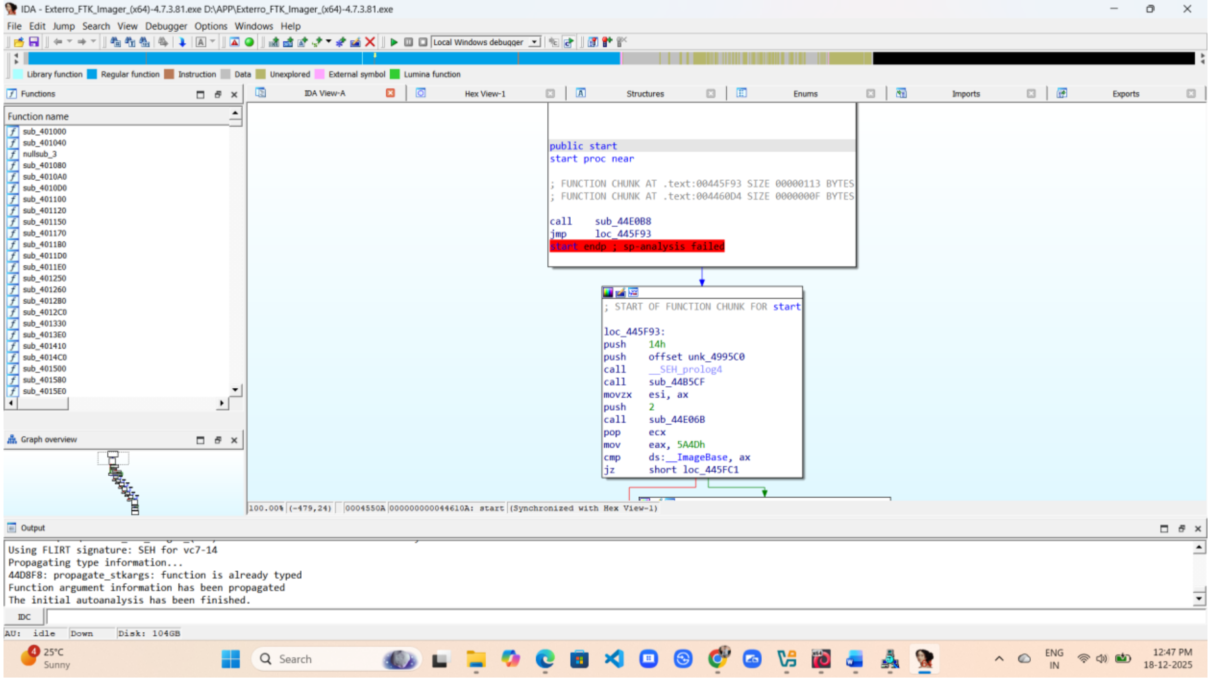
Malware disassembly is a static analysis technique used to study malicious programs by converting machine code into human-readable assembly code. IDA (Interactive Disassembler) is a widely used professional tool that helps analysts understand a program’s internal logic **without executing it**.

Working

IDA analyzes the binary file and breaks it down into assembly instructions, functions, and code flow graphs. It allows analysts to trace program behavior, identify suspicious routines, API calls, and hidden logic. Since the malware is not run, the system remains safe—slow, careful analysis over reckless execution. Tradition wins.

Steps

1. Open IDA on a secure analysis system.
2. Load the suspicious executable file.
3. Allow IDA to analyze and disassemble the binary automatically.
4. Review functions, strings, and code flow to identify malicious behavior.
5. Note important findings for documentation and further analysis.



IDA - Exterro_FTK_Imager_(x64)-4.7.3.81.exe D:\APP\Exterro_FTK_Imager_(x64)-4.7.3.81.exe

```
sub_401000
sub_401040
nullsub_3
sub_401080
sub_4010A0
sub_4010D0
sub_401100
sub_401120
sub_401150
sub_401170
sub_4011B0
sub_4011D0
sub_4011E0
sub_401250
sub_401260
sub_4012B0
sub_4012C0
sub_401330
sub_4013E0
sub_401410
sub_4014C0
sub_401500
sub_401580
sub_4015E0
```

```
public start
start proc near

; FUNCTION CHUNK AT .text:00445F93 SIZE 00000113 BYTES
; FUNCTION CHUNK AT .text:004460D4 SIZE 0000000F BYTES

call    sub_44E0B8
jmp     loc_445F93
start endp ; sp-analysis failed
```

```
; START OF FUNCTION CHUNK FOR start

loc_445F93:
push    14h
push    offset unk_4995C0
call    __SEH_prolog4
call    sub_44B5CF
movzx   esi, ax
push    2
call    sub_44E06B
pop     ecx
mov     eax, 5A4Dh
cmp     ds:__ImageBase, ax
jz      short loc_445FC1
```

```
100.00% (-479,24)  0004550A 000000000044610A: start (Synchronized with Hex View-1)
```

```
Using FLIRT signature: SEH for vc7-14
Propagating type information...
44D8F8: propagate_stkargs: function is already typed
Function argument information has been propagated
The initial autoanalysis has been finished.
```

```
AU:  idle   Down    Disk: 104GB
```

