



149 lines (109 loc) · 4.97 KB

Preview

Code

Blame



Raw



Ex.No.9: Use Process Explorer to Identify Suspicious Processes

Aim

To identify and analyze suspicious or potentially malicious processes running on a Windows system using **Process Explorer**, a tool from Microsoft Sysinternals Suite.

STEP 1 — Download and Set Up Process Explorer

Instructions

1. Download Process Explorer

- Visit the official Microsoft Sysinternals website:

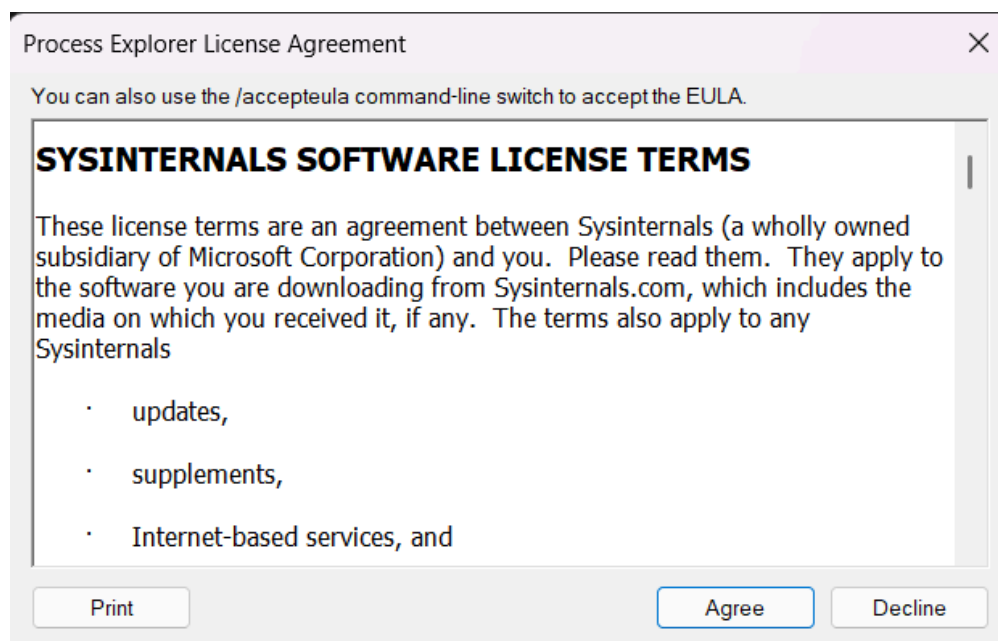
 [Download Process Explorer](#)

2. Extract the Program

- Extract the downloaded ZIP file to a preferred location on your computer.

3. Run Process Explorer

- Open the folder and launch the appropriate version:
 - `procexp64.exe` for 64-bit systems
 - `procexp.exe` for 32-bit systems
- Right-click and select **Run as Administrator** to ensure full privileges.



STEP 2 — Familiarize Yourself with the Interface

Key Components

- **Process Tree:** Displays hierarchical structure of running processes.
- **Color Codes:**
 - Pink → Suspended processes
 - Light Blue → Processes under the current user
 - Dark Blue → System or service processes
 - Green → Newly created processes
 - Red → Recently exited processes

Columns Overview

- **PID:** Process ID number
- **CPU Usage:** Real-time processor consumption
- **Memory Usage:** RAM utilization
- **Description & Company Name:** Metadata for legitimacy verification

STEP 3 — Identify Suspicious Processes

1 Look for Unfamiliar Processes

- Review all running processes and identify unknown or oddly named ones.

- Malware often disguises itself using similar names to legitimate processes.

2 Verify Digital Signatures

- Right-click a process → **Properties** → **Image Tab** → **Verify**.
- Check for a valid **Digital Signature**.
 - Valid Signature → Legitimate software
 - No/Invalid Signature → Potentially malicious

3 Check Process Path

- In the **Properties** → **Image Tab**, review the file path.
 - Legitimate processes reside in:

C:\Windows\System32



- Suspicious if running from:
 - Temporary folders
 - User download folders
 - Unknown directories

4 Monitor Resource Usage

- Observe CPU, Memory, and Disk columns.
- Abnormally high or fluctuating usage could signal malware.

5 Review Description & Company Name

- Missing or misleading information may indicate fake or rogue software.

6 Check Network Activity

- Right-click process → **Properties** → **TCP/IP Tab**.
- Monitor for unexpected network connections to unknown IPs.

