



MALWARE

A smartphone is shown from a top-down perspective, tilted slightly. The screen displays a large red warning icon with a white exclamation mark inside. Below the icon, the word "MALWARE" is written in white capital letters. The phone is set against a dark background with glowing blue and yellow circuit board patterns, suggesting a high-tech or digital environment.

-ATHARVA KATKAR

INDEX

1. Introduction to Malware

- 1.1 Definition of Malware
- 1.2 Purpose and Impact of Malware

2. Types of Malware

- 2.1 Virus
- 2.2 Worm
- 2.3 Trojan Horse
- 2.4 Ransomware
- 2.5 Spyware
- 2.6 Adware
- 2.7 Rootkit
- 2.8 Botnet
- 2.9 Fileless Malware
- 2.10 Scareware

3. Gaining Access to Target System Using Trojans

- 3.1 NetBus Trojan
- 3.2 njRAT Trojan
- 3.3 Working of Remote Access Trojans (RATs)

4. Malware Analysis

- 4.1 Definition of Malware Analysis
- 4.2 Objectives of Malware Analysis

5. Types of Malware Analysis

- 5.1 Static Malware Analysis
- 5.2 Dynamic Malware Analysis

6. Static Malware Analysis Tools

- 6.1 Hybrid Analysis
- 6.2 VirusTotal
- 6.3 Autoruns
- 6.4 BinText
- 6.5 Dependency Walker

7. Dynamic Malware Analysis

- 7.1 System Baselingining
- 7.2 Host Integrity Monitoring

8. System Baselingining Using Regshot

9. Process and Network Monitoring Tools

- 9.1 TCPView
- 9.2 CurrPorts

10. Malware Analysis Module – Overall Summary

MALWARE THREAT

Malware stands for Malicious Software. It is any software intentionally designed to cause damage, steal data, or disrupt systems, networks, or devices. Hackers use malware to gain unauthorized access, steal sensitive information, or disrupt operations.

Types of Malware --

1. Virus

- How it works: Attaches itself to a clean file or program and spreads to other files.
- Damage: Corrupts or deletes files, causes system crashes.
- Needs user action? Yes (e.g., opening an infected file).
Example: ILOVEYOU virus.

2. Worm

- How it works: Spreads through networks automatically without user interaction.
- Damage: Consumes bandwidth, drops payloads, or crashes systems.
- Self-replicating.Example:

3. Trojan Horse

- How it works: Disguises as legitimate software. Once installed, it opens a backdoor.
- Damage: Allows attackers remote access, data theft, or installing more malware.
- Example: Zeus Trojan.

- SQL Slammer, WannaCry.

4. Ransomware

- How it works: Encrypts user files and demands a ransom to unlock them.
- Damage: Data loss, financial loss, operational disruption.
- Famous attack: WannaCry, REvil.
- Note: Common in healthcare, education, and government sectors.

5. Spyware

- How it works: Secretly records user activity (keystrokes, browsing history).
- Damage: Identity theft, financial fraud.
- Example: Keyloggers, banking trojans.

6. Adware

- How it works: Displays unwanted ads, redirects browsers to malicious sites.
- Damage: Slows down system, potential backdoor for malware.
- Example: Fireball.

7. Rootkit

- How it works: Hides its presence and provides privileged access to the attacker.
- Damage: Bypasses security controls, steals data silently.
- It is Hard to detect
- Used for: Long-term espionage or persistent access.

8. Botnet (Bot + Network)

- How it works: A network of infected devices controlled by an attacker (botmaster).
- Damage: Used for DDoS attacks, spamming, spreading malware.
- Example: Mirai botnet.

9. Fileless Malware

- How it works: Operates in memory (RAM), doesn't leave files on disk.
- Damage: Harder to detect with traditional antivirus.
- Example: PowerShell-based attacks.

10. Scareware

- How it works: Tricks users into thinking their system is infected to force them into buying fake software.
- Damage: Financial loss, malware download.
- Example: Fake antivirus pop-ups.

Gaining Access To The Target System Using NetBus Trojan

NetBus17 is a type of Remote Administration Tool (RAT) — but more specifically, it's a Trojan Horse program that allows an attacker to remotely control a victim's computer. It was popular in the late 1990s, particularly on Windows systems.

- Attacker Machine – Windows 11
 - Target machine –Windows 7
 - Download and Open netbus17

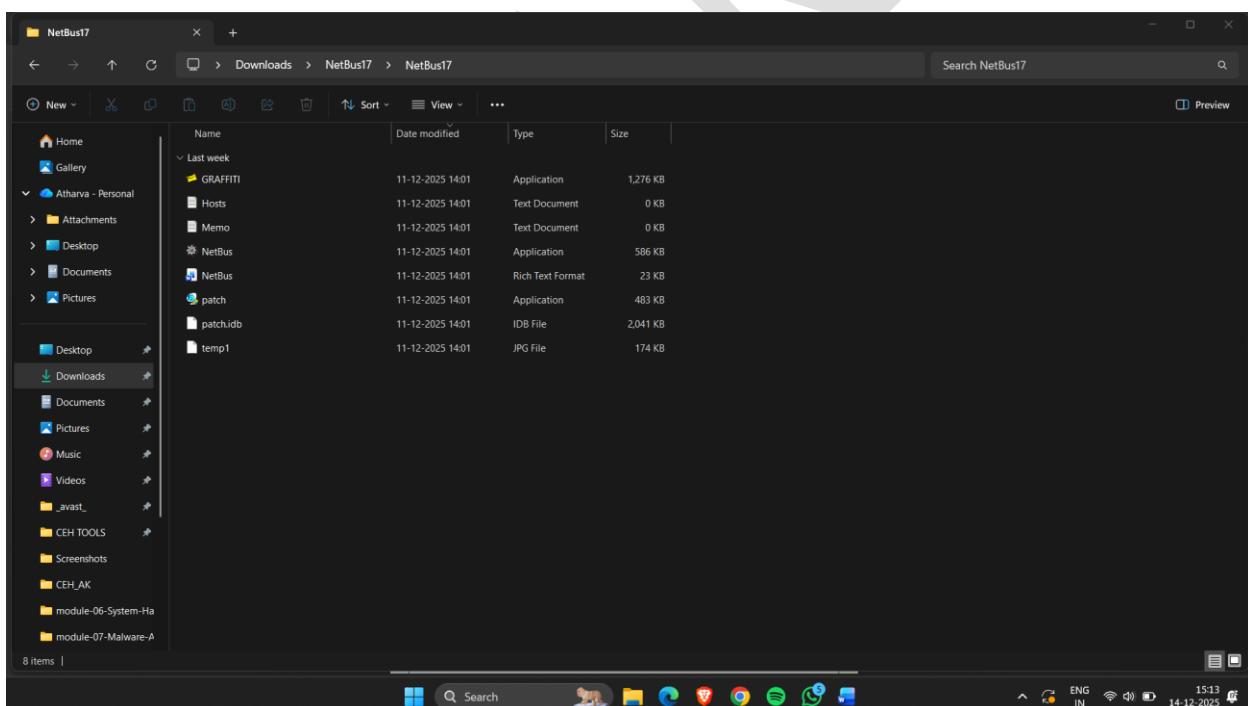


Fig 1

- Now share this folder on victims computer
- Here victim machine is windows 10 and attacker machine is windows 11.
- See attacker machine ip address.

```

Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\cyber>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : 
IPv6 Address . . . . . : fd17:625c:f037:2:3299:8ff0:96e4:8aa7
Temporary IPv6 Address . . . . . : fd17:625c:f037:2:e9af:d67e:b69f:bdd6
Link-local IPv6 Address . . . . . : fe80::ff10:fa72:e89c:9368%3
IPv4 Address . . . . . : 10.0.2.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::2%3
                                         10.0.2.2

C:\Users\cyber>

```

Fig 2

- Now go victim machine and open netbus17-> patch.exe file .
- Go to attacker machine and click on Netbus.exe.
- Here windows 7 connected .
- Click screendump .
- Now click on File manager – To access victims file manager.

