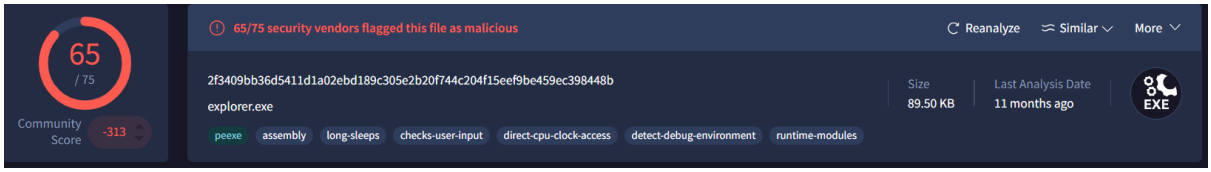
Malware Analysis

Task info:

Trojan.GenericKD.3943952 Trojan.GenericKD.3943952

Hash: 2f3409bb36d5411d1a02ebd189c305e2b20f744c204f15eef9be459ec398448b



Contacted URLs (1)

Scanned	Detections	Status	URL
2024-04-25	0 / 92	-	http://limlim00000.rozblog.com/page/main

Contacted Domains (4)

Domain	Detections	Created	Registrar
limlim00000.rozblog.com	0 / 94	2009-12-07	OnlineNIC, Inc.
rozblog.com	0 / 94	2009-12-07	OnlineNIC, Inc.
smtp.mail.yahoo.com	0 / 94	1995-01-18	MarkMonitor Inc.
www.google.com	0 / 94	1997-09-15	MarkMonitor Inc.

Contacted IP addresses (16)

IP	Detections	Autonomous System	Country
13.107.4.52	0 / 94	8068	US
172.217.11.68	0 / 94	15169	US
172.217.14.68	0 / 94	15169	US
172.217.5.196	0 / 94	15169	US
192.229.211.108	0 / 94	15133	US
20.22.113.133	0 / 94	8075	US
20.99.133.109	0 / 94	8075	US
20.99.184.37	0 / 94	8075	US
20.99.186.246	0 / 94	8075	US
23.216.147.61	0 / 94	20940	US

Execution Parents (5)

Scanned	Detections	Type	Name
2023-07-31	6 / 68	Win32 EXE	MalwareDownloader.dll
2024-08-07	65 / 75	Win32 EXE	d (95).exe
2022-02-04	50 / 61	ZIP	Malware.zip
2023-07-31	28 / 57	ISO image	DeadlyNightShadeIII.iso
2020-09-18	43 / 60	ZIP	ec52b72c369a5d79926790ecdc6aeec47039c58d.zip

Bundled Files (12)

