-ATHARVA KATKAR

INDEX

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

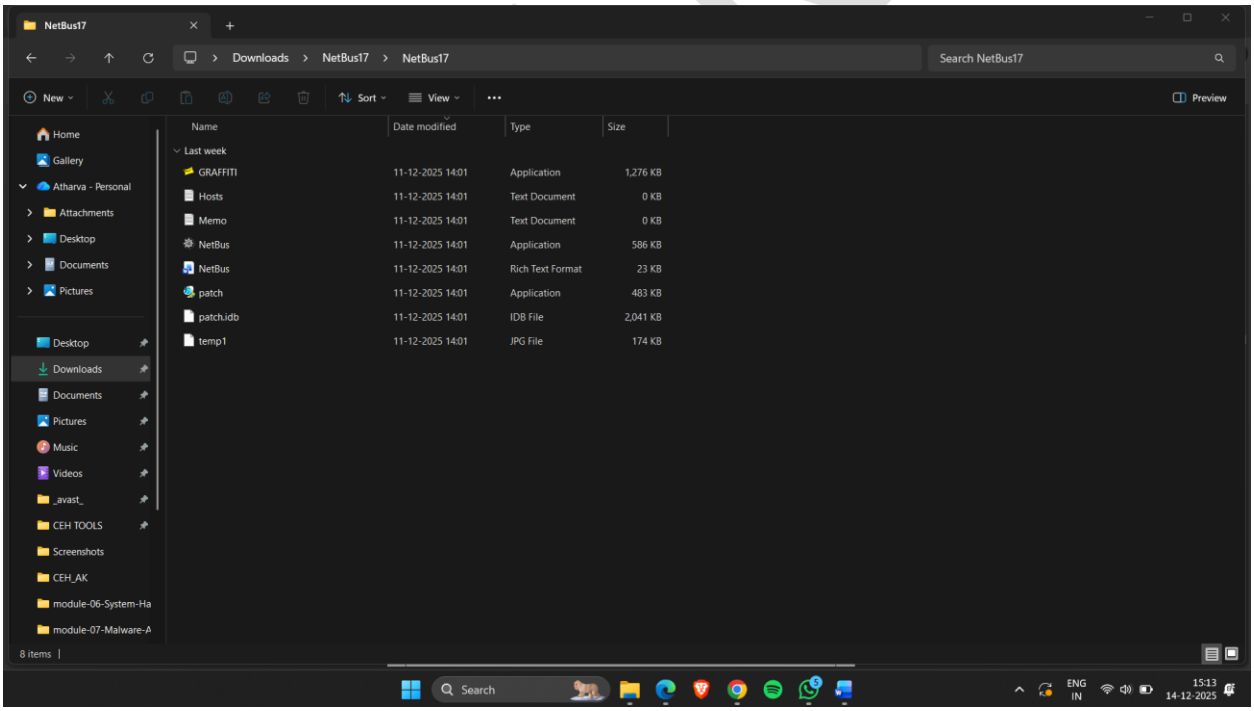

Fig 1

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

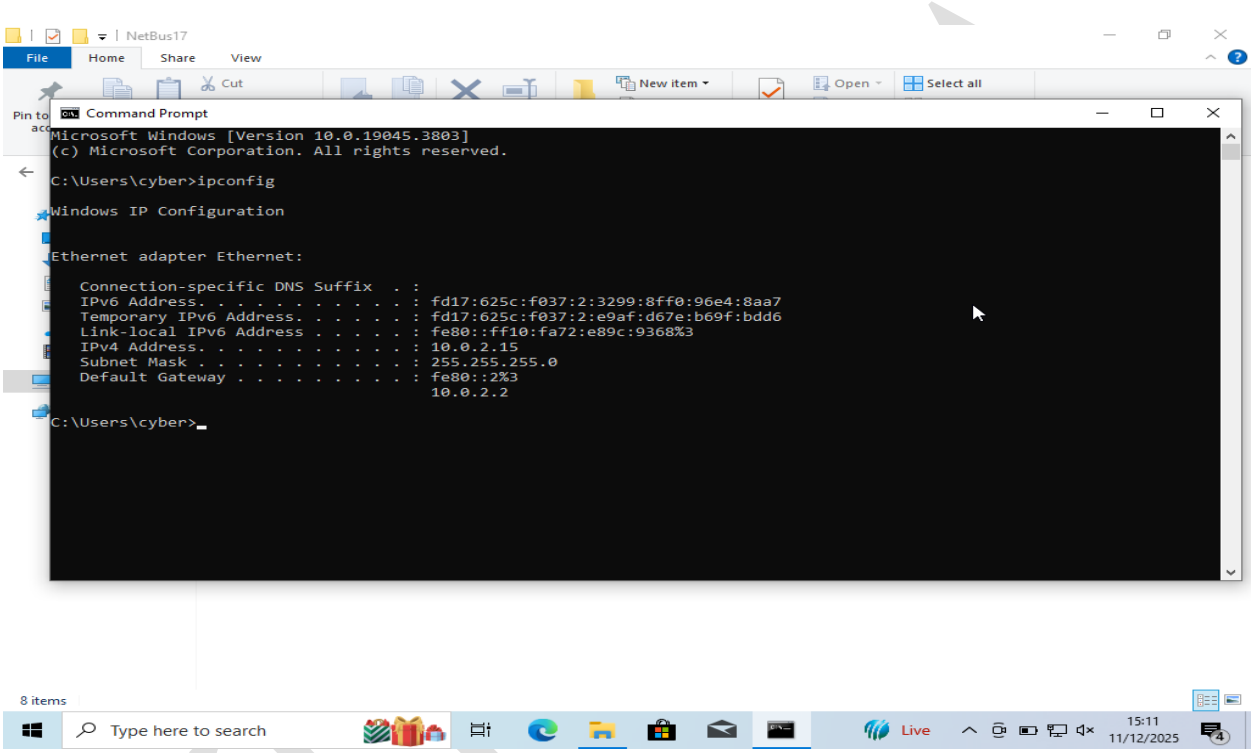

Fig 2

- 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.