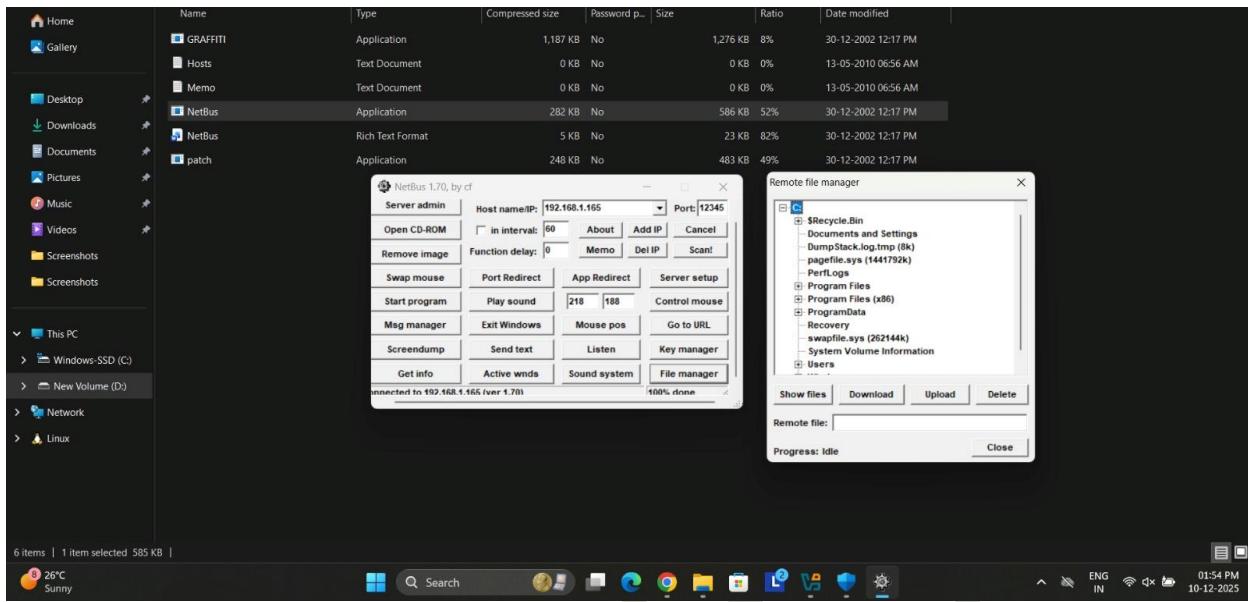


Fig 3

- As shown in this figure we get the attackers Gaining Remote Access Done

Gaining Access To The Target System Using njRAT Trojan

Remote Access Trojans (RATs) are malicious programs that allow unauthorized remote control of a victim's computer. RATs are usually delivered through phishing emails, malicious attachments, or fake software downloads that trick the user into executing the file.

Once executed, the RAT runs silently in the background and establishes a remote connection with the attacker without the user's knowledge. Attackers can perform activities such as keylogging, file access, system monitoring, and remote command execution, posing a major security threat.

- Open njrat and extract file .
- Now click on njrat tool
- Now click on builder and set attacker machine (your machine ip) ip in host sections .

