Malware Analysis Using FlareVM

WE Innovate X Zero$ploit

Supervised by : Zeyad Waleed

Prepared by: Omar Hassan – Ali Abdelrahman – Ahmed Taha – Omar Tarek – Noha Sayed – Rami Khaled

1. Prepare the Environment

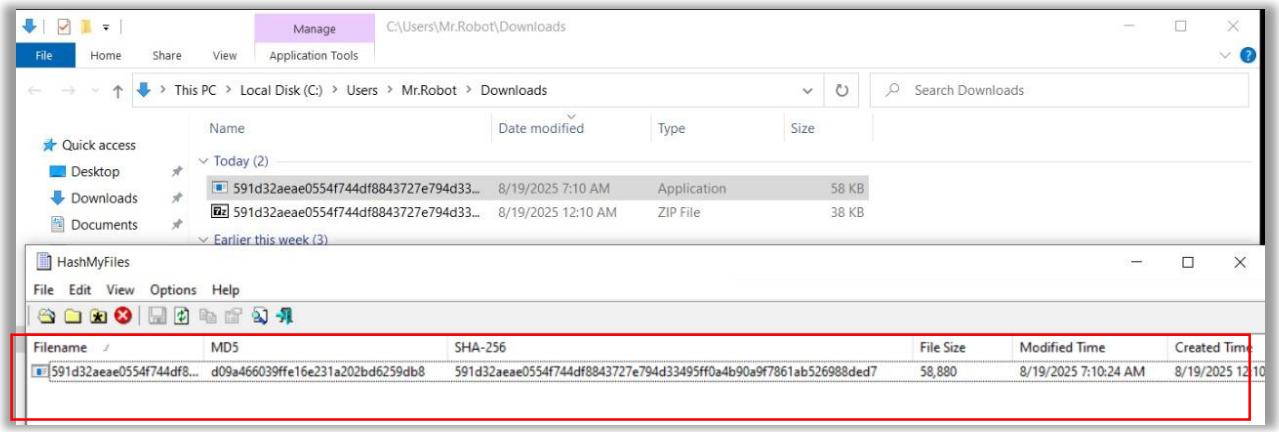
- Make sure you are running in **Flare VM** (isolated Windows VM preloaded with malware analysis tools).
- Take a **snapshot** before analysis (so you can revert if something goes wrong).
- Ensure **network isolation** (disable internet or use controlled lab network).

---

2. Collect Basic File Information

Use built-in tools in Flare VM:

- **File properties** (right-click → Properties): check file size, timestamp, company info.
- Using **HashMyFile or Powershell**



---

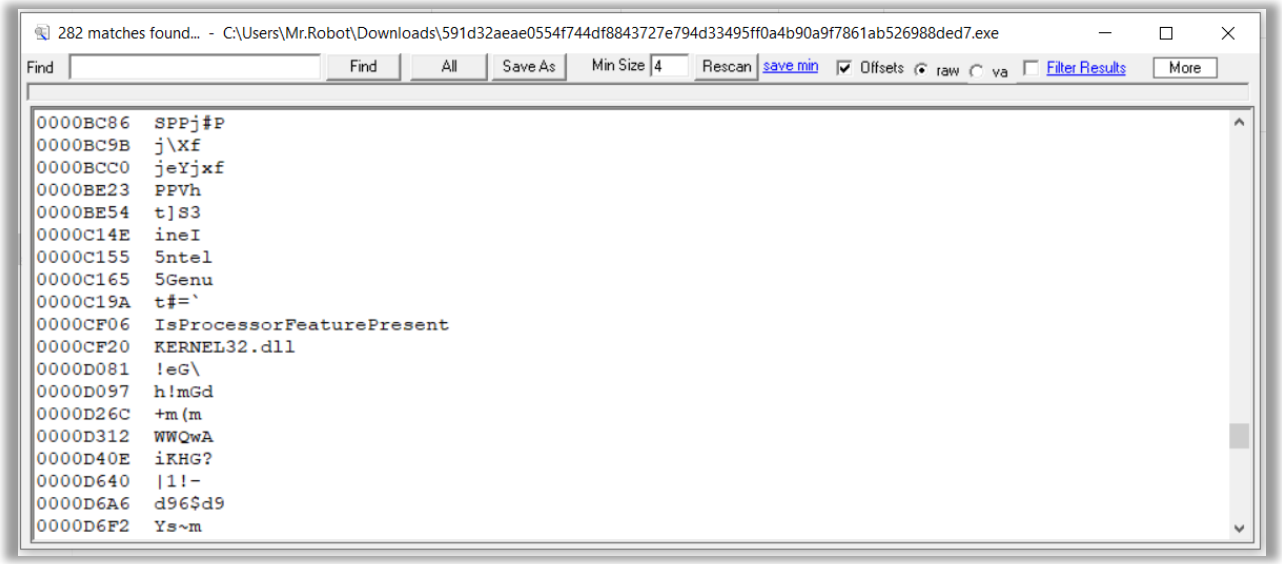
3. Check Strings

Run:

```
strings sample.exe > strings.txt
```

Look for:

- URLs, IPs
- Registry keys
- File paths
- API calls (like VirtualAlloc, LoadLibrary, GetProcAddress)
- Suspicious keywords (e.g., MZ, cmd.exe, powershell, svchost, etc.)

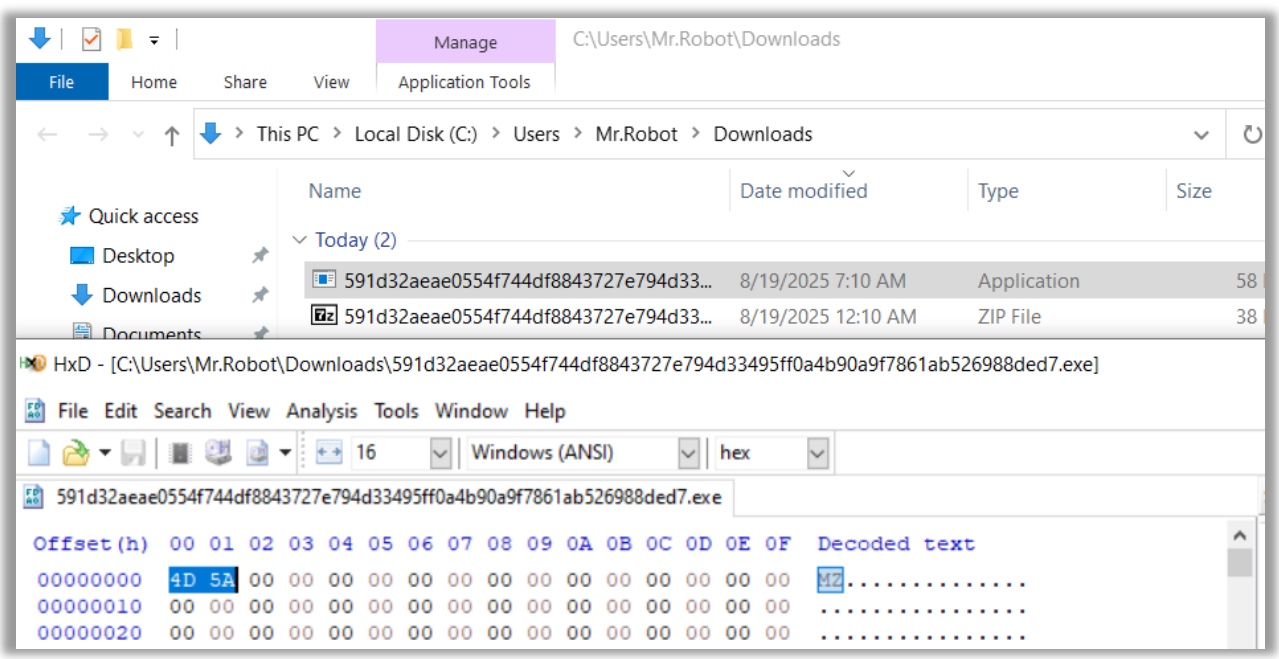


---

4. Inspect File Structure

Use **PE analysis tools**:

- **PEStudio** (GUI) → Shows imported functions, suspicious indicators, entropy, resources.
- **CFF Explorer** or **PE-bear** → Inspect PE headers (sections, imports, exports).