12:47 PM
18-12-2025

Conclusion

Malware disassembly using IDA provides deep insight into how malicious programs are structured and operate internally. It is a powerful technique for understanding threats, strengthening defenses, and improving incident response—proof that real security starts with patience, precision, and respect for fundamentals.

Dynamic Malware Analysis

Dynamic malware analysis involves running the suspicious file inside a controlled, isolated environment (sandbox or virtual machine) to directly observe how it behaves. This approach reveals its real-time actions, such as system changes, network activity, or process creation.

Working

Once executed, the malware interacts with the system as it normally would. Analysts monitor changes such as file creation, registry modification, process spawning, and network communication. Unlike static analysis, this method shows what the malware **actually does**, not just what it could do.

Process Monitoring Using TCPView

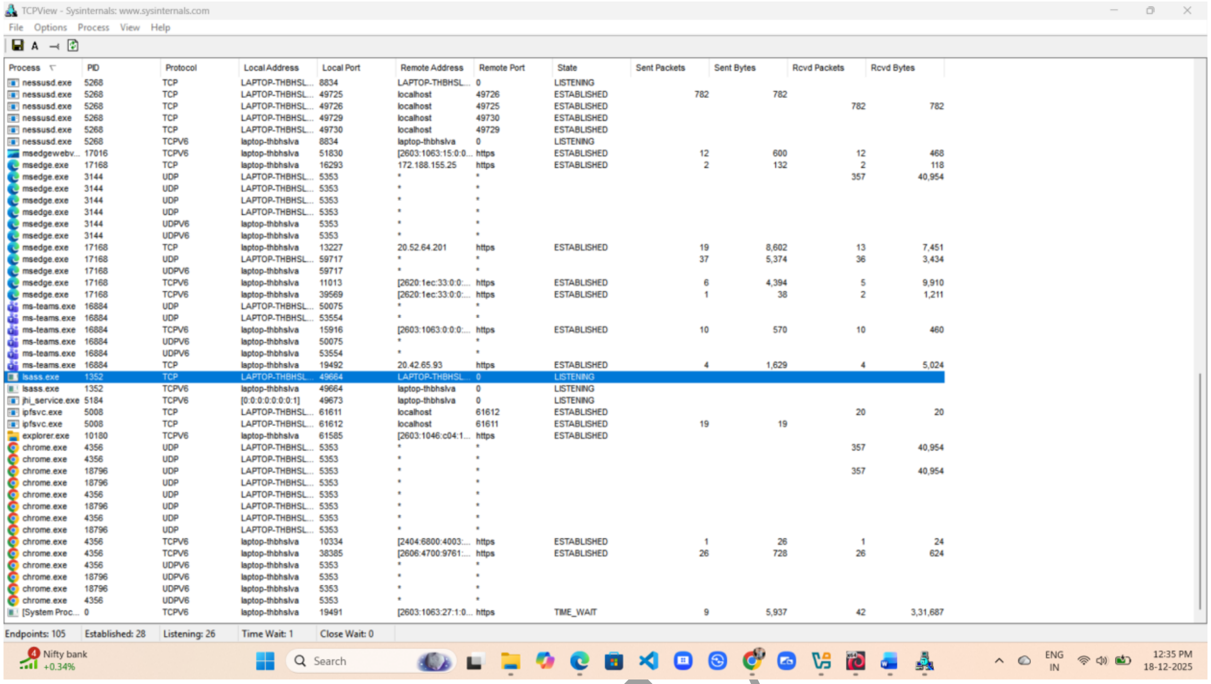
TCPView is a powerful network monitoring tool from Microsoft Sysinternals that shows all active TCP and UDP connections on a Windows system. It displays real-time details such as local and remote IP addresses, port numbers, connection states, and the exact processes (PIDs) using those connections. This makes it extremely useful for spotting suspicious programs or hidden malware communications.