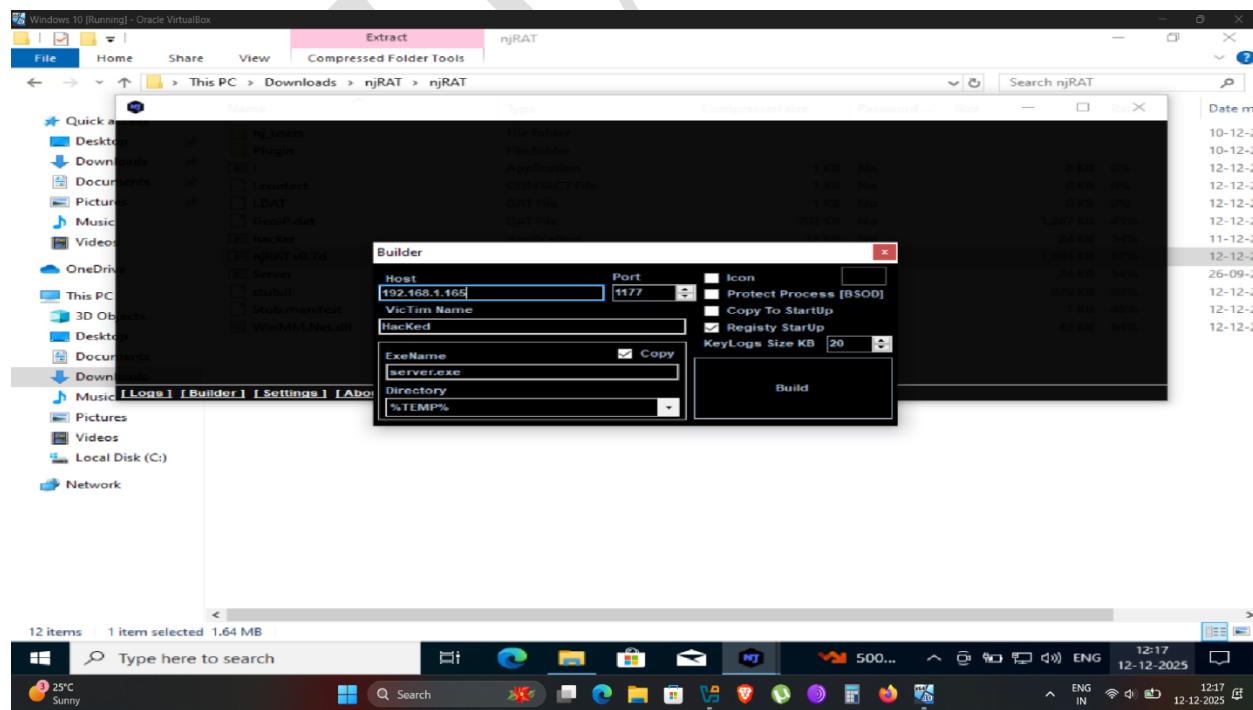


Fig 5

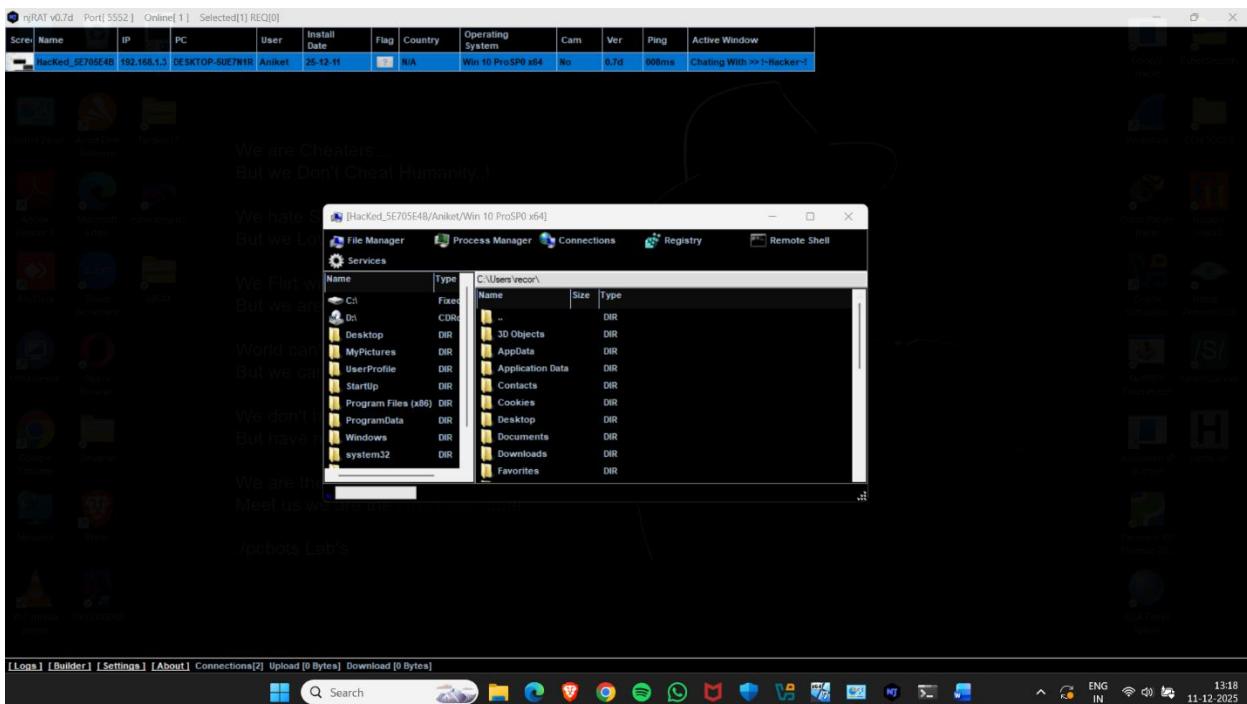


Fig 6

- Right click and show options and here we get file manager access of victim machine .
- As shown in the fig we get remote access of victim machine.

njRAT working:

- The attacker creates a malicious payload using the njRAT builder.
- When the victim executes the file, it silently installs and runs in the background.
- The infected system connects back to the attacker's Command-and-Control (C2) server.
- njRAT maintains a persistent connection, allowing remote commands and data access. It can perform functions like file upload/download, keylogging, process control, and webcam monitoring.
- The RAT communicates over network ports, making it possible to analyze and detect using firewalls and antivirus tools.

Malware Analysis

Malware Analysis is the process of studying malicious software (malware) to understand its behavior, origin, and impact. The goal is to identify what the malware does, how it operates, how to detect it, and how to remove or prevent it.

Types of Malware Analysis –

- 1.Static Malware Analysis
- 2.Dynamic Malware Analysis

Static Malware Analysis

Static analysis involves examining malware without executing it. Analysts inspect the code, strings, metadata, and structure of the file to learn about its behavior.

- **Static Malware Analysis Using Hybrid Malware**

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

- Search hybrid analysis on browser ,[here](#)