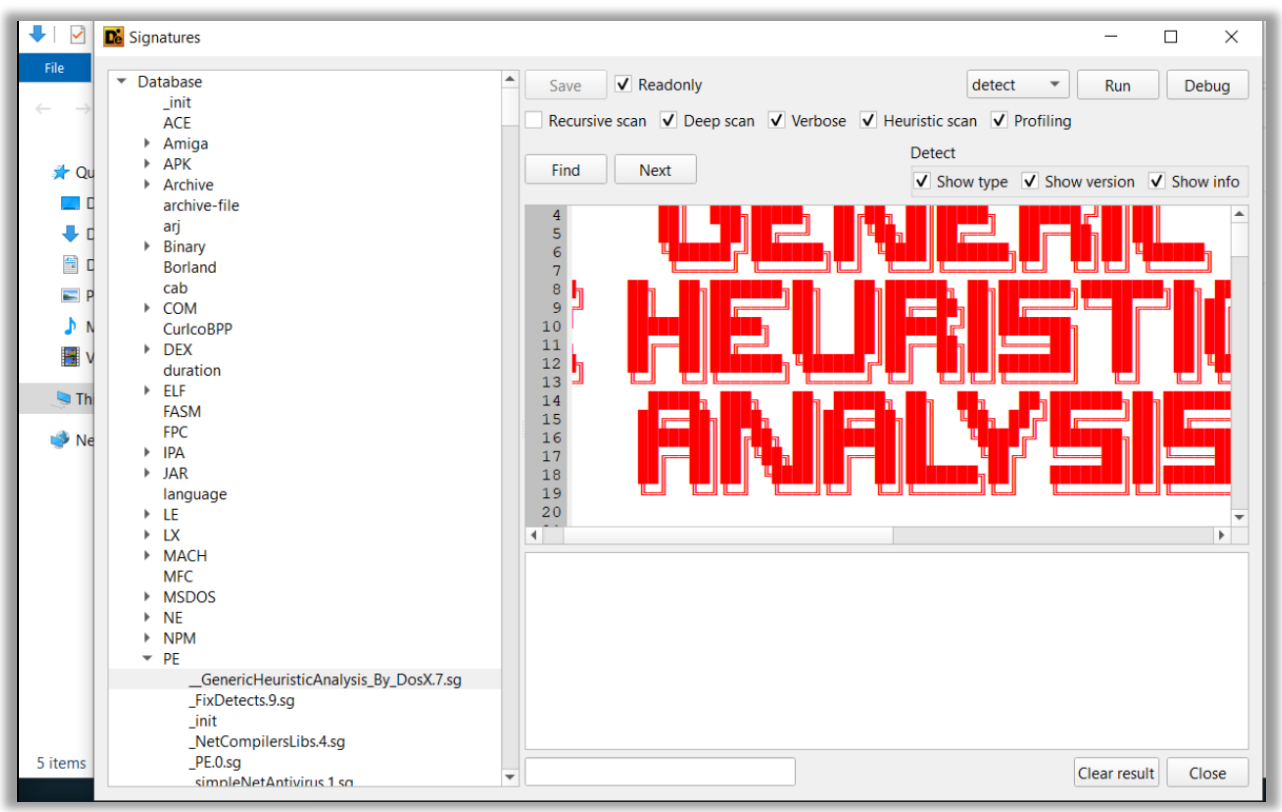


- **Things to check** :
  - Abnormal section names (.text, .rdata, .data, vs unusual names like .xyz).
  - Entropy (high entropy suggests packing/encryption).
  - Imports (API calls like CreateRemoteThread, WriteProcessMemory, InternetOpenUrl)
  -