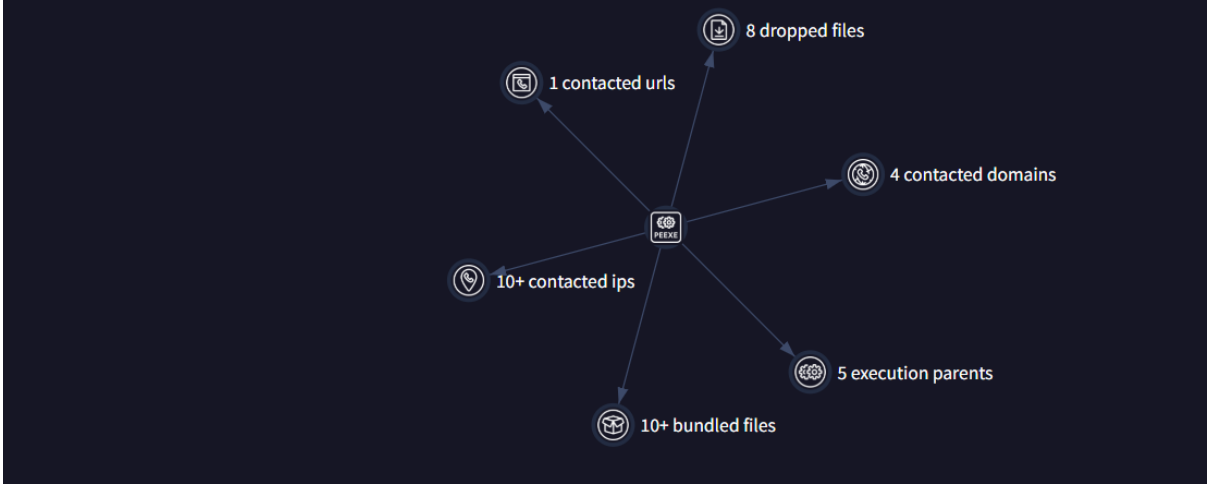
Scanned	Detections	File type	Name
2021-11-23	0 / 56	ICO	81.ico
2025-07-31	0 / 62	XML	1
?	?	file	1a197d491731f88ed07044c1c15f99288ac1e458e8e81965f346c38d76c4cc62
?	?	file	f1185e3ccf71314c365c77b787a2d0735790cebb8abb889ce166b0e0b37d4392
?	?	file	c9689871288363c1d4e480c379cda076cfcf64cf8b53cf22d93767d54c08a395
?	?	file	cf8461030e5b262b86bf4106212e997acfb0a40f0a6e110805ce749c0fbc6382
?	?	file	46d0be879a54e62f9354a3c827ef0aea050b46058d78bd1590ac852008bd2fb3
?	?	file	58f0a84f4520678fadd457efb012ae9a078713b25b2d56978bf0555840890ac7
?	?	file	9143bbd4ab316c01f6ec02c11dc07c20797c40d5055807ba13fa0d9a7776e98b
?	?	file	7e3f8d2df22afee117bb91f6d8d34d45e4d9d0f2eae1bc447fe71fcdce71b837

• • •

Dropped Files (8)

Scanned	Detections	File type	Name
2025-08-01	0 / 61	INI	software.exe:Zone.Identifier
2024-08-07	65 / 75	Win32 EXE	d (95).exe
2024-06-19	38 / 74	Win32 EXE	taskmgr.exe
2016-03-05	0 / 56	Text	.rodata..Lanon.c0575aa61b5f6a7001fb4c730bc31bb9.3499
2023-07-06	0 / 59	JavaScript	executable.exe.log
2024-02-29	0 / 58	JavaScript	executable.exe.log
?	?	file	c6033dce8aff1513326b97066f33381afa07542105242c84b7f6bd690d7853b2
?	?	file	e1aa39b4ddb928403ebb319106e0619095c12273cf37f33fba00ddf4ca873ca8

Graph Summary



There are two primary types of malware analysis: static analysis and dynamic analysis.

STATIC ANALYSIS:

🔎 Binary Analysis (under Static Analysis)

Definition:
Binary analysis means studying a malware file (like .exe) without running it, by looking directly at its binary content — the raw 0s and 1s that make up the file.

```
C:\Users\3520 i5 16GB>strings malware.exe
```

This command disassembles malware.exe and shows its machine instructions in human-readable assembly format.

Disassembly

To disassemble a malware executable and view its low-level assembly instructions

```
C:\Users\3520 i5 16GB>objdump -d malware.exe
```

📝 Note: objdump is available in tools like **MinGW** or **Cygwin** on Windows.

Decompilation

To decompile a binary into a higher-level language (like C), tools like Ghidra or Decompiler tools like RetDec are used.

```
C:\Users\3520 i5 16GB>retdec-decompiler.py malware.exe
```

Signature Analysis

To check a malware sample against a database of known malware signatures (like those in VirusTotal CLI):

```
C:\Users\3520 i5 16GB>vt scan file malware.exe
```

This command uses VirusTotal's CLI to upload and scan the file malware.exe.