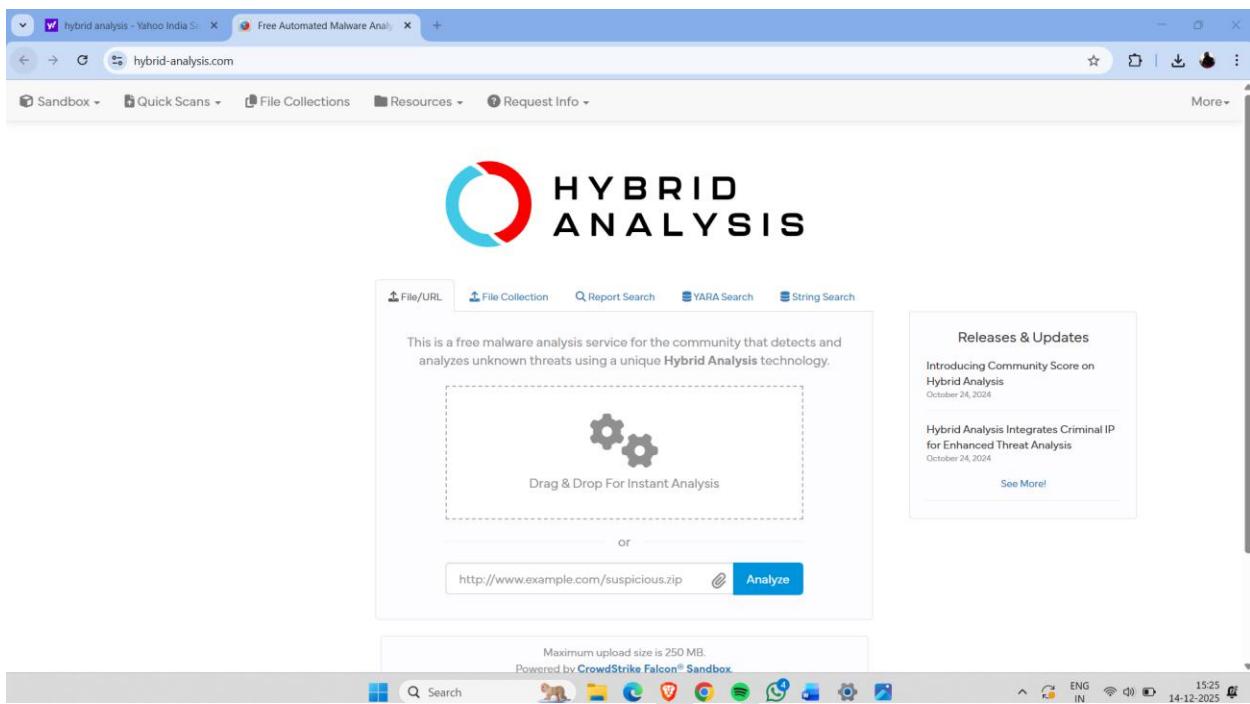


Fig 7

- Add file that you want to

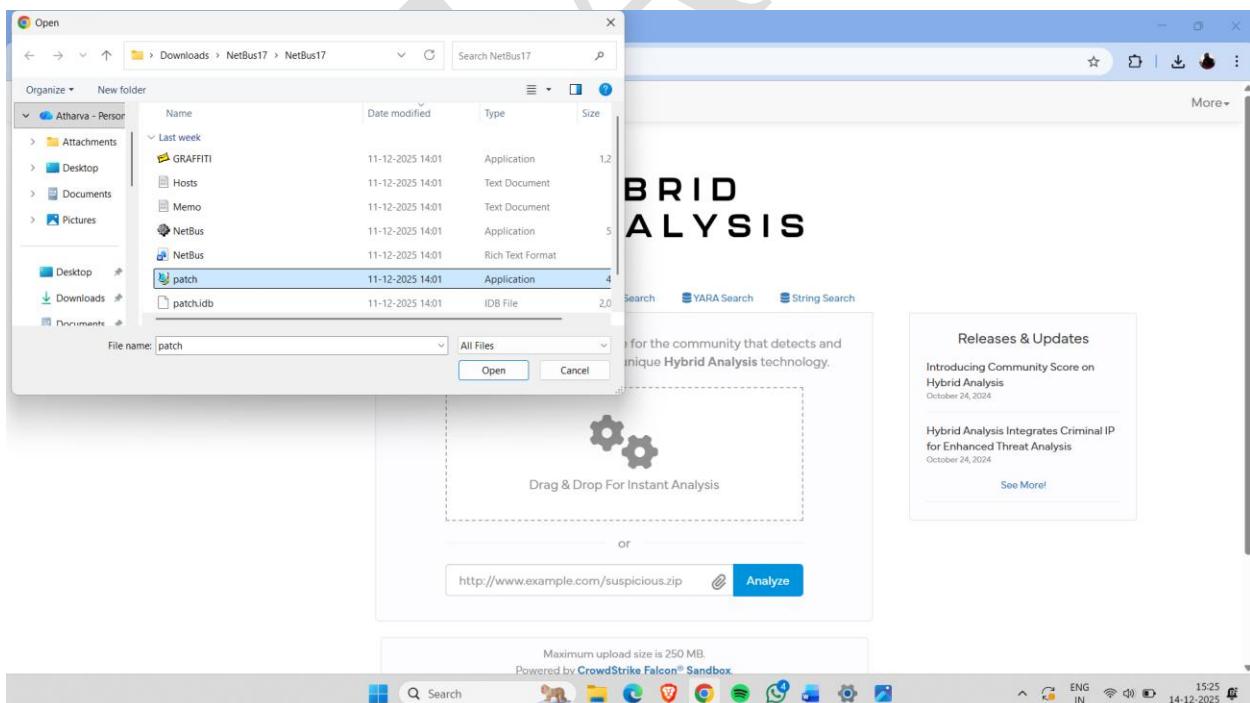


Fig 8

- Here scan completed and says it is a malicious file

The screenshot shows a hybrid malware analysis interface. At the top, there are tabs for VirusTotal, VirusTotal File, hybrid-analysis, and Free Automated Malware Analy. The main page displays an 'Analysis Overview' for a file named 'Patch.exe'. The submission details include: Name: Patch.exe, Size: 483KB, Type: PE32 executable, Mimetype: application/x-dosexec, SHA256: 73a62d6593e3c70b60455299b793bb18d31eddd5f15d04442932c1d3ccb7eb0c, Submitted At: 2018-01-31 08:58:08 (UTC), Last Anti-Virus Scan: 2024-07-22 08:54:09 (UTC), and Last Sandbox Report: 2024-01-04 11:35:57 (UTC). A large red box labeled 'malicious' is present. The Threat Score is 100/100, AV Detection is 96%, and it is Labeled As: Trojan.Netbus. Below this are sharing options (X Post, oLink, E-Mail) and a 'Community Score' of 0. To the right, there's a sidebar with links to Analysis Overview, Anti-Virus Scanner Results (Falcon Sandbox Reports [4]), Relations, Incident Response, and Community. At the bottom, there's a 'Back to top' link.

Fig 9

- As shown in this fig given file is malicious .

Hybrid malware used for:

- Hybrid malware is a combination of different types of malware, such as viruses, worms, trojans, and ransomware.
 - This type of malware is often able to bypass traditional security measures, making it especially dangerous.
 - The goal of hybrid malware is to gain unauthorized access to systems, steal sensitive information, or cause damage to devices.

- **Static Malware Analysis Using Virustotal**

VirusTotal is a free online malware analysis service that scans files, URLs, and hashes using multiple antivirus engines and sandbox tools to detect viruses, trojans, malicious behavior, and other security threats.

What VirusTotal Does:

- Detects viruses, worms, trojans, ransomware
 - Checks malicious websites and phishing links
 - Analyzes suspicious files and hashes
 - Helps in incident response & malware research
-
- Open browser and search virustotal
Website :- <https://www.virustotal.com/gui/home/upload>

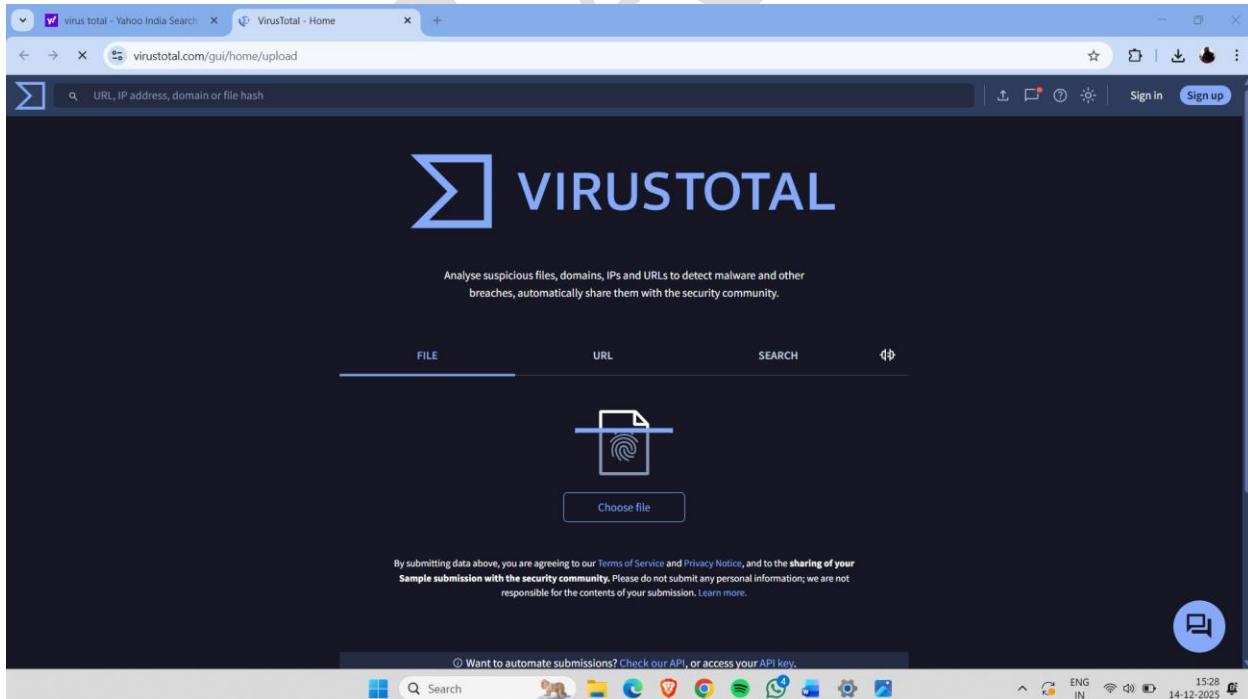


Fig 10

- Now select file that you want to scan.

- After selecting scan file.
- Here scan completes and says its malicious file .

The screenshot shows the VirusTotal analysis interface for a file identified by the SHA-256 hash 73a62d6593e3c70b60455299b793bb18d31eddd5f15d04442932c1d3ccb7eb0c. The main summary panel indicates a high Community Score of 65/72, with a note that it is distributed by Dark Bay Ltd. The file is a Patch.exe file, and the analysis was completed 1 month ago. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. Below these tabs, there's a call-to-action to join the community for additional insights. The SECURITY VENDORS' ANALYSIS section lists various security vendors and their findings, such as AhnLab-V3 identifying Win-Trojan/Netbus, Alibaba identifying Backdoor:Win32/Netbus.46c57d86, and AVG identifying Win32:NetBus-AO [Trj]. The bottom of the screen shows the Windows taskbar with various pinned icons.