---

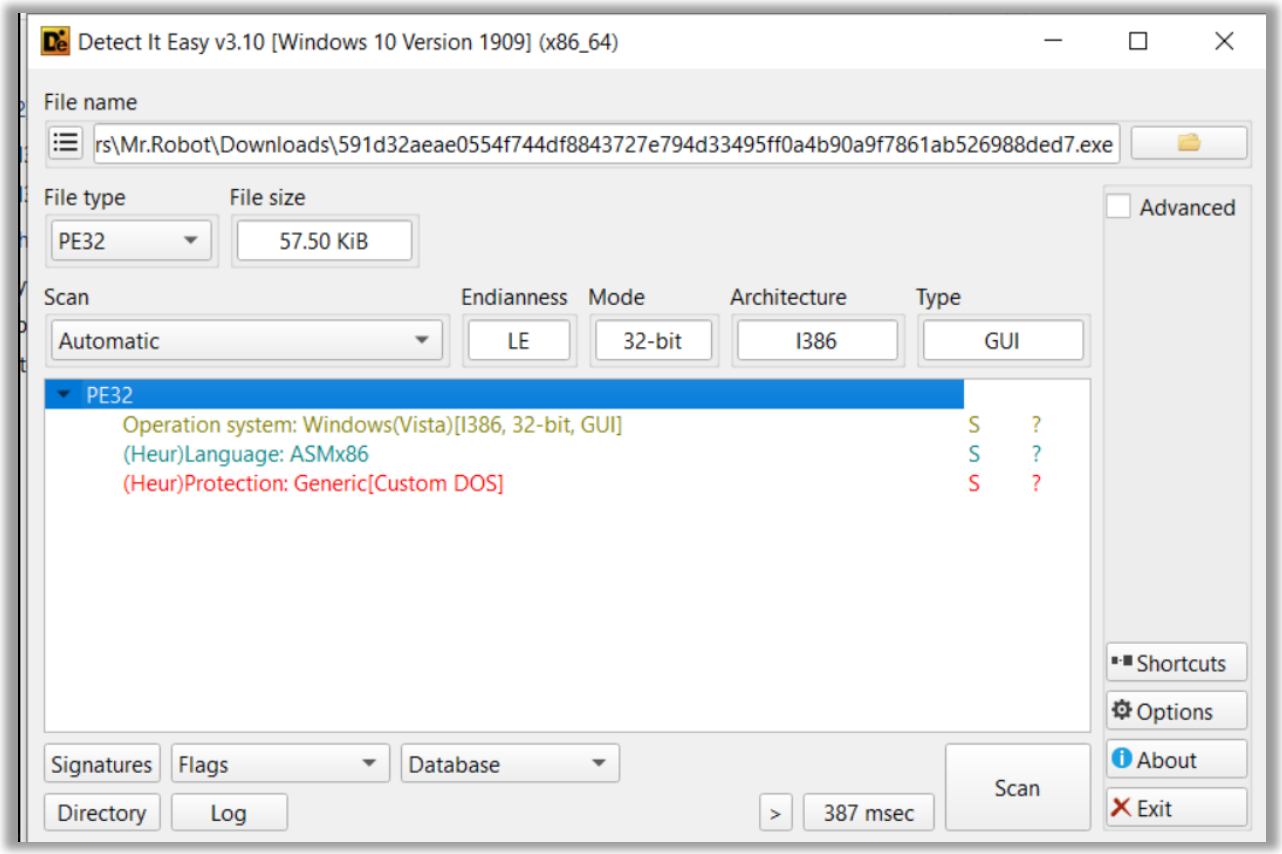
5. Detect Packing or Obfuscation

- Tools:
  - **Detect It Easy (DIE)** → Identifies compiler/packer (UPX, ASPack, Themida, etc.).
  - **PEiD** (old but sometimes useful).
- If packed:
  - Try **unpacking** (e.g., with UPX: upx -d sample.exe).
  - Or prepare for dynamic unpacking later.