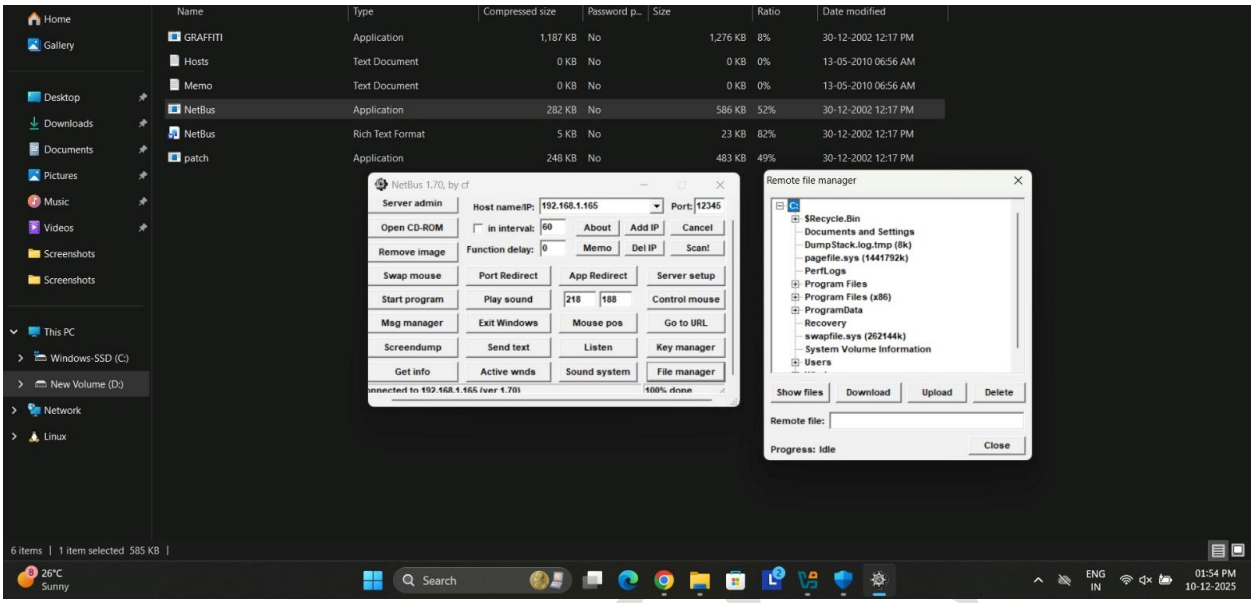

Fig 3

- 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 .