Fig 11

This screenshot is identical to Fig 11, showing the same VirusTotal analysis results for the same file hash. It displays the high community score of 65/72, the file type as Patch.exe, and the analysis date as 1 month ago. The SECURITY VENDORS' ANALYSIS section provides a detailed list of vendor detections, including Tencent, TrendMicro, Varist, VIPRE, ViRobot, WithSecure, Yandex, ZoneAlarm by Check Point, Baidu, SecureAge, Trapmine, Avast-Mobile, and Symantec Mobile Insight. The bottom of the screen shows the Windows taskbar.

Fig 12

- **Static Malware Analysis Autoruns**

Autoruns is used to identify programs and services that automatically start during system boot or user logon, helping detect malicious persistence mechanisms.

- Detect malicious startup entries
- Find persistence techniques used by malware
- Analyze registry and startup folders
- Incident response & forensics

How to do it:

- Download and open tcpview now see all process and ports.

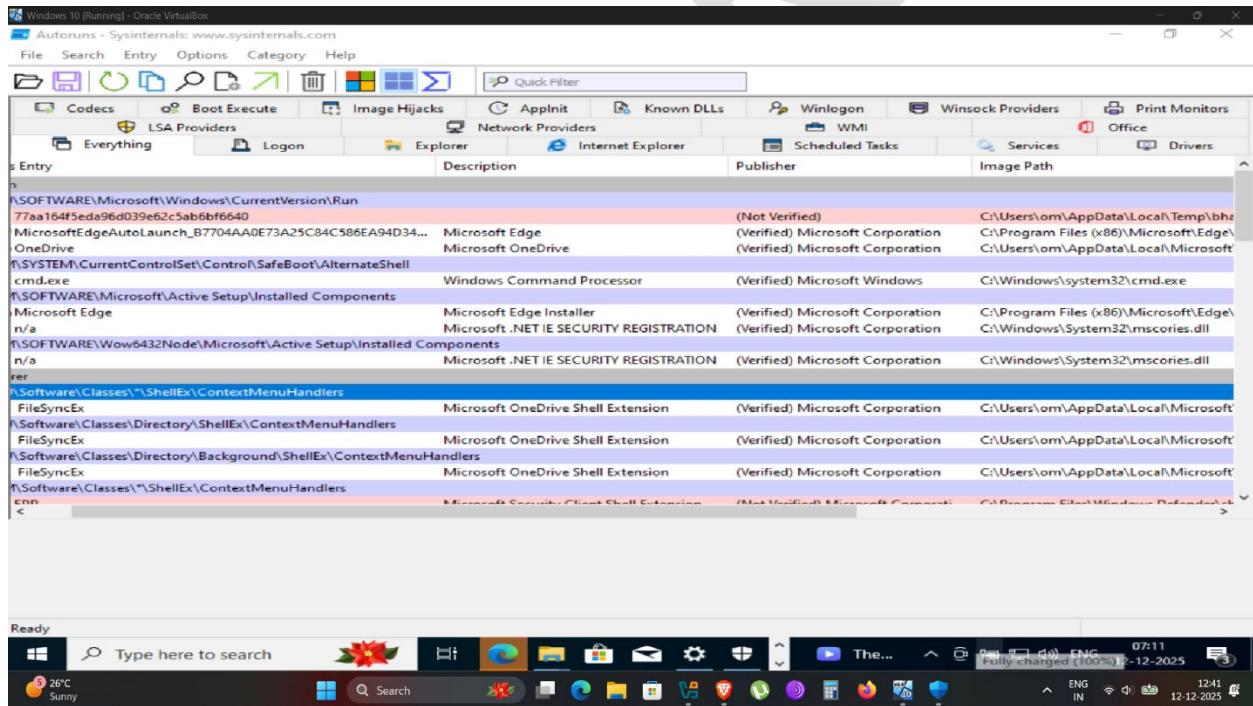


Fig 13

- It helps to detect malicious entries added to maintain persistence after reboot.
- Useful for network monitoring and malware analysis.

- **Static Malware Analysis BinText**

BinText extracts readable strings from executable files without executing them, which makes it a static analysis tool.

- **Bintext tool uses :**

- Used in **static malware analysis**.
- Extracts **readable strings** from executable files.
- Identifies **URLs, IP addresses, commands, and file paths**.
- Helps understand **malware behavior without execution**.
- Useful for **initial malware investigation and reporting**

How does it work:

- Start the bintext tool and upload file that you want to scan .

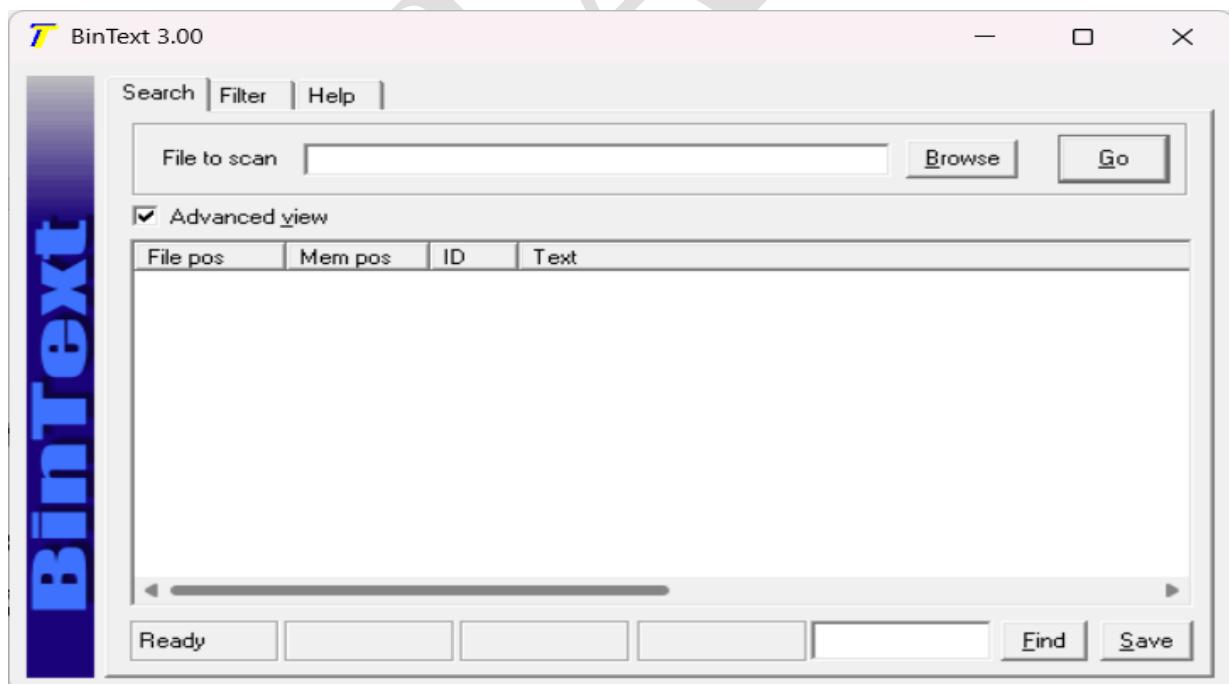


Fig 14

- Now selected file is under scan .

- Here, Result is generated .