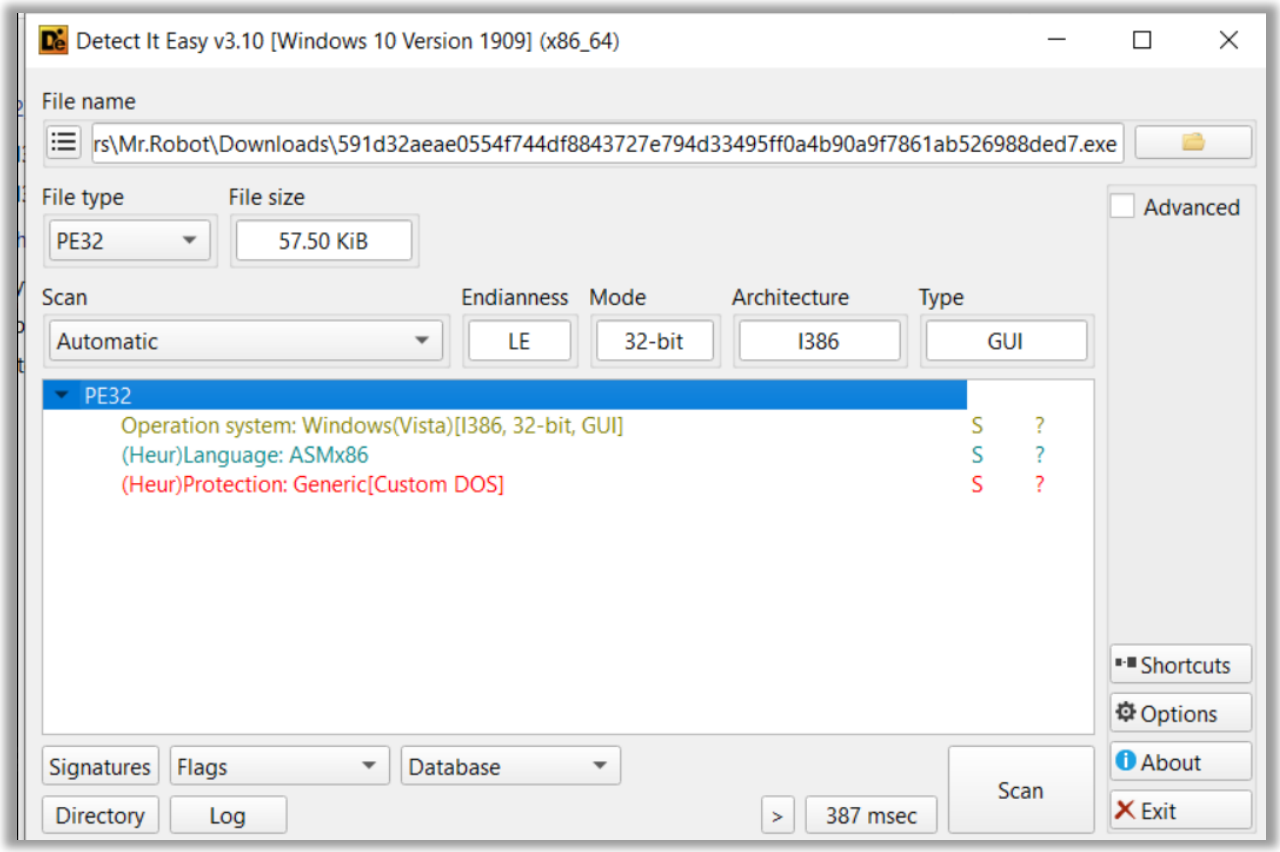
6. Disassemble / Decompile

- Open sample in **IDA Free**, **Ghidra**, or **x64dbg (static mode)**:
  - Look at main() function or entry point.
  - Identify suspicious API calls (networking, process injection, persistence).
  - Trace possible control flow.



7. Analyze Resources

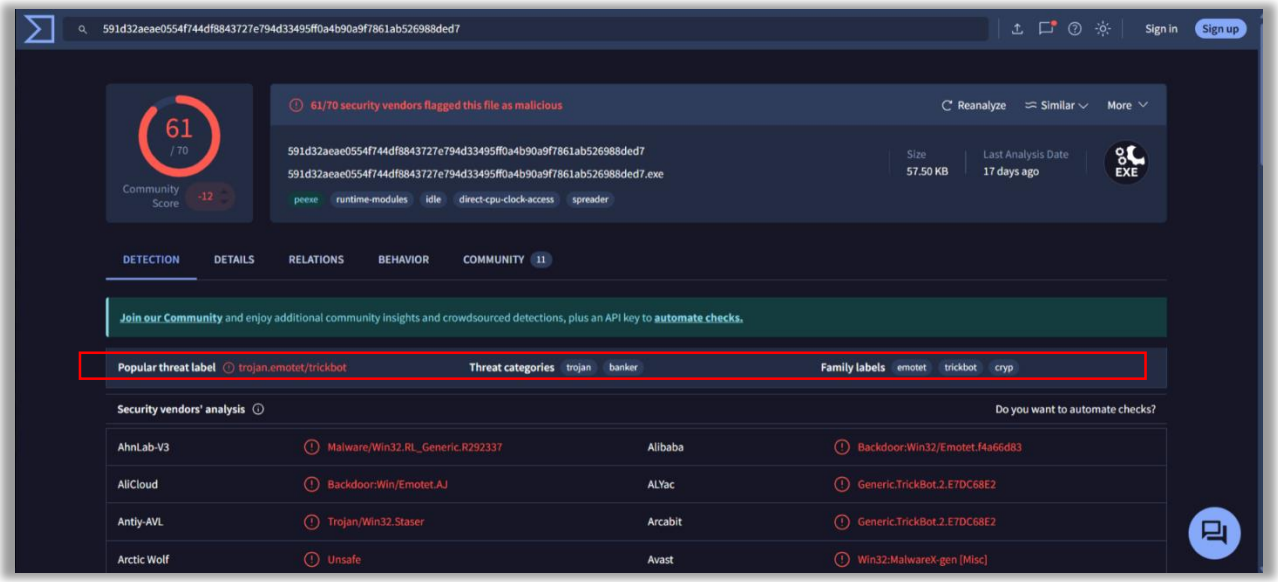
- Use **Resource Hacker** or **PEStudio**:
  - Look at embedded icons, DLLs, scripts.
  - Sometimes malware hides config or payloads in .rsrc.