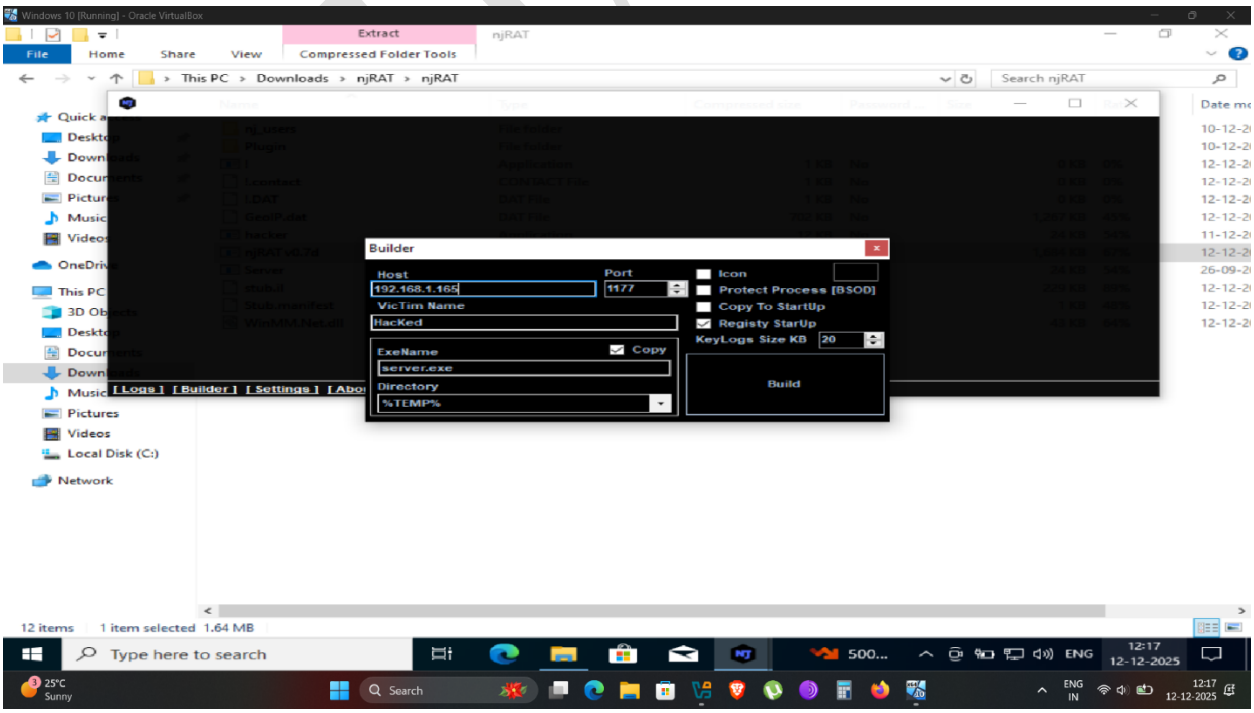

Fig 5

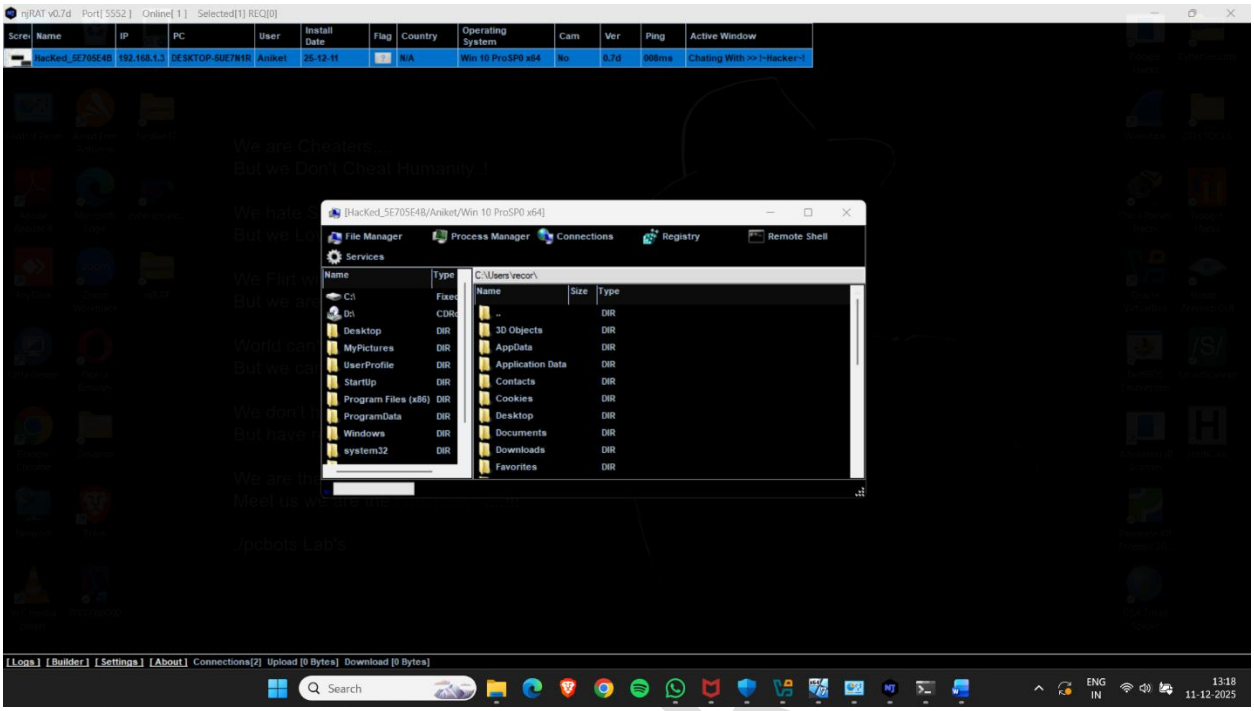

Fig 6

- 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

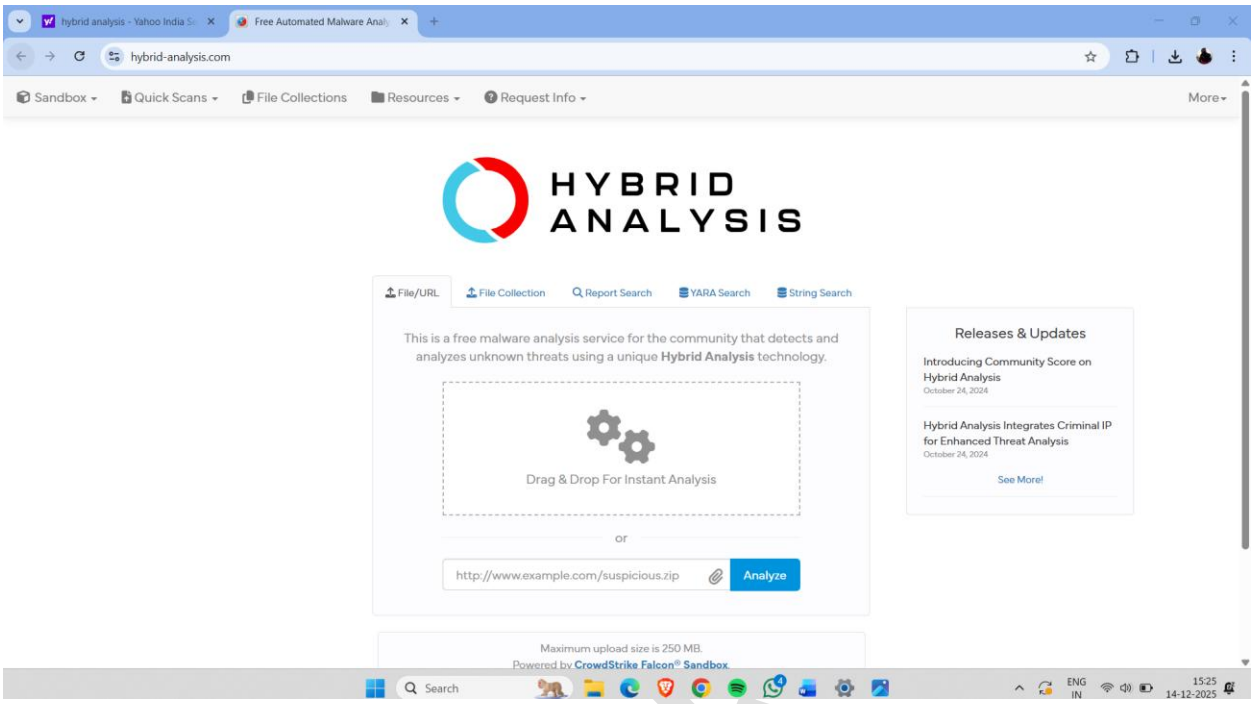

Fig 7

- Add file that you want to

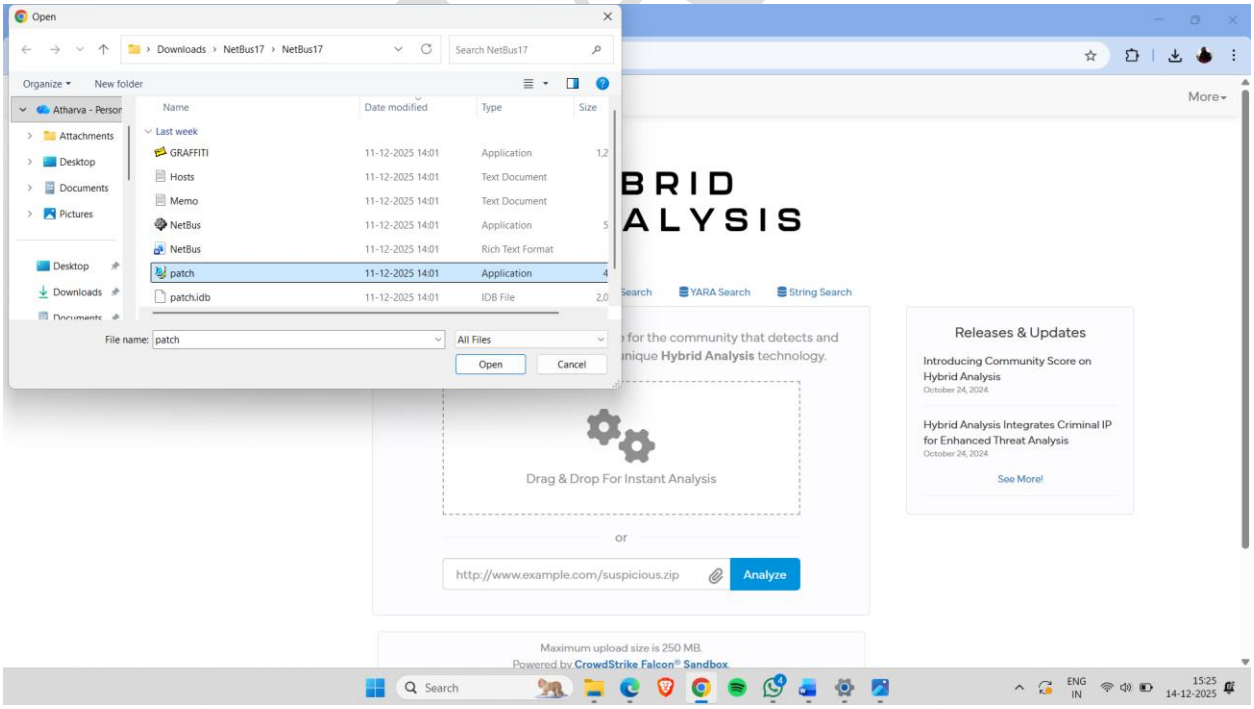