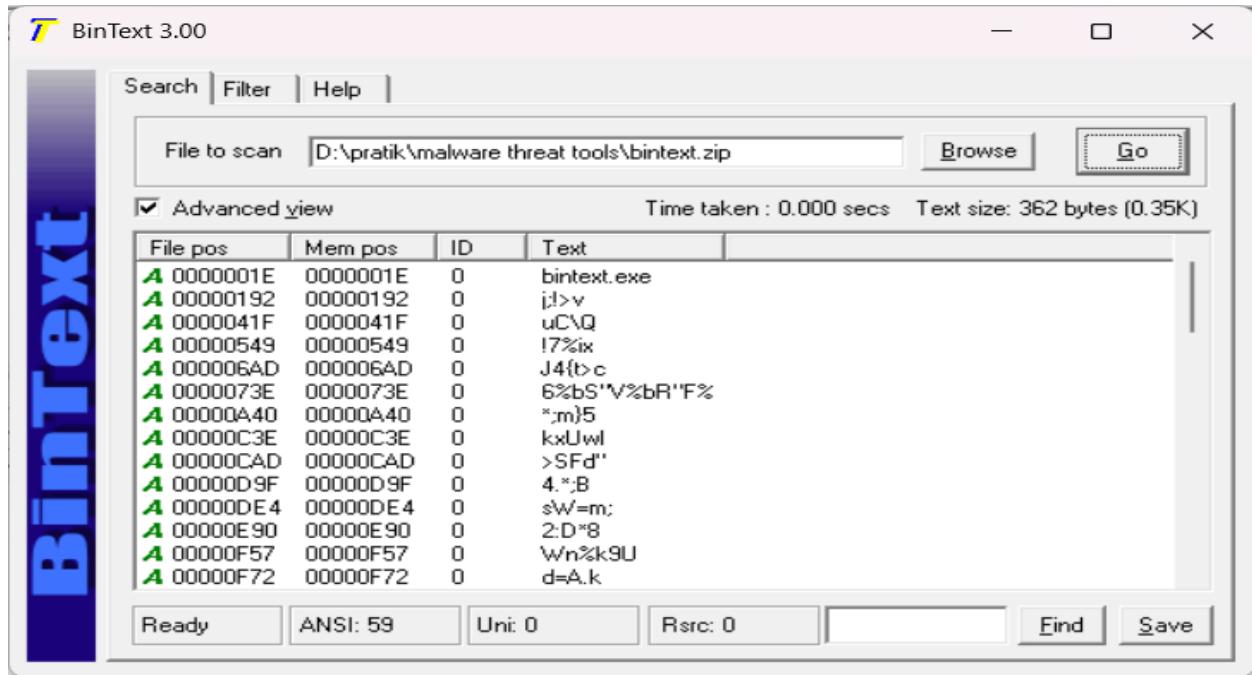


Fig 15

- Here is scanning output .

The screenshot shows a terminal or text editor window with a dark theme. The title bar includes 'greenbone pass 57ae8a18-f6b6', 'hosts', 'exploit them. Information collie', '-res-x64.txt', '-res-x64.txt', 'bin.txt', and a zoom icon. The main area displays the same memory dump data as Fig 15, with file and memory positions, IDs, and text values. The text is mostly identical to Fig 15, with some minor differences in line endings or character representation due to the different terminal settings.

File pos	Mem pos	ID	Text
00000001E	0000001E	0	bintext.exe
000000192	00000192	0	j;!>v
0000041F	0000041F	0	uC\ Q
00000549	00000549	0	!7%ix
000006AD	000006AD	0	J4{t>c
0000073E	0000073E	0	6%b\$"V%bR"!F%
00000A40	00000A40	0	*;m}5
00000C3E	00000C3E	0	kxUwl
00000CAD	00000CAD	0	>SFd"
00000D9F	00000D9F	0	4.*;B
00000DE4	00000DE4	0	sW=m;
00000E90	00000E90	0	2:D*8
00000F57	00000F57	0	Wn%k9U
00000F72	00000F72	0	d=A.k
00001122	00001122	0	z}42R
00001233	00001233	0	h)9EE
00001242	00001242	0	?Q+KS
00001346	00001346	0	.j\$<E4
0000141D	0000141D	0	OCE\$+
00001477	00001477	0	RJ9*:b
0000149B	0000149B	0	''ip-
000014D0	000014D0	0	'<KZAJV
00001755	00001755	0	I 8\$n

Fig 16

- **Static malware analysis using Dependency Walker**

Dependency Walker is used in static malware analysis to examine DLL dependencies of executables.

- Analyzes DLL dependencies of executable files
- Identifies missing, hidden, or suspicious DLLs
- Helps detect malware packing or injection techniques
- Does not execute the file (safe analysis)
- Useful for malware structure and behavior understanding
- Download and start the dependency walker tool.

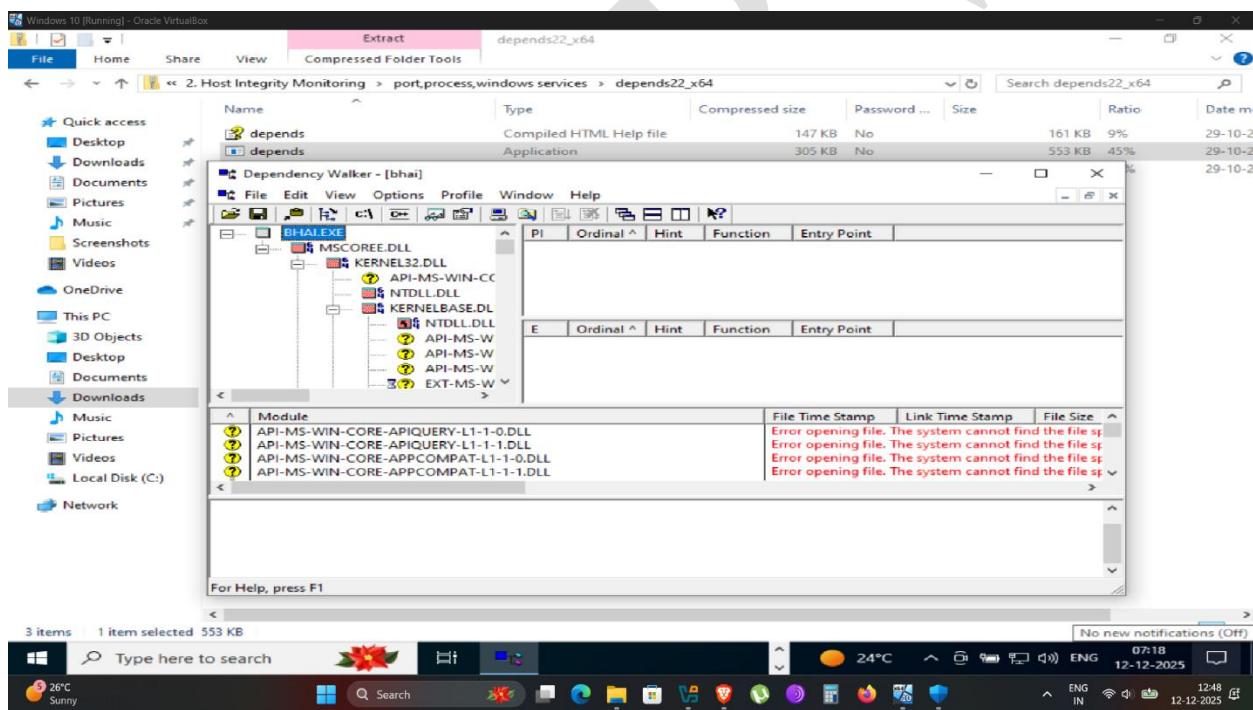


Fig 17

- selected executable and displays its DLL dependencies, imported/exported functions, and missing or suspicious files without running the program.