How to Install TCPView:

- Open your browser and search for **"TCPView download"**.

You can get the official version from the Microsoft Sysinternals website:
https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview

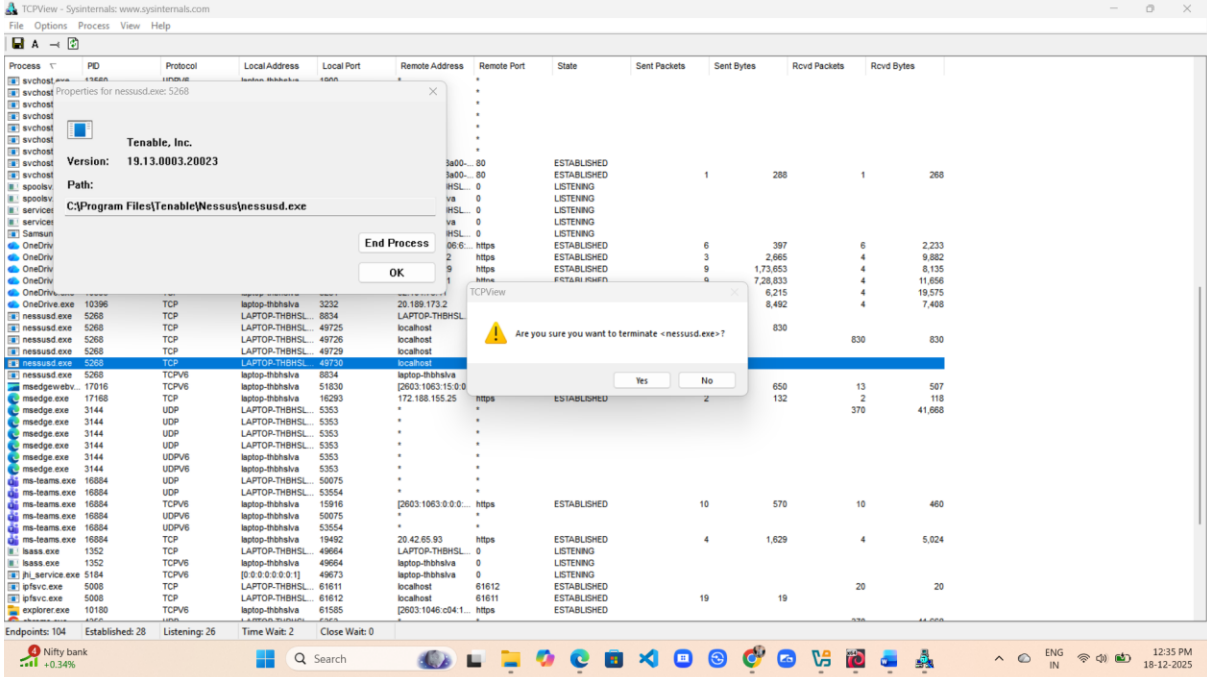
- After Download, Open It


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Nifty bank
+0.34%
Search
ENG
IN
12:35 PM
18-12-2025