Fig 8

- Here scan completed and says it is a malicious file

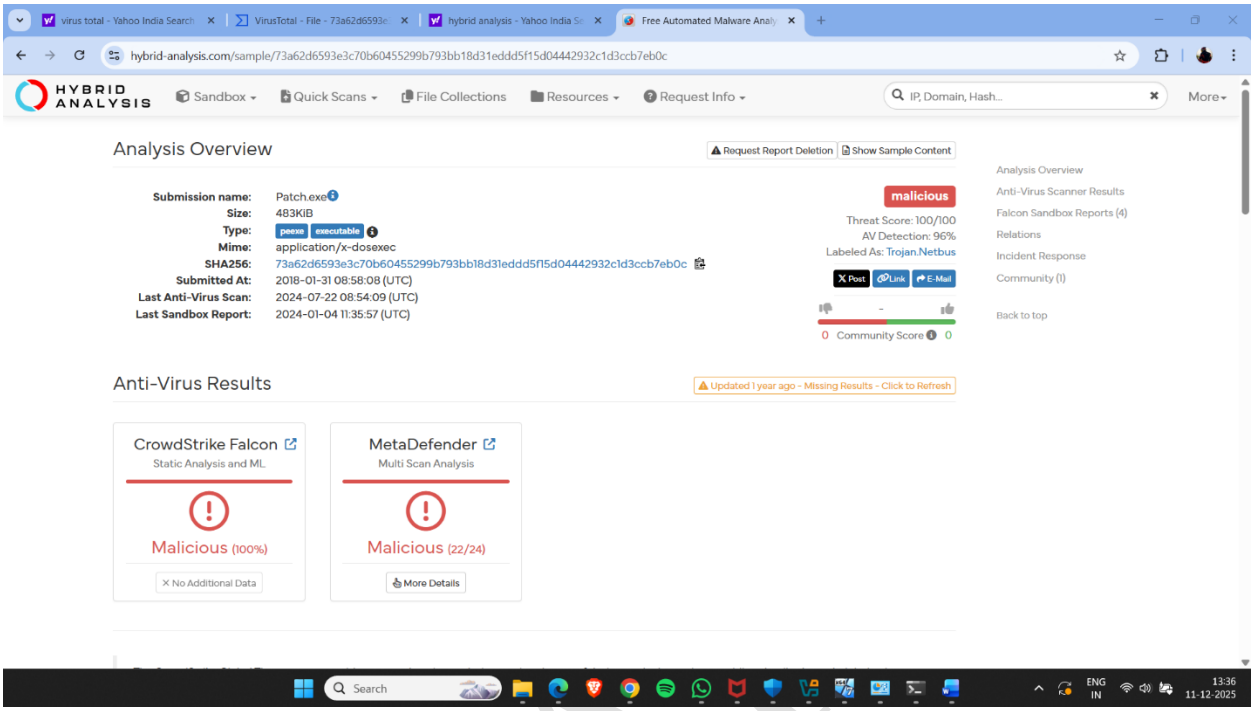

Fig 9

- 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

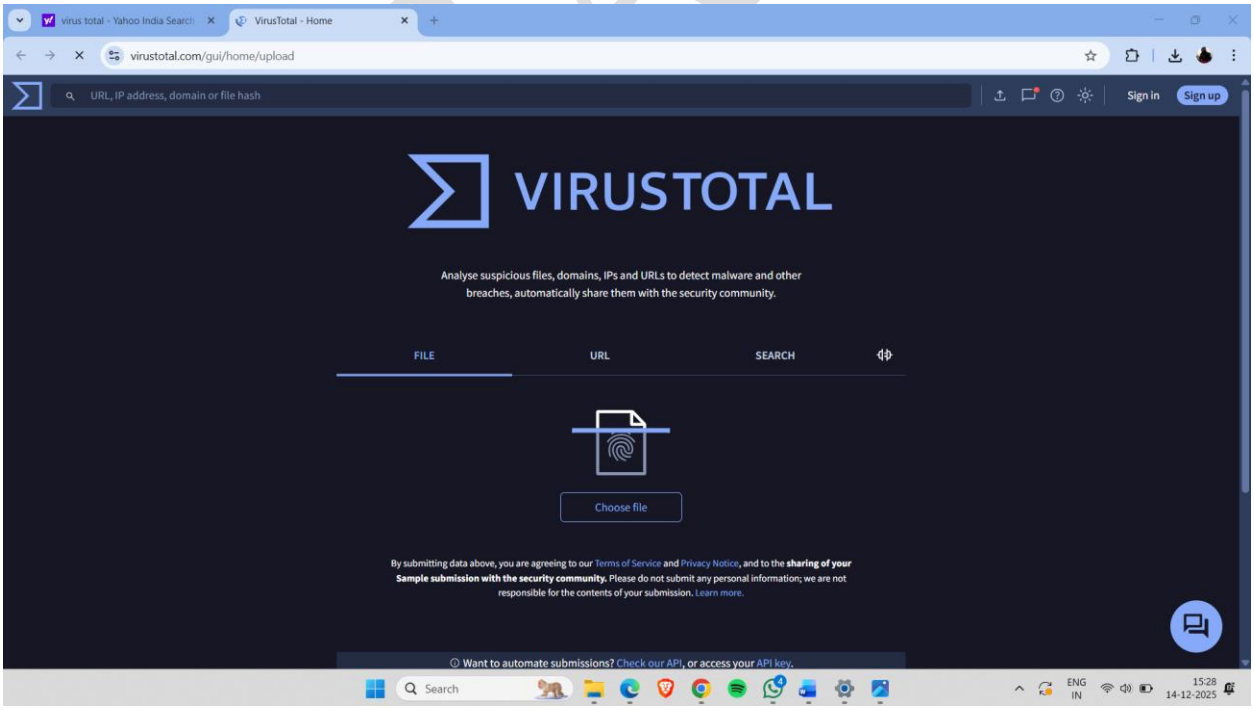

Fig 10

- Now select file that you want to scan.