Dynamic Malware Analysis

Dynamic analysis involves executing the malware in a sandboxed environment to observe its real-time behavior.

Type of Dynamic Malware Analysis --

1. System Baselining –
2. Host Integrity Monitoring –

System baselining

System Baselining refers to process of capturing system state (taking snapshots at the time malware analysis begins

- **System Baselining Using Regshot**

Regshot is a lightweight, open-source registry comparison tool commonly used in system baselining and malware analysis. It allows you to take snapshots of the Windows Registry and file system before and after a particular event (like installing software or running a program), and then compare them to identify changes.

- Start Regshot and Click on first shot ...that capture / snapshot of system

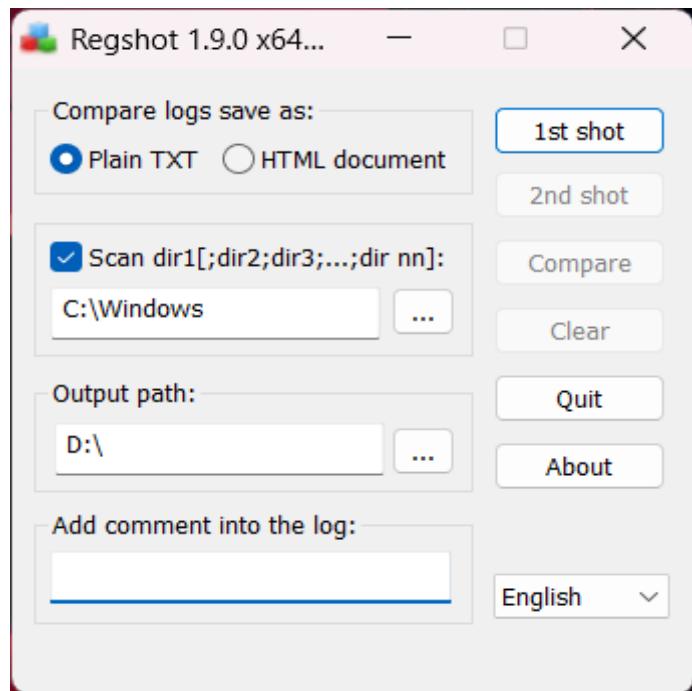


Fig 18

- as shown in this shot it captures the registry and file system.

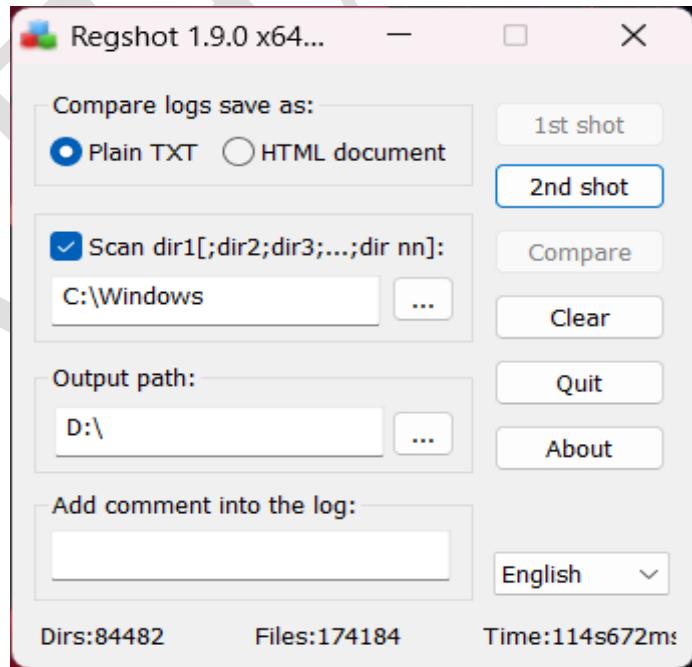


Fig 19

- Before click on second shot run a any other file or folder to determine the changes between first shot and second shot and compare .

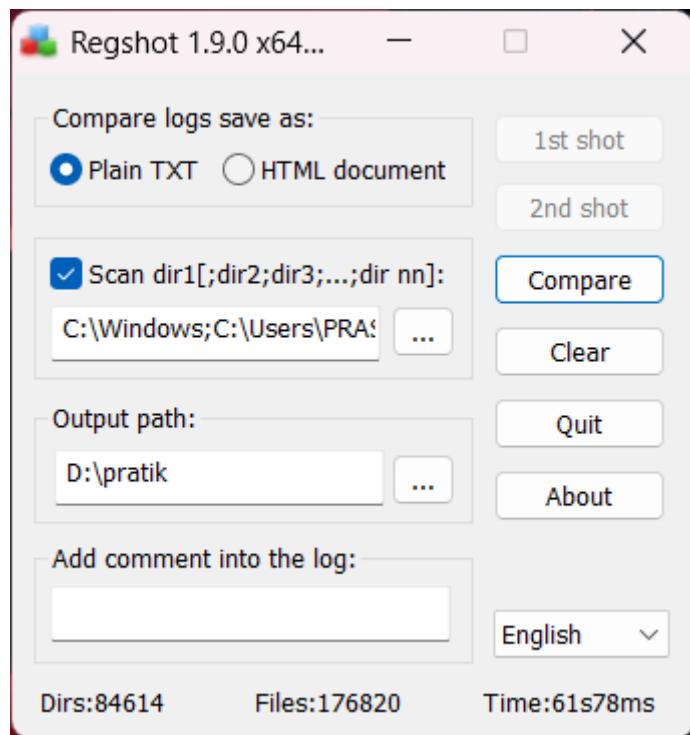


Fig 20

- **Process Monitoring Using TCPVIEW**

TCPView is a Windows network monitoring tool developed by Microsoft Sysinternals that provides a real-time list of all TCP and UDP endpoints on your system — including the local and remote addresses, ports, and associated processes (PIDs).

- Download and setup tcpview tool.
- Now open tcpview .