Before using, you must configure your VirusTotal API key with:

```
C:\Users\3520 i5 16GB>vt init
```

O/p:-

```
C:\Users\3520 i5 16GB>retdec-decompiler.py malware.exe
[INFO] Decompiling 'malware.exe'...
[INFO] Running pre-processing...
[INFO] Starting decompilation...
[INFO] Saving output to: malware.c
[INFO] Decompilation finished successfully.
```

```
C:\Users\3520 i5 16GB>vt scan file malware.exe
Submitting file: malware.exe
Analysis started...
File ID: 2f3409bb36d5411d1a02ebd189c305e2b20f744c204f15eef9be459ec398448b

Waiting for analysis to complete...

Analysis complete.
Detection: 34/70 vendors flagged this file as malicious.
Scan link: https://www.virustotal.com/gui/file/2f3409bb36d5411d1a02ebd189c305e2b2
```

DYNAMIC ANALYSIS:

Command 1: Nmap Scan for Open Ports

```
C:\Users\3520 i5 16GB>nmap -sV localhost
```

🔍 **What it means:**

Part	Meaning
nmap	This is the network scanning tool you're using.
-sV	This option tells Nmap to detect the version of services running on each open port.

Part	Meaning
localhost	This means you're scanning your own computer (127.0.0.1).

So, this command scans your system to:

- Check which TCP ports are open.
- Identify what services are running on them.
- Find the version of those services.

```
Starting Nmap 7.94 ( https://nmap.org ) at 2025-08-01 14:42 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00032s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 10 microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
```

Column	Meaning
PORT	The open port number and protocol (TCP).
STATE	It's open and accepting connections.
SERVICE	The type of service running on that port.
VERSION	Version info about the service (e.g., Windows 10 services).

So in simple terms:

- Your system is listening on ports 135, 139, and 445.
- These are used by Windows networking and file sharing services.
- Nothing looks suspicious in this scan. (But this is useful when checking for unknown services on infected machines.)

Command 2: netstat -ano

```
C:\Users\3520 i5 16GB>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1020
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:8080         0.0.0.0:0              LISTENING       12284
  TCP    127.0.0.1:8080         127.0.0.1:52012        ESTABLISHED     12284
  UDP    0.0.0.0:1900           *:*                                    1036
```

What it does:

- Lists all active network connections and listening ports on your computer.
- Shows the protocol (TCP/UDP), local address and port, remote address and port, connection state, and PID (Process ID).

Output explained:

Column	Meaning
Proto	Protocol used (TCP or UDP)
Local Address	Your computer's IP and port number
Foreign Address	Remote IP and port connected to (or *:* for UDP listening)
State	Status of the connection (LISTENING, ESTABLISHED, etc.)
PID	The process ID that owns the connection

Command 3: Netstat with PID

```
C:\Users\3520 i5 16GB>netstat -anb

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  RpcSs
 [svchost.exe]
  TCP    127.0.0.1:8080         0.0.0.0:0              LISTENING
 [python.exe]
  TCP    127.0.0.1:8080         127.0.0.1:52012        ESTABLISHED
 [python.exe]
  UDP    0.0.0.0:1900           *:*
  SSDPSRV
 [svchost.exe]
```

What it does:

- Same as netstat -ano but also shows the executable (process) name using the port.
- Requires admin privileges to run.
- Helps link open ports directly to running programs.

Command 4: Netstat with Process Name (Admin Privileges Required)

```
C:\Users\3520 i5 16GB>netstat -anb

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  RpcSs
 [svchost.exe]
  TCP    127.0.0.1:8080         0.0.0.0:0              LISTENING
 [python.exe]
  TCP    127.0.0.1:8080         127.0.0.1:52012        ESTABLISHED
 [python.exe]
  UDP    0.0.0.0:1900           *:*
  SSDPSRV
 [svchost.exe]
```

What it does:

- Shows details about the process with PID 12284.
- Filters the task list by the given PID.

Command 5: Find Process Using PID

```
C:\Users\3520 i5 16GB>tasklist /FI "PID eq 12284"

Image Name                     PID        Session Name        Mem Usage
========================= ======== ======================== ============
python.exe                   12284       Console                    18,500 K
```

What it does:

- Shows details about the process with PID 12284.
- Filters the task list by the given PID.

Name:Shreya pandey

Intern id:120

What this poc intends to achieve

This PoC (Proof of Concept) demonstrates how to analyze suspicious files and detect potential malware by inspecting open ports, active processes, and verifying files using tools like Nmap, Netstat, Tasklist, and VirusTotal. It helps identify malicious behavior without executing the file.