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

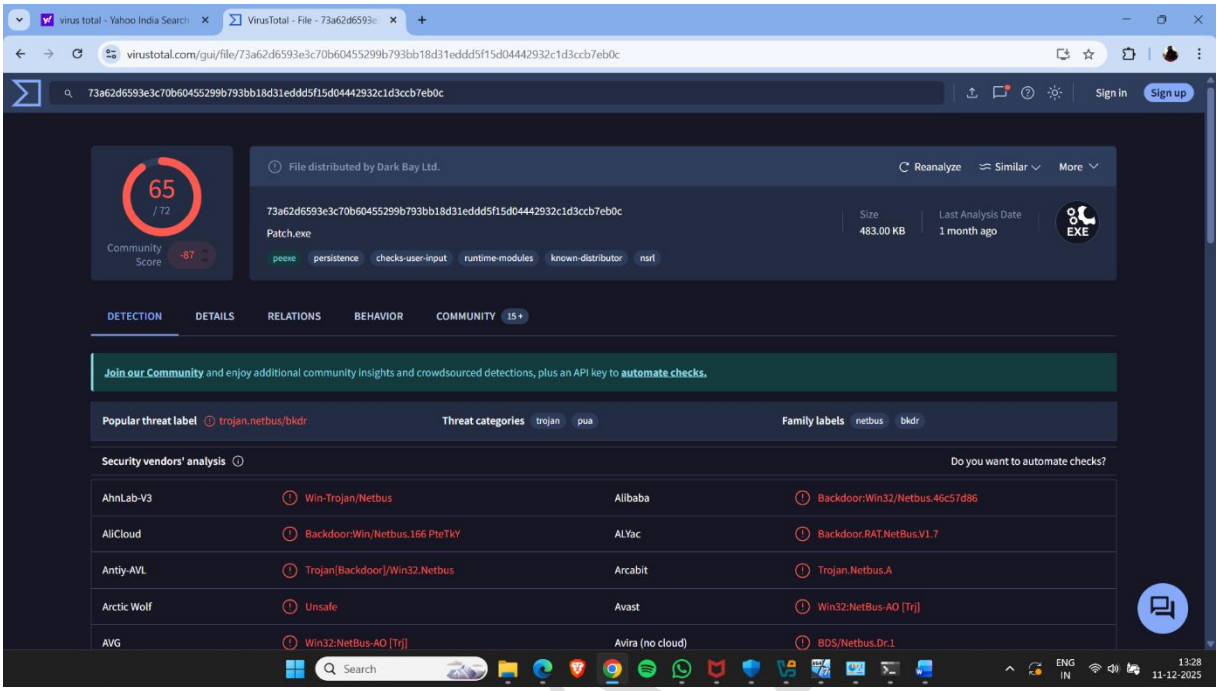

Fig 11

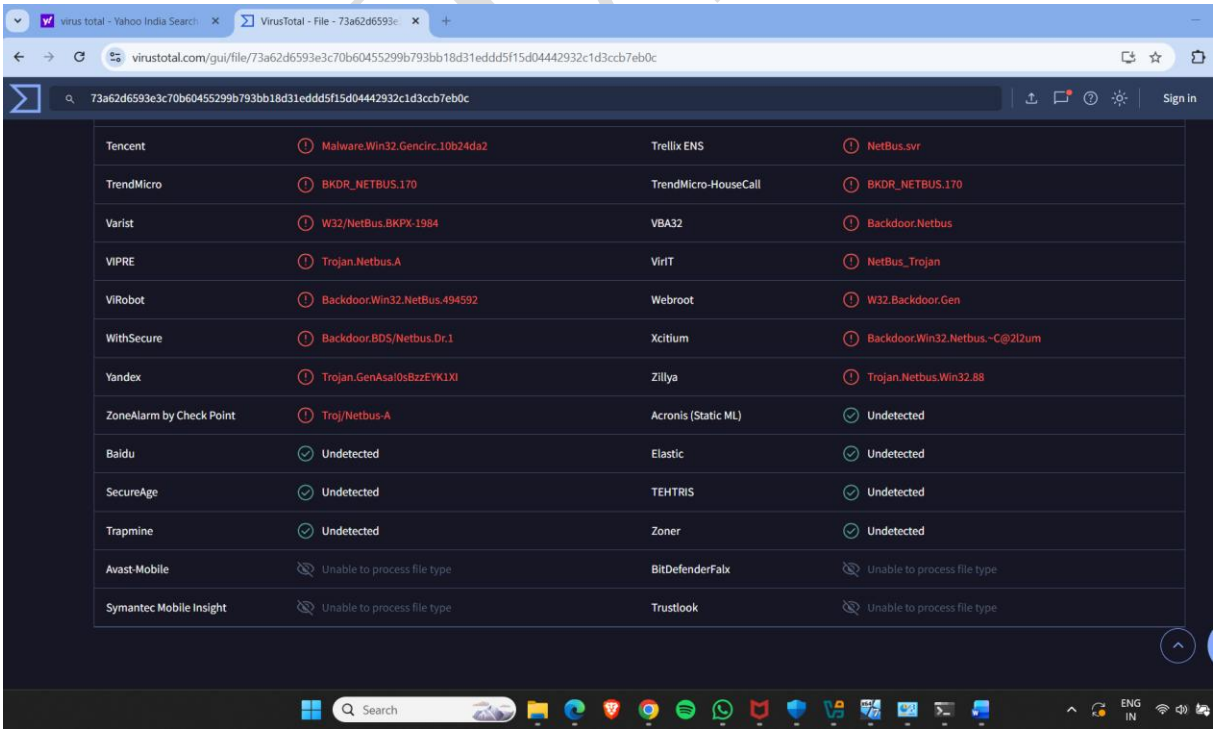

Fig 12

- **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.

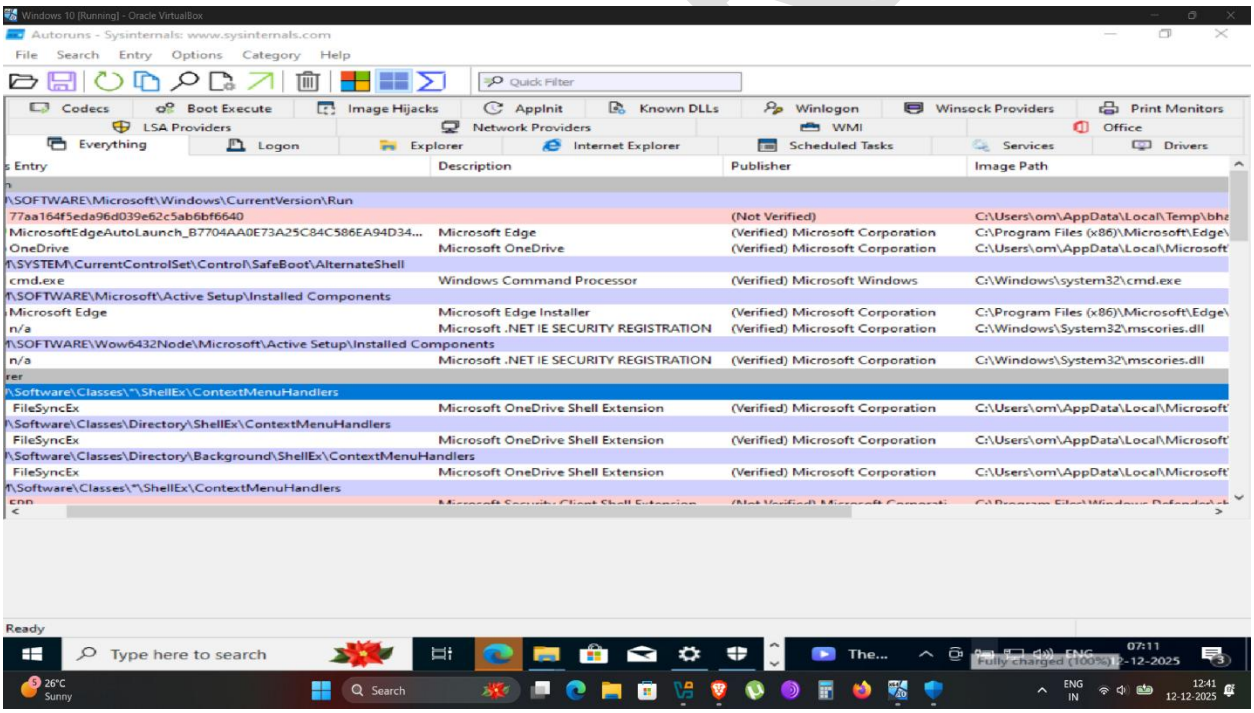

Fig 13

- 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 .