8. Document Findings

Create a simple report with:

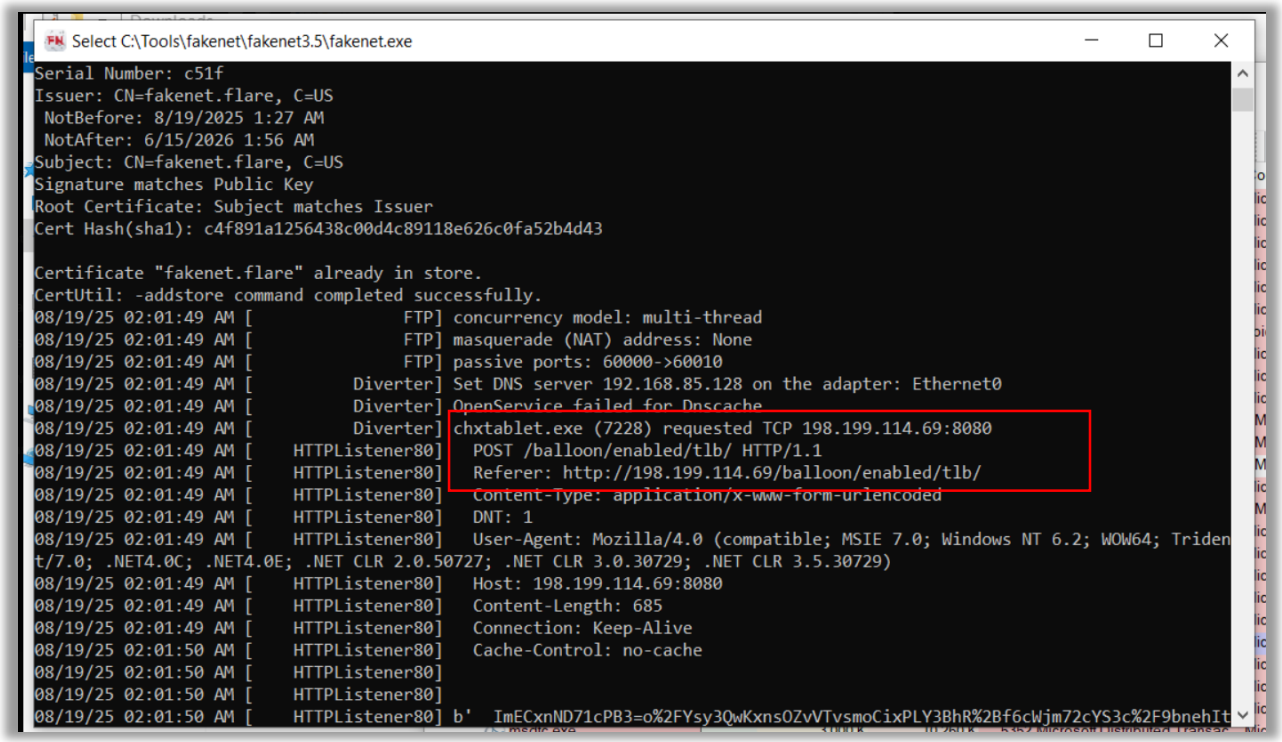
- **Hashes** (MD5, SHA256)
- **Strings** (notable URLs, commands, registry keys)
- **PE details** (imports, sections, entropy)
- **Possible behavior** (injection, persistence, exfiltration)
- **Indicators of Compromise (IOCs)**



Workflow Order

1. Start **Fakenet-NG** (simulate network).
2. Run **Process Explorer + Process Hacker** (monitor new processes & mutex).
3. Start **Procmon** (file + registry activity).
4. Execute malware sample.
5. Record:
    - New process names.
    - Mutex.
    - Copied/dropped files.
    - Registry modifications.
    - Persistence (autorun keys, services, tasks).
    - Network activity from Fakenet.
6. Save logs + document IOCs.