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
nessusd.exe	5268	TCP	LAPTOP-THBHSL...	8834	LAPTOP-THBHSL...	0	LISTENING				
nessusd.exe	5268	TCP	LAPTOP-THBHSL...	49725	localhost	49726	ESTABLISHED	782	782		
nessusd.exe	5268	TCP	LAPTOP-THBHSL...	49726	localhost	49725	ESTABLISHED			782	782
nessusd.exe	5268	TCP	LAPTOP-THBHSL...	49729	localhost	49730	ESTABLISHED				
nessusd.exe	5268	TCP	LAPTOP-THBHSL...	49730	localhost	49729	ESTABLISHED				
nessusd.exe	5268	TCPV6	laptop-thbhslva	8834	laptop-thbhslva	0	LISTENING				
msedgewebv...	17016	TCPV6	laptop-thbhslva	51830	[2603:1063:15:0:0...	https	ESTABLISHED	12	600	12	468
msedge.exe	17168	TCP	laptop-thbhslva	16293	172.188.155.25	https	ESTABLISHED	2	132	2	118
msedge.exe	3144	UDP	LAPTOP-THBHSL...	5353	*	*				357	40,954
msedge.exe	3144	UDP	LAPTOP-THBHSL...	5353	*	*					
msedge.exe	3144	UDP	LAPTOP-THBHSL...	5353	*	*					
msedge.exe	3144	UDP	LAPTOP-THBHSL...	5353	*	*					
msedge.exe	3144	UDPV6	laptop-thbhslva	5353	*	*					
msedge.exe	3144	UDPV6	laptop-thbhslva	5353	*	*					
msedge.exe	17168	TCP	laptop-thbhslva	13227	20.52.64.201	https	ESTABLISHED	19	8,602	13	7,451
msedge.exe	17168	UDP	LAPTOP-THBHSL...	59717	*	*		37	5,374	36	3,434
msedge.exe	17168	UDPV6	laptop-thbhslva	59717	*	*					
msedge.exe	17168	TCPV6	laptop-thbhslva	11013	[2620:1ec:33:0:0:...	https	ESTABLISHED	6	4,394	5	9,910
msedge.exe	17168	TCPV6	laptop-thbhslva	39569	[2620:1ec:33:0:0:...	https	ESTABLISHED	1	38	2	1,211
ms-teams.exe	16884	UDP	LAPTOP-THBHSL...	50075	*	*					
ms-teams.exe	16884	UDP	LAPTOP-THBHSL...	53554	*	*					
ms-teams.exe	16884	TCPV6	laptop-thbhslva	15916	[2603:1063:0:0:0:...	https	ESTABLISHED	10	570	10	460
ms-teams.exe	16884	UDPV6	laptop-thbhslva	50075	*	*					
ms-teams.exe	16884	UDPV6	laptop-thbhslva	53554	*	*					
ms-teams.exe	16884	TCP	laptop-thbhslva	19492	20.42.65.93	https	ESTABLISHED	4	1,629	4	5,024
lsass.exe	1352	TCP	LAPTOP-THBHSL...	49664	LAPTOP-THBHSL...	0	LISTENING				
lsass.exe	1352	TCPV6	laptop-thbhslva	49664	laptop-thbhslva	0	LISTENING				
jhi_service.exe	5184	TCPV6	[0:0:0:0:0:0:0:1]	49673	laptop-thbhslva	0	LISTENING				
ipfsvc.exe	5008	TCP	LAPTOP-THBHSL...	61611	localhost	61612	ESTABLISHED			20	20
ipfsvc.exe	5008	TCP	LAPTOP-THBHSL...	61612	localhost	61611	ESTABLISHED	19	19		
explorer.exe	10180	TCPV6	laptop-thbhslva	61585	[2603:1046:c04:1...	https	ESTABLISHED				
chrome.exe	4356	UDP	LAPTOP-THBHSL...	5353	*	*				357	40,954
chrome.exe	4356	UDP	LAPTOP-THBHSL...	5353	*	*					
chrome.exe	18796	UDP	LAPTOP-THBHSL...	5353	*	*				357	40,954
chrome.exe	18796	UDP	LAPTOP-THBHSL...	5353	*	*					
chrome.exe	4356	UDP	LAPTOP-THBHSL...	5353	*	*					
chrome.exe	18796	UDP	LAPTOP-THBHSL...	5353	*	*					
chrome.exe	4356	UDP	LAPTOP-THBHSL...	5353	*	*					
chrome.exe	18796	UDP	LAPTOP-THBHSL...	5353	*	*					
chrome.exe	4356	TCPV6	laptop-thbhslva	10334	[2404:6800:4003:...	https	ESTABLISHED	1	26	1	24
chrome.exe	4356	TCPV6	laptop-thbhslva	38385	[2606:4700:9761:...	https	ESTABLISHED	26	728	26	624
chrome.exe	4356	UDPV6	laptop-thbhslva	5353	*	*					
chrome.exe	18796	UDPV6	laptop-thbhslva	5353	*	*					
chrome.exe	18796	UDPV6	laptop-thbhslva	5353	*	*					
chrome.exe	4356	UDPV6	laptop-thbhslva	5353	*	*					
[System Proc...	0	TCPV6	laptop-thbhslva	19491	[2603:1063:27:1:0...	https	TIME_WAIT	9	5,937	42	3,31,687

Endpoints: 105 Established: 28 Listening: 26 Time Wait: 1 Close Wait: 0

• You can also see the path/location of running process, simply click on the running process


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
End Process
OK
Yes
No
Nifty bank
+0.34%
Search
ENG
IN
12:35 PM
18-12-2025

Properties for nessusd.exe: 5268

Tenable, Inc.