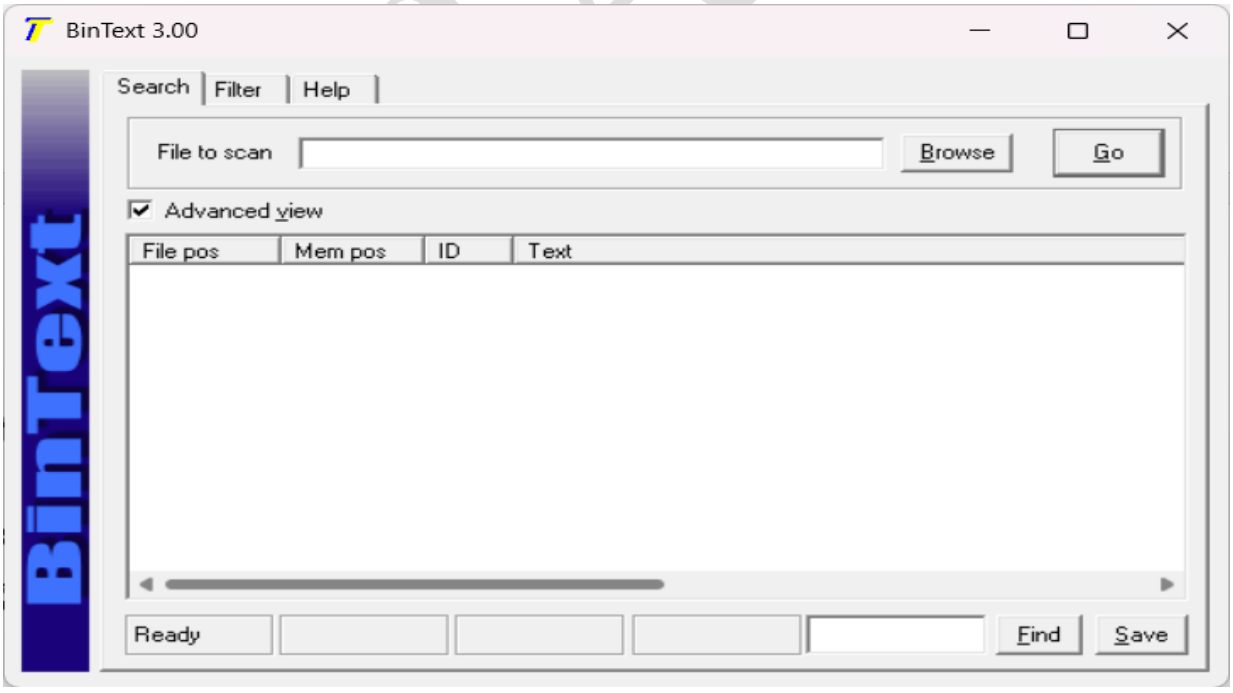

Fig 14

- Now selected file is under scan .

- Here,Result is generated .

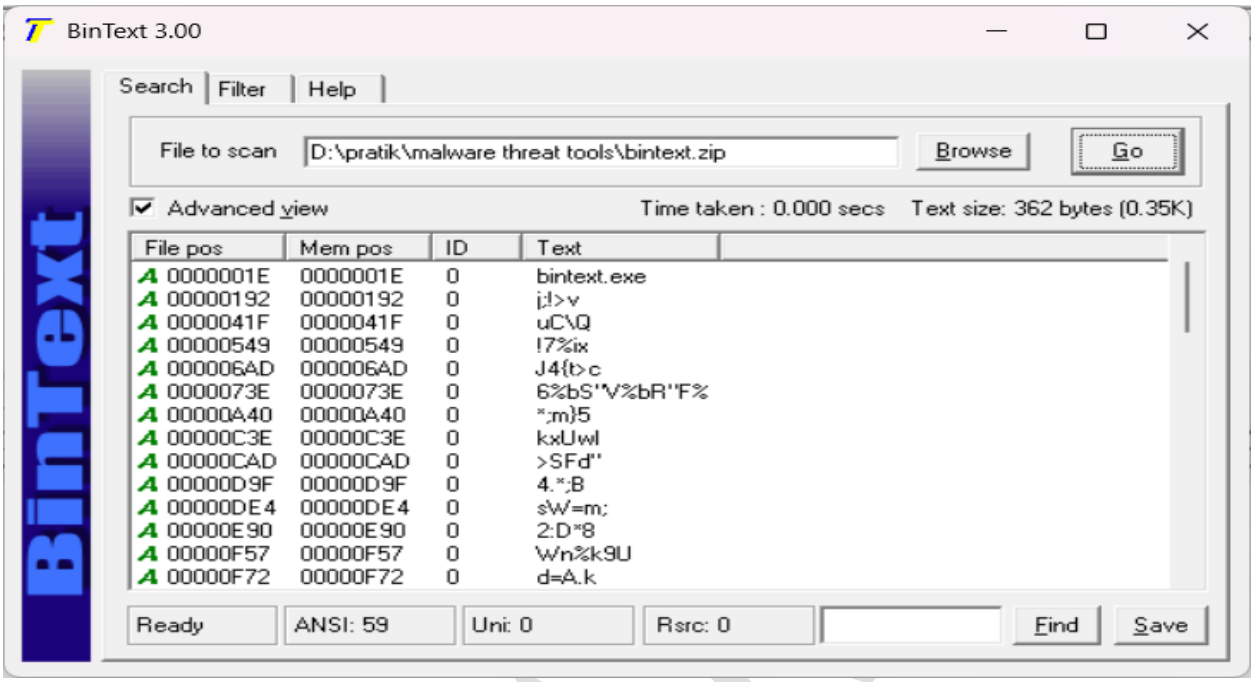

Fig 15

- Here is scanning output .

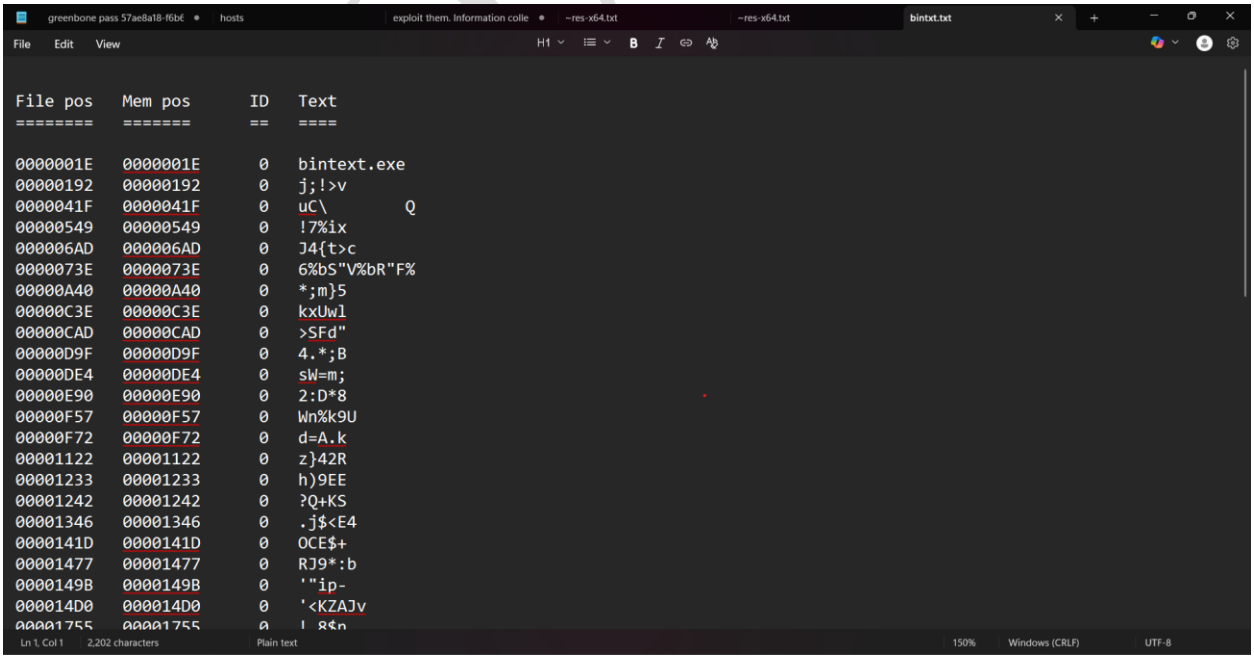

Fig 16

- **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.