Starting Fakenet & Processhacker



C:\Tools\fakenet\fakenet3.5

File Home Share View

This PC > Local Disk (C:) > Tools > fakenet > fakenet3.5 >

Search fakenet3.5

Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Network

Name	Date modified	Type	Size
defaultFiles	4/8/2025 12:48 PM	File folder	
docs	4/8/2025 12:48 PM	File folder	
listeners	4/8/2025 12:48 PM	File folder	
CHANGELOG.txt	4/9/2025 8:38 AM	Text Document	5 KB
fakenet.exe	4/9/2025 8:42 AM	Application	7,992 KB
http_20250819_010738.txt	8/19/2025 1:07 AM	Text Document	2 KB
http_20250819_010742.txt	8/19/2025 1:07 AM	Text Document	2 KB
http_20250819_010747.txt	8/19/2025 1:07 AM	Text Document	2 KB
http_20250819_010755.txt	8/19/2025 1:07 AM	Text Document	2 KB
http_20250819_010759.txt	8/19/2025 1:07 AM	Text Document	2 KB
http_20250819_010806.txt	8/19/2025 1:08 AM	Text Document	2 KB
http_20250819_010810.txt	8/19/2025 1:08 AM	Text Document	2 KB
http_20250819_010816.txt	8/19/2025 1:08 AM	Text Document	2 KB
http_20250819_010821.txt	8/19/2025 1:08 AM	Text Document	2 KB
http_20250819_010830.txt	8/19/2025 1:08 AM	Text Document	2 KB
http_20250819_010836.txt	8/19/2025 1:08 AM	Text Document	2 KB
http_20250819_010840.txt	8/19/2025 1:08 AM	Text Document	2 KB
http_20250819_010846.txt	8/19/2025 1:08 AM	Text Document	2 KB
http_20250819_010856.txt	8/19/2025 1:08 AM	Text Document	2 KB
http_20250819_010905.txt	8/19/2025 1:09 AM	Text Document	2 KB
http_20250819_010909.txt	8/19/2025 1:09 AM	Text Document	2 KB

30 items

Process Hacker [DESKTOP-DQF89JN\Mr.Robot]+

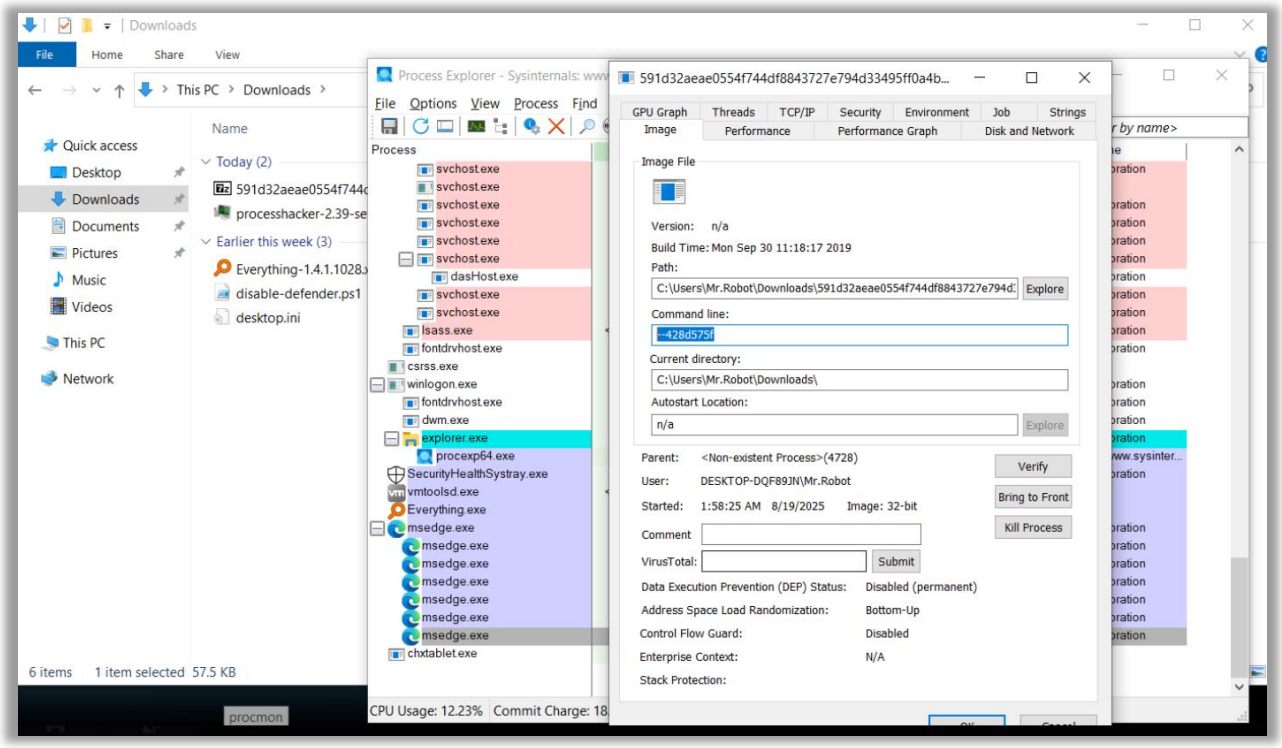
Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information Search Processes (Ctrl+K)