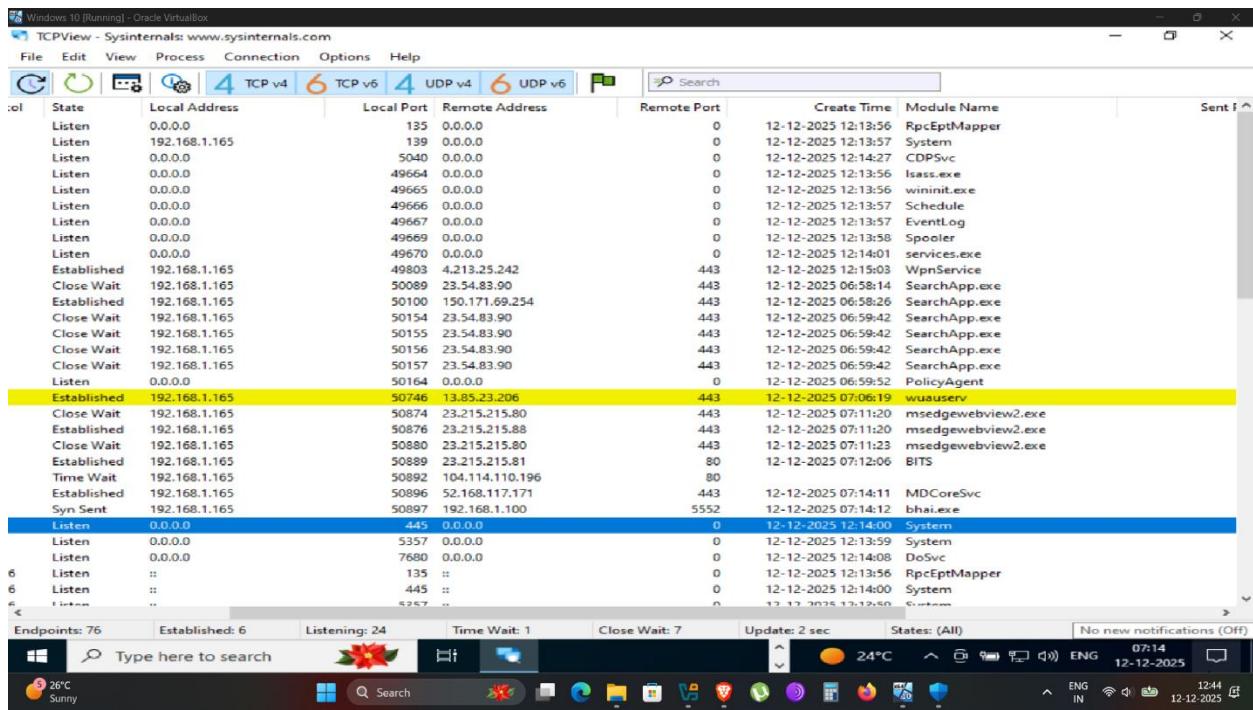


Fig 21

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

RESULT:

- Shows all current TCP/UDP connections, local & remote IP addresses, and port numbers.
- Helps detect unknown or malicious processes making network connections.
- Displays which process is using which port (useful in troubleshooting port conflicts).
- Connections change live, making it easy to track new or closed sessions.
- Useful for analyzing network delays, unauthorized connections, or malware behavior.
- Clearly links process name ↔ network connection (better than netstat).

- **Dynamic Analysis using Currport**

CurrPorts is used in dynamic malware analysis to monitor real-time network connections and associated processes.

- Download and setup the currport .
- Now see all process and ports .

Process...	Proce...	Proto...	Local P...	Local Addr...	Remot...	Remote Adr...	Remote Host...	State	Sent Bytes	Received B...	Sent Pac...	Receive...	Process Path	Product Name	File Description
AvastSvcs...	4656	TCP	27275	127.0.0.1		0.0.0.0		Listening					AvastSvcs.exe		
AvastSvcs...	4656	TCP	49769	192.168.157...	7500	34.74.148...	245.148.74.34...	Establish...					AvastSvcs.exe		
AvastSvcs...	4656	TCP	50226	192.168.157...	443	34.98.110.65	65.110.93.48...	Establish...					AvastSvcs.exe		
AvastSvcs...	4656	TCP	50454	192.168.157...	443	23.60.172...	a23.60-172-18...	Establish...					AvastSvcs.exe		
brave.exe	13032	TCP	27275	=1		:	HP	Listening					AvastSvcs.exe		
brave.exe	13032	TCP	50436	192.168.157...	443	https	18.245.60...	server-18-245...	Establish...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50438	192.168.157...	443	https	18.239.111...	server-18-239...	Establish...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50439	192.168.157...	443	https	18.239.111...	server-18-239...	Establish...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50443	192.168.157...	443	https	18.239.153...	server-18-239...	Establish...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50445	192.168.157...	443	https	35.160.251...	ec2-35-160-25...	Close W...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50446	192.168.157...	443	https	108.159.80...	server-108-159...	Establish...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50447	192.168.157...	443	https	18.239.153...	server-18-239...	Establish...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50449	192.168.157...	443	https	107.190.138...	hdserver1nriso...	Close W...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50450	192.168.157...	443	https	142.250.182...	bom0729-in-f...	Establish...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50452	192.168.157...	443	https	142.250.76...	bom1210-in-f...	Establish...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50457	192.168.157...	443	https	52.89.182...	ec2-52-89-182...	Close W...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
brave.exe	13032	TCP	50458	192.168.157...	443	https	35.160.251...	ec2-35-160-25...	Establish...				C:\Users\aniket\AppData\Local\BraveSoftware\Brave Browser	Brave Browser	Brave Browser
chrome.exe	12668	TCP	64555	192.168.157...	5228	142.251.175...	sh-in-1188.1e1...	Establish...				C:\Program Files\Google\Chrome\Application...	Google Chrome	Google Chrome	
chrome.exe	15036	UDP	5353	=		HP							C:\Program Files\Google\Chrome\Application...	Google Chrome	Google Chrome
IPMediaNL	12008	TCP	50455	192.168.157...	443	https	148.11.133...	ns5033994(p-...	Establish...				C:\Program Files\HP\HP Media Network\HP...	HP Recommends	HP Recommends
pfsvc.exe	4632	TCP	49705	127.0.0.1	49706	127.0.1	HP	Establish...					ipfsvc.exe		
pfsvc.exe	4632	TCP	49706	127.0.0.1	49705	127.0.0.1	HP	Establish...					ipfsvc.exe		
hi_service...	6336	TCP	49675	=1		:	HP	Listening					jhi_service.exe		
sass.exe	1432	TCP	49664	0.0.0.0		0.0.0.0		Listening					lsass.exe	Microsoft® Windows® ...	Local Security Aut
sass.exe	1432	TCP	49664	=		:	HP	Listening					lsass.exe	Microsoft® Windows® ...	Local Security Aut
MSSHHOST...	6688	TCP	6646	0.0.0.0		0.0.0.0		Listening					MSSHHOST.exe		
MSSHHOST...	6688	UDP	6646	0.0.0.0		0.0.0.0		Listening					MSSHHOST.exe		
msedgewe...	14144	TCP	50941	0.0.0.0		0.0.0.0		Listening					C:\Program Files (x86)\Microsoft\EdgeWebV...	Microsoft Edge WebView...	Microsoft Edge W...
nessusd.exe	7760	TCP	8834	0.0.0.0		0.0.0.0		Listening					nessusd.exe		
nessusd.exe	7760	TCP	49729	127.0.0.1	49730	127.0.1	HP	Establish...					nessusd.exe		
nessusd.exe	7760	TCP	49730	127.0.0.1	49729	127.0.1	HP	Establish...					nessusd.exe		
nessusd.exe	7760	TCP	49733	127.0.0.1	49734	127.0.1	HP	Establish...					nessusd.exe		
nessusd.exe	7760	TCP	49734	127.0.0.1	49733	127.0.1	HP	Establish...					nessusd.exe		
maxscript...	7720	TCP	8834	=		-	-	Listening					maxscript.exe		

Fig 22

- **Curport used for:**

- Displays active TCP/UDP network connections.
- Shows process name, PID, local & remote ports.
- Identifies suspicious outbound connections.
- Helps monitor live network activity of malware.
- Useful for network-based malware detection.

- **Malware Analysis overall summary:-**
- Studied static and dynamic malware analysis techniques.
- Analyzed malware without execution using static tools (BinText, Dependency Walker, Autoruns)
- Observed runtime behavior and network activity using dynamic tools (TCPView, CurrPorts).
- Identified persistence mechanisms, DLL dependencies, and readable strings
- Monitored active connections, ports, and suspicious processes
- Understood how malware communicates, persists, and impacts system security
- This module improved threat detection, analysis, and incident response skills