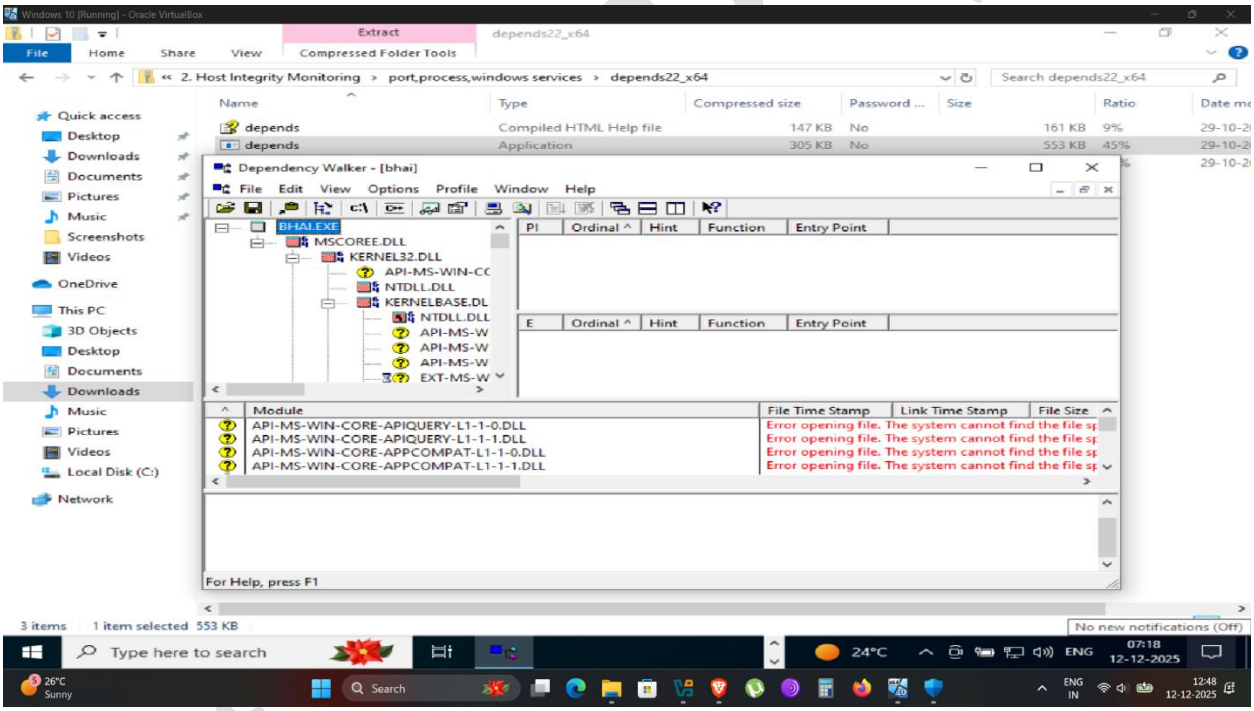

Fig 17

- 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

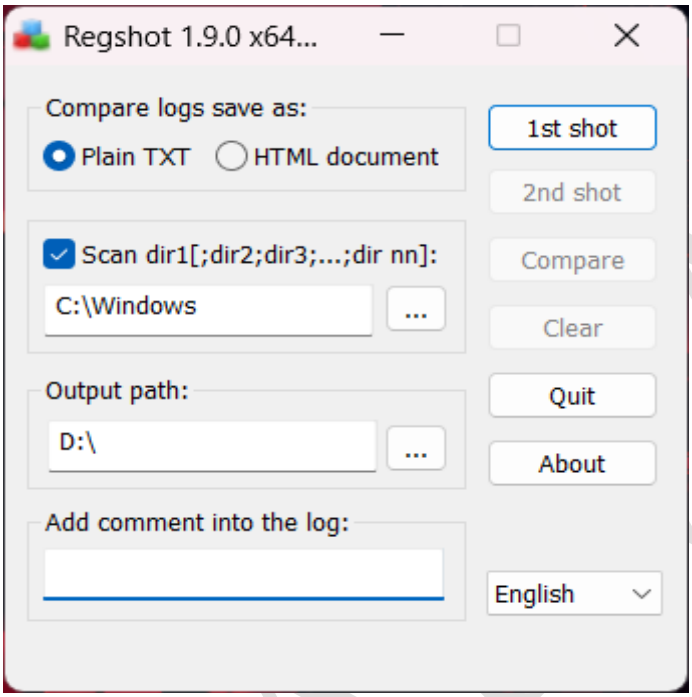

Fig 18

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

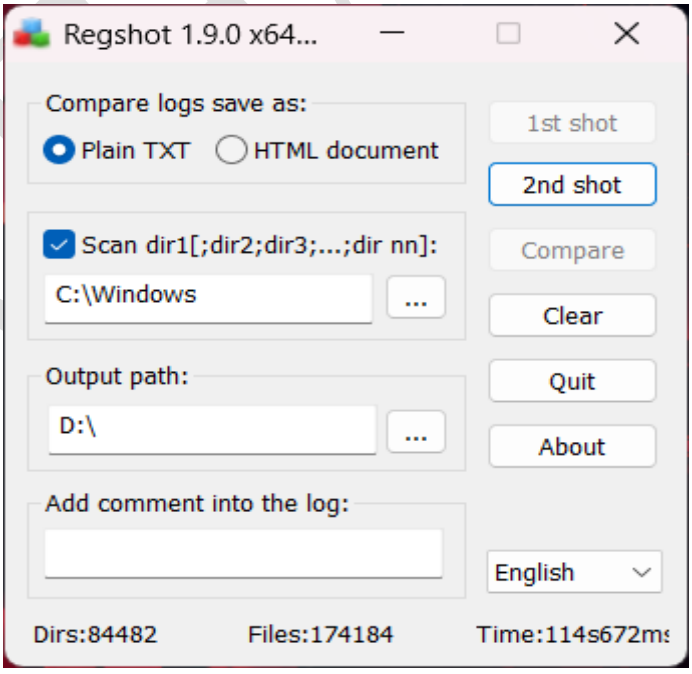

Fig 19

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