Processes Services Network Disk

Name	PID	CPU	I/O total r...	Private by...	User name	Description
System Idle Process	0	92.62		60 kB	NT AUTHORITY\SYSTEM	
System	4	0.42		196 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	308			1.14 MB	NT AUTHORITY\SYSTEM	Windows Session Manager
Interrupts		1.73		0		Interrupts and DPCs
Registry	104			7.45 MB	NT AUTHORITY\SYSTEM	
csrss.exe	428	0.01		1.71 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	508			1.34 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	588	0.01		5.18 MB	NT AUTHORITY\SYSTEM	Services and Controller app
svchost.exe	784			900 kB	NT AUTHORITY\SYSTEM	Host Process for Windows Serv...
svchost.exe	808		88 B/s	9.6 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Serv...
WmiPrvSE.exe	3032			8.55 MB	NT...\NETWORK SERVICE	WMI Provider Host
dllhost.exe	5224			3.19 MB	NT AUTHORITY\SYSTEM	COM Surrogate
RuntimeBroker.exe	5896			6.5 MB	DESKTOP-D...\Mr.Robot	Runtime Broker
RuntimeBroker.exe	3580			9.63 MB	DESKTOP-D...\Mr.Robot	Runtime Broker
WmiPrvSE.exe	4900			12.75 MB	NT AUTHORITY\SYSTEM	WMI Provider Host
SecurityHealthHos...	1332			2.36 MB	DESKTOP-D...\Mr.Robot	Windows Security Health Host
RuntimeBroker.exe	8136			2.77 MB	DESKTOP-D...\Mr.Robot	Runtime Broker
StartMenuExperien...	2220			25.24 MB	DESKTOP-D...\Mr.Robot	
SearchUI.exe	3960			73.63 MB	DESKTOP-D...\Mr.Robot	Search and Cortana application
ShellExperienceHo...	1872			14.48 MB	DESKTOP-D...\Mr.Robot	Windows Shell Experience Host
RuntimeBroker.exe	6032			3.17 MB	DESKTOP-D...\Mr.Robot	Runtime Broker
TiWorker.exe	9336			3.46 MB	NT AUTHORITY\SYSTEM	Windows Modules Installer Wo...
svchost.exe	924	0.05		6.67 MB	NT...\NETWORK SERVICE	Host Process for Windows Serv...
svchost.exe	972			2.29 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Serv...
svchost.exe	1040			2.07 MB	NT AU...\LOCAL SERVICE	Host Process for Windows Serv...

msedge.exe	8116	8.38 MB	DESKTOP-D...\Mr.Robot	Microsoft Edge
msedge.exe	9144	75.34 MB	DESKTOP-D...\Mr.Robot	Microsoft Edge
msedge.exe	8344	20.05 MB	DESKTOP-D...\Mr.Robot	Microsoft Edge
chxtablet.exe	1260	3.07 MB	NT AUTHORITY\SYSTEM	



Main Tactics used by Emotet:

1. **Execution**
   - T1204.002 – User Execution: Malicious File
     (Victim runs the .exe after being tricked).
   - T1059 – Command and Scripting Interpreter
     (Uses PowerShell or VBScript for execution).

2. **Persistence**
   - T1547.001 – Registry Run Keys / Startup Folder
     (Copies itself to Run/RunOnce keys).

3. **Privilege Escalation & Defense Evasion**
   - T1562.001 – Impair Defenses: Disable Security Tools
     (Disables AV/EDR or edits registry).
   - T1036 – Masquerading
     (Renames itself to look like a legit program, e.g., chorethemes.exe).

4. **Discovery**
   - T1082 – System Information Discovery
   - T1018 – Remote System Discovery

5. **Lateral Movement**
   - T1021.002 – SMB/Windows Admin Shares

6. **Command and Control (C2)**
   - T1071.001 – Application Layer Protocol: Web Protocols (HTTP/S)
     (Communicates with C2 via HTTP/S).
   -
7. **Impact / Secondary Payloads**
   - **T1105 – Ingress Tool Transfer**
     (Downloads extra malware like TrickBot or Ryuk).