Version: 19.13.0003.20023

Path:

C:\Program Files\Tenable\Nessus\nessusd.exe

TCPView

Are you sure you want to terminate <nessusd.exe>?

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
svchost.exe	13560	UDPV6	laptop-thbhslva	1900	*	*					
svchost						*					
svchost						*					
svchost						*					
svchost						*					
svchost						*					
svchost						*					
svchost					3a00-...	80	ESTABLISHED				
svchost					3a00-...	80	ESTABLISHED	1	288	1	268
spoolsv.					HSL...	0	LISTENING				
spoolsv.					va	0	LISTENING				
service					HSL...	0	LISTENING				
service					va	0	LISTENING				
Samsun					HSL...	0	LISTENING				
OneDriv					06:6:...	https	ESTABLISHED	6	397	6	2,233
OneDriv					2	https	ESTABLISHED	3	2,665	4	9,882
OneDriv					9	https	ESTABLISHED	9	1,73,653	4	8,135
OneDriv					1	https	ESTABLISHED	9	7,28,833	4	11,656
OneDrive.exe									6,215	4	19,575
OneDrive.exe	10396	TCP	laptop-thbhslva	3232	20.189.173.2				8,492	4	7,408
nessusd.exe	5268	TCP	LAPTOP-THBHSL...	8834	LAPTOP-THBHSL...						
nessusd.exe	5268	TCP	LAPTOP-THBHSL...	49725	localhost				830		
nessusd.exe	5268	TCP	LAPTOP-THBHSL...	49726	localhost					830	830
nessusd.exe	5268	TCP	LAPTOP-THBHSL...	49729	localhost						
nessusd.exe	5268	TCP	LAPTOP-THBHSL...	49730	localhost						
nessusd.exe	5268	TCPV6	laptop-thbhslva	8834	laptop-thbhslva						
msedgewebv...	17016	TCPV6	laptop-thbhslva	51830	[2603:1063:15:0:0				650	13	507
msedge.exe	17168	TCP	laptop-thbhslva	16293	172.188.155.25	https	ESTABLISHED	2	132	2	118
msedge.exe	3144	UDP	LAPTOP-THBHSL...	5353	*	*				370	41,668
msedge.exe	3144	UDP	LAPTOP-THBHSL...	5353	*	*					
msedge.exe	3144	UDP	LAPTOP-THBHSL...	5353	*	*					
msedge.exe	3144	UDP	LAPTOP-THBHSL...	5353	*	*					
msedge.exe	3144	UDPV6	laptop-thbhslva	5353	*	*					
msedge.exe	3144	UDPV6	laptop-thbhslva	5353	*	*					
ms-teams.exe	16884	UDP	LAPTOP-THBHSL...	50075	*	*					
ms-teams.exe	16884	UDP	LAPTOP-THBHSL...	53554	*	*					
ms-teams.exe	16884	TCPV6	laptop-thbhslva	15916	[2603:1063:0:0:0:...	https	ESTABLISHED	10	570	10	460
ms-teams.exe	16884	UDPV6	laptop-thbhslva	50075	*	*					
ms-teams.exe	16884	UDPV6	laptop-thbhslva	53554	*	*					
ms-teams.exe	16884	TCP	laptop-thbhslva	19492	20.42.65.93	https	ESTABLISHED	4	1,629	4	5,024
lsass.exe	1352	TCP	LAPTOP-THBHSL...	49664	LAPTOP-THBHSL...	0	LISTENING				
lsass.exe	1352	TCPV6	laptop-thbhslva	49664	laptop-thbhslva	0	LISTENING				
jhi_service.exe	5184	TCPV6	[0:0:0:0:0:0:0:1]	49673	laptop-thbhslva	0	LISTENING				
ipfsvc.exe	5008	TCP	LAPTOP-THBHSL...	61611	localhost	61612	ESTABLISHED			20	20
ipfsvc.exe	5008	TCP	LAPTOP-THBHSL...	61612	localhost	61611	ESTABLISHED	19	19		
explorer.exe	10180	TCPV6	laptop-thbhslva	61585	[2603:1046:c04:1...	https	ESTABLISHED				

Endpoints: 104 Established: 28 Listening: 26 Time Wait: 2 Close Wait: 0

Conclusion

Dynamic malware analysis exposes the true intent of malicious software by watching it operate live. Tools like TCPView help uncover hidden network activity and command-and-control communication. The takeaway is timeless: trust behavior over promises—because malware always tells the truth when it thinks no one's watching.