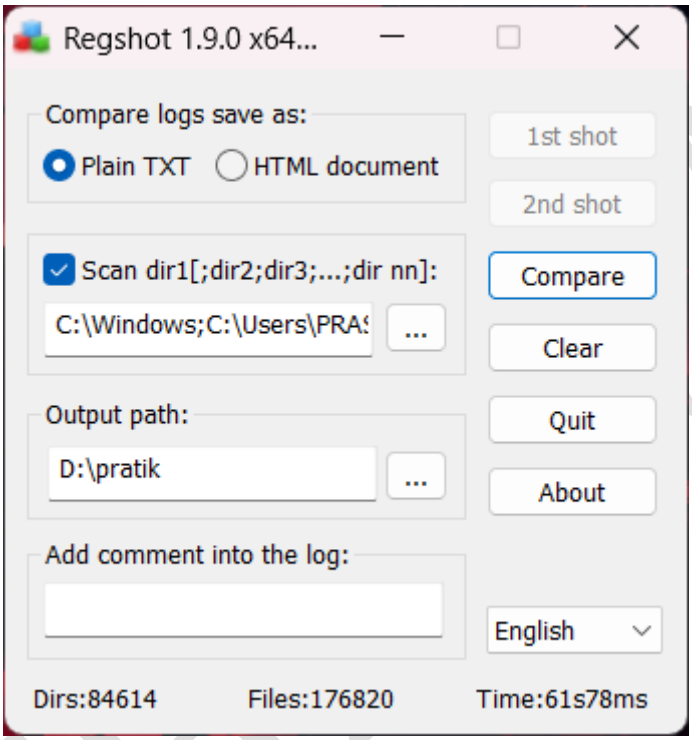

Fig 20

- **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 .

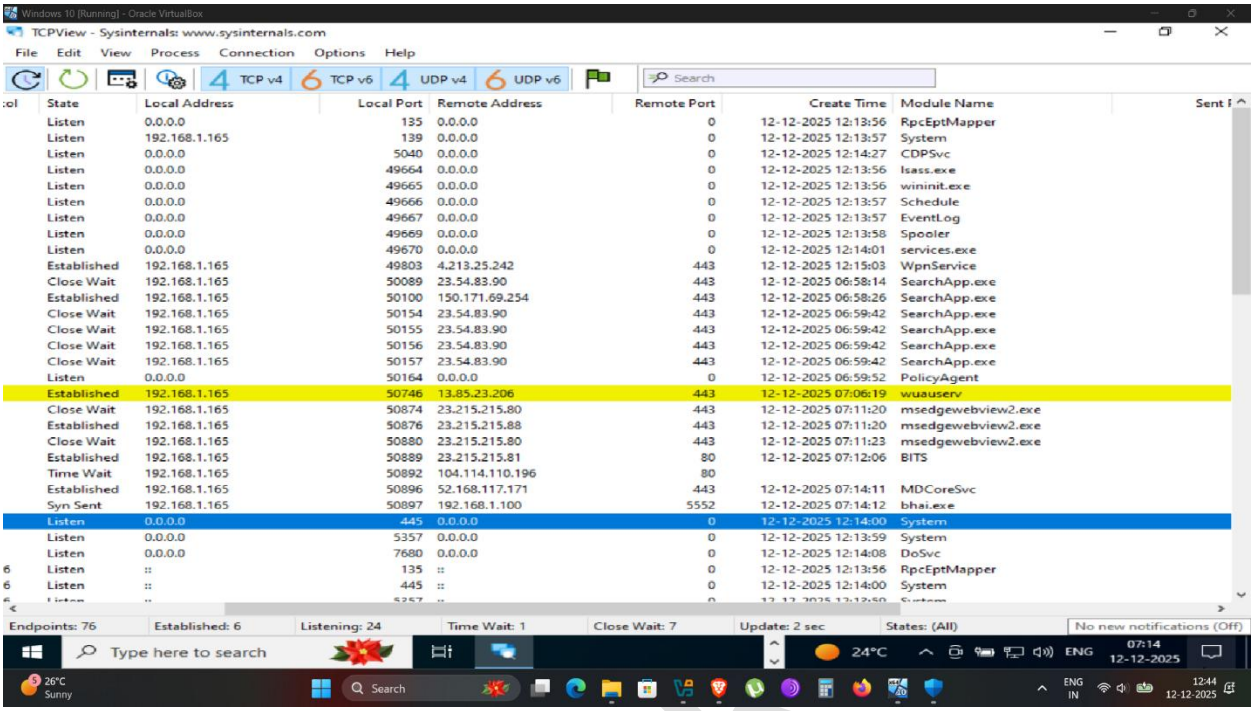

Fig 21

- 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 .

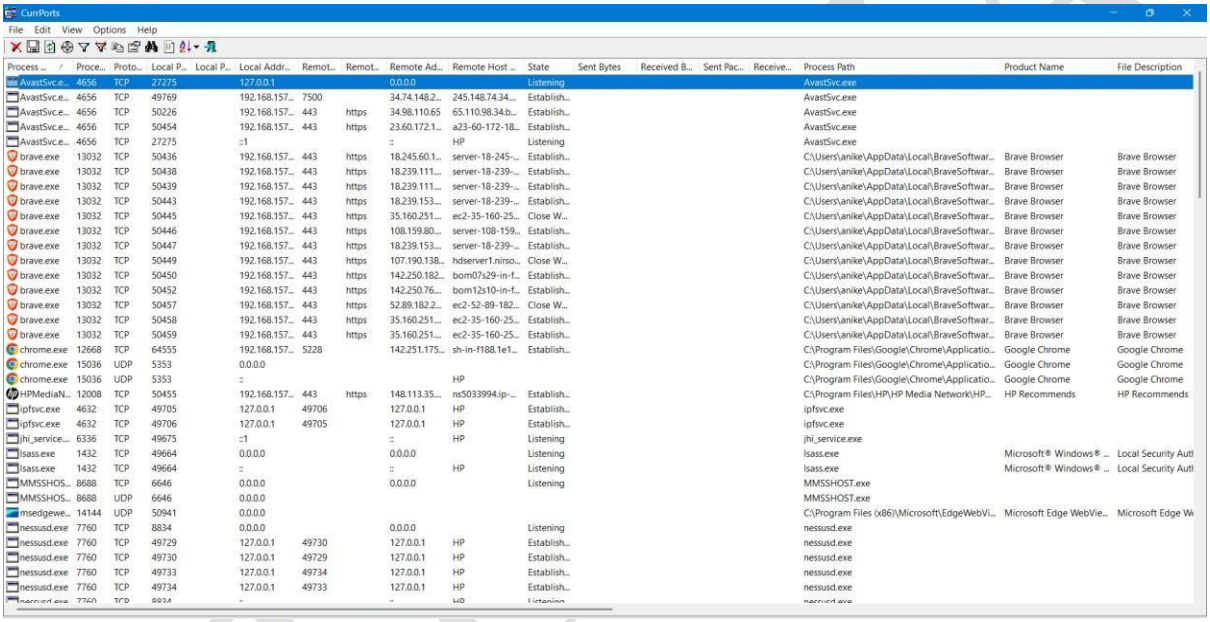

Fig 22

- **Currport 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