Infecting a Target System Using a Virus

A computer virus is a self-replicating malicious program that spreads by attaching its code to legitimate executable files. Once activated, it operates without the knowledge or consent of the user, quietly doing its thing behind the curtain. Classic villain energy.

Lab Scenario

Viruses remain one of the oldest yet most persistent threats in modern computing. From personal laptops to enterprise networks, no system is truly immune. The true strength of a virus lies in its ability to reproduce—often repeatedly—based on parameters defined by its creator.

Virus Creation Using JPS Virus Maker

The JPS Virus Maker is a legacy malware-generation tool that allows the creation of customized malicious programs by enabling predefined behaviors. These behaviors may include automatic execution at system startup, forced system shutdown, disruption of user input devices, interference with system services, and termination of operating system processes.

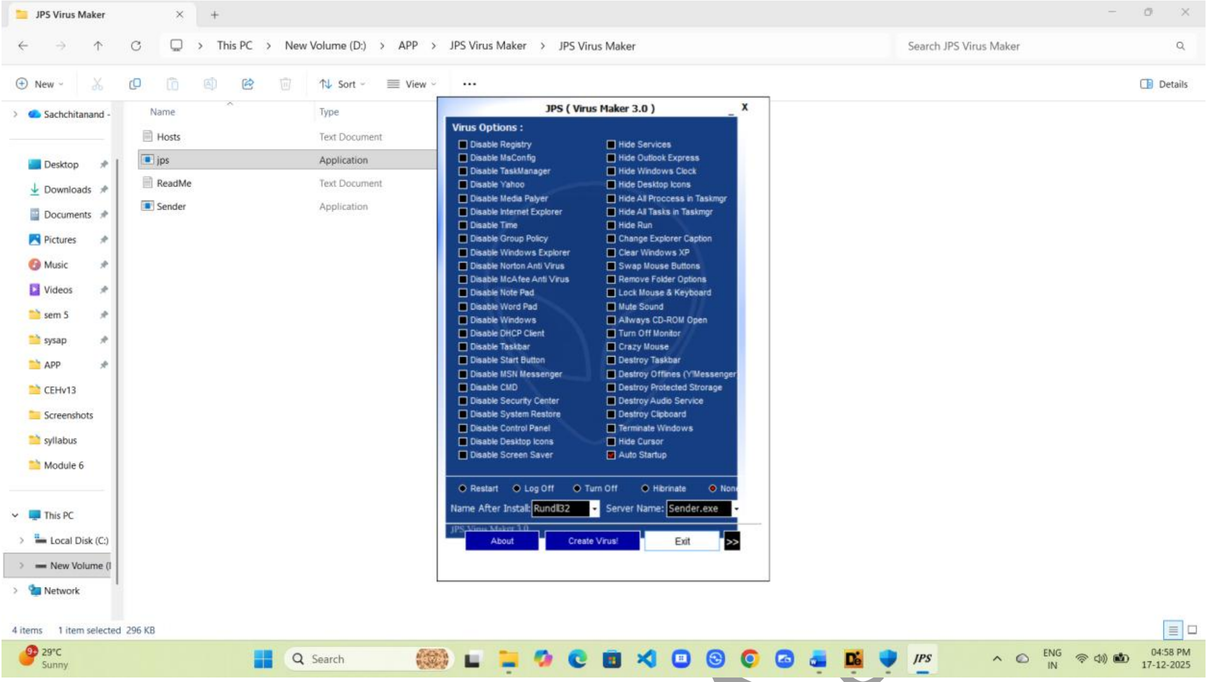
From a cybersecurity education perspective, such tools are discussed **only as proof-of-concept artifacts**. Ethical hackers and penetration testers study them to understand how malware operates, how attackers abuse system privileges, and how defensive controls can be evaluated against real-world threats.

In controlled laboratory environments, simulated malware is sometimes used to assess:

- Effectiveness of antivirus and endpoint protection
- User privilege restrictions
- System hardening and recovery mechanisms
- Incident response readiness

Using JPS Virus Maker

- Open JPS Virus Maker in a controlled virtual machine environment.
- Select the type of virus to create (e.g., file infector, system disruptor).
- Configure the virus's behavior, such as target file types or execution triggers.
- Compile the virus into an executable file.
- Test the virus in an isolated, sandboxed environment to observe its effects without risking actual systems.



Name	Type
Hosts	Text Document
jps	Application
ReadMe	Text Document
Sender	Application

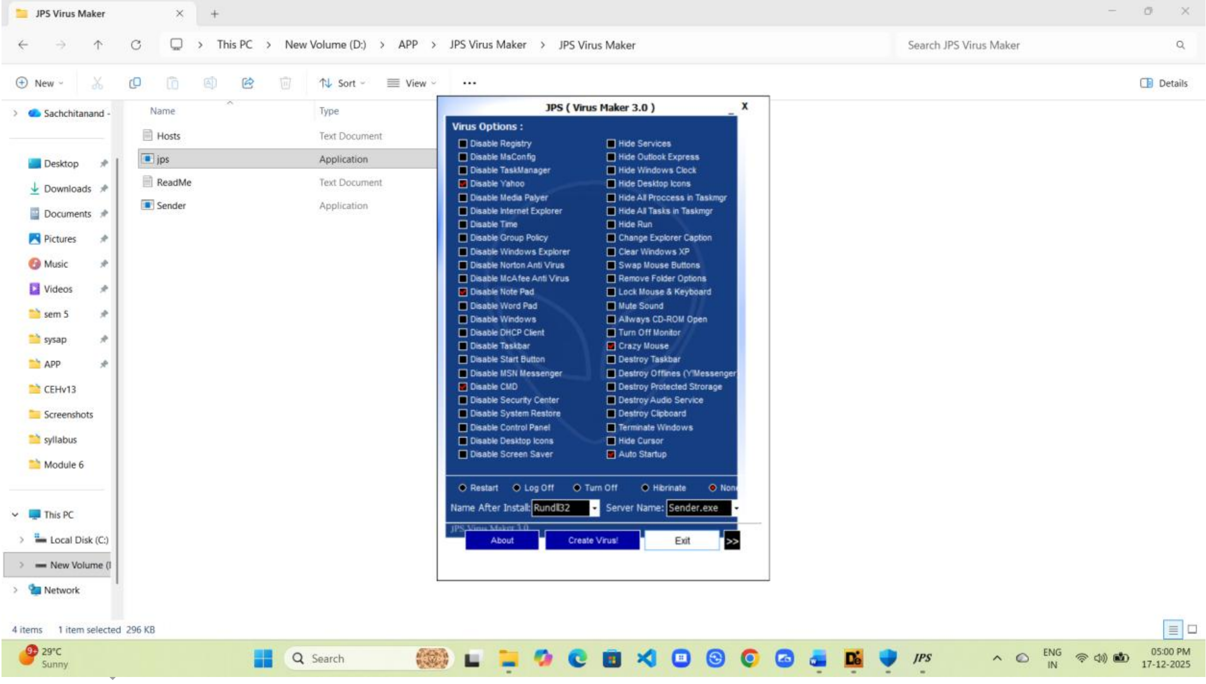
Virus Options :

☐ Disable Registry
☐ Disable MsConfig
☐ Disable TaskManager
☐ Disable Yahoo
☐ Disable Media Palyer
☐ Disable Internet Explorer
☐ Disable Time
☐ Disable Group Policy
☐ Disable Windows Explorer
☐ Disable Norton Anti Virus
☐ Disable McAfee Anti Virus
☐ Disable Note Pad
☐ Disable Word Pad
☐ Disable Windows
☐ Disable DHCP Client
☐ Disable Taskbar
☐ Disable Start Button
☐ Disable MSN Messenger
☐ Disable CMD
☐ Disable Security Center
☐ Disable System Restore
☐ Disable Control Panel
☐ Disable Desktop Icons
☐ Disable Screen Saver
☐ Hide Services
☐ Hide Outlook Express
☐ Hide Windows Clock
☐ Hide Desktop Icons
☐ Hide All Proccess in Taskmgr
☐ Hide All Tasks in Taskmgr
☐ Hide Run
☐ Change Explorer Caption
☐ Clear Windows XP
☐ Swap Mouse Buttons
☐ Remove Folder Options
☐ Lock Mouse & Keyboard
☐ Mute Sound
☐ Allways CD-ROM Open
☐ Turn Off Monitor
☐ Crazy Mouse
☐ Destroy Taskbar
☐ Destroy Offlines (Y!Messenger
☐ Destroy Protected Strorage
☐ Destroy Audio Service
☐ Destroy Clipboard
☐ Terminate Windows
☐ Hide Cursor
☑ Auto Startup

○ Restart ○ Log Off ○ Turn Off ○ Hibrinate ● Non

Name After Install: Rundll32 Server Name: Sender.exe

4 items 1 item selected 296 KB



Name	Type
Hosts	Text Document
jps	Application
ReadMe	Text Document
Sender	Application

Virus Options :

☐ Disable Registry
☐ Disable MsConfig
☐ Disable TaskManager
☑ Disable Yahoo
☐ Disable Media Palyer
☐ Disable Internet Explorer
☐ Disable Time
☐ Disable Group Policy
☐ Disable Windows Explorer
☐ Disable Norton Anti Virus
☐ Disable McAfee Anti Virus
☑ Disable Note Pad
☐ Disable Word Pad
☐ Disable Windows
☐ Disable DHCP Client
☐ Disable Taskbar
☐ Disable Start Button
☐ Disable MSN Messenger
☑ Disable CMD
☐ Disable Security Center
☐ Disable System Restore
☐ Disable Control Panel
☐ Disable Desktop Icons
☐ Disable Screen Saver
☐ Hide Services
☐ Hide Outlook Express
☐ Hide Windows Clock
☐ Hide Desktop Icons
☐ Hide All Proccess in Taskmgr
☐ Hide All Tasks in Taskmgr
☐ Hide Run
☐ Change Explorer Caption
☐ Clear Windows XP
☐ Swap Mouse Buttons
☐ Remove Folder Options
☐ Lock Mouse & Keyboard
☐ Mute Sound
☐ Allways CD-ROM Open
☐ Turn Off Monitor
☑ Crazy Mouse
☐ Destroy Taskbar
☐ Destroy Offlines (Y!Messenger
☐ Destroy Protected Strorage
☐ Destroy Audio Service
☐ Destroy Clipboard
☐ Terminate Windows
☐ Hide Cursor
☑ Auto Startup

○ Restart ○ Log Off ○ Turn Off ○ Hibrinate ● Non

Name After Install: Rundll32 Server Name: Sender.exe

4 items 1 item selected 296 KB

Conclusion

This task helped in understanding the basic working of computer viruses and their impact on system security. It emphasizes the importance of secure configurations, user awareness, and effective defensive measures to protect systems from malware attacks.

Explain Malware Countermeasures

Malware countermeasures are the strategies and controls used to **prevent, detect, and respond** to malicious software attacks. Old wisdom, new tools—the goal stays the same: keep systems clean and trustworthy.

1. Preventive Countermeasures

Prevention is the first line of defense, and honestly, still the strongest.

- Install and regularly update antivirus and anti-malware software
- Keep operating systems and applications patched
- Use firewalls to block unauthorized access
- Avoid downloading software from untrusted sources
- Apply least-privilege access to users and services

2. Detection Countermeasures

Because let's be real—some threats will slip through.

- Monitor system processes and network traffic
- Use intrusion detection and endpoint protection systems
- Perform regular malware scans and log analysis
- Watch for abnormal behavior like unknown processes or network connections

3. Corrective Countermeasures

When malware hits, speed and discipline matter.

- Isolate the infected system immediately
- Remove malware using trusted security tools
- Restore systems from clean backups
- Apply security updates to prevent reinfection

Key Malware Countermeasures

- Avoid opening email attachments from unknown or untrusted senders
- Do not download or execute software from untrusted sources
- Install OS and application patches and keep systems updated
- Use reputable antivirus and anti-malware tools and keep them up to date
- Enable firewalls and block unnecessary ports at the host and network level
- Regularly back up important data
- Enable pop-up blockers and use internet security features

- Do not open files with multiple or suspicious extensions
- Always verify applications before installation
- Keep security tools running with current virus definitions

Conclusion

Malware defense is not about one tool—it's about habits. Strong prevention, smart monitoring, and fast response form a security posture that actually works. The tech evolves, threats mutate, but the rule stays old-school and undefeated: **protect, monitor, recover—repeat**.

Module Summary

This module walked through the fundamentals of malware and how it spreads—viruses, Trojans, worms, ransomware, fileless threats, and AI-powered malware. It broke down how these threats infect systems and evolve through their lifecycle. Static and dynamic malware analysis techniques were explored to understand detection in real-world scenarios, along with practical countermeasures and anti-malware tools. Bottom line: know the threat, read its moves, shut it down. Old threats, new tricks—but disciplined defense still wins.

THANK YOU