Process Explorer - Sysinternals: www.sysinternals.com [BHUVAN\J B NAIDU]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System		176 K	65,528 K	284		
Registry		10,140 K	48,644 K	328		
System Idle Process	91.40	60 K	8 K	0		
System	0.61	52 K	4,204 K	4		
Interrupts	0.61	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,168 K	868 K	900		
Memory Compression	< 0.01	2,088 K	6,41,504 K	3440		
csrss.exe	< 0.01	2,936 K	4,080 K	1332		
wininit.exe		1,696 K	3,520 K	1440		
services.exe	0.15	7,324 K	10,980 K	1516		
svchost.exe	0.08	13,852 K	30,640 K	1768	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		7,332 K	14,352 K	4604		
unsecapp.exe		3,616 K	5,760 K	6724		
mic-neo-host.exe		24,796 K	14,104 K	12948		
unsecapp.exe		1,704 K	9,688 K	17816		
SearchHost.exe	< 0.01	69,196 K	1,10,184 K	18548		Microsoft Corporation
msedgewebview2.exe	< 0.01	39,472 K	98,996 K	18720	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		2,320 K	8,580 K	19240	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		67,324 K	57,604 K	21076	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		14,852 K	35,472 K	6768	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		9,428 K	18,532 K	19796	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe	< 0.01	59,732 K	60,568 K	4344	Microsoft Edge WebView2	Microsoft Corporation
StartMenuExperienceHo...	< 0.01	88,008 K	1,21,456 K	20504	Windows Start Experience H...	Microsoft Corporation
RuntimeBroker.exe	< 0.01	7,576 K	47,164 K	13984	Runtime Broker	Microsoft Corporation
Widgets.exe		14,044 K	71,204 K	20888		Microsoft Corporation
msedgewebview2.exe		42,220 K	5,496 K	1700	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		2,764 K	10,992 K	12228	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		1,21,280 K	2,156 K	20812	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		14,228 K	608 K	16048	Microsoft Edge WebView2	Microsoft Corporation
msedgewebview2.exe		10,072 K	112 K	5316	Microsoft Edge WebView2	Microsoft Corporation

CPU Usage: 8.45% | Commit Charge: 69.94% | Processes: 269 | Physical Usage: 56.18%

STEP 4 — Perform Online Verification

Actions

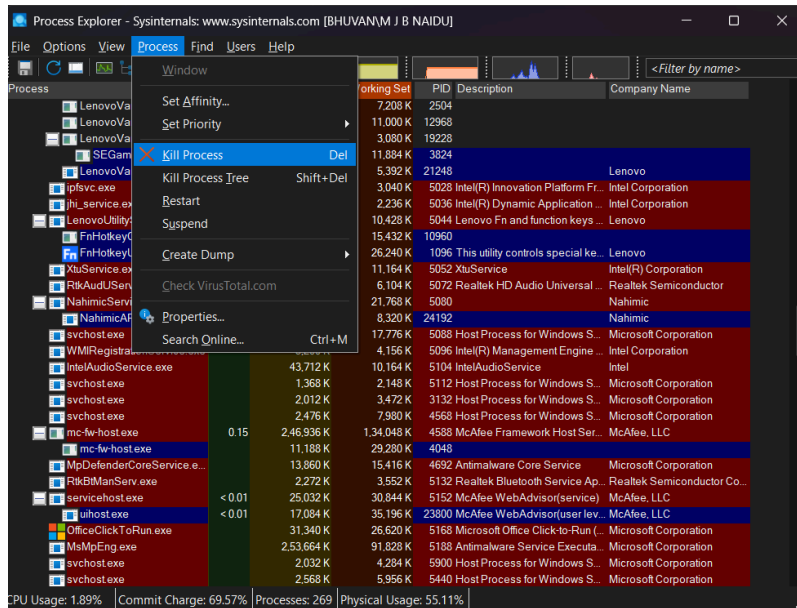
- Perform a quick Google search using the suspicious process name (e.g., `randomname.exe`).
- Cross-check the process in malware databases like:
 - [VirusTotal](#)
 - [ProcessLibrary](#)

STEP 5 — Take Action on Suspicious Processes

Options

- **Kill Process:**
Terminate the process immediately:
Right-click → Kill Process
- **Suspend Process:**
Temporarily pause activity for further analysis:
Right-click → Suspend
- **Delete Source File:**
Locate the file via **Path** and delete it if confirmed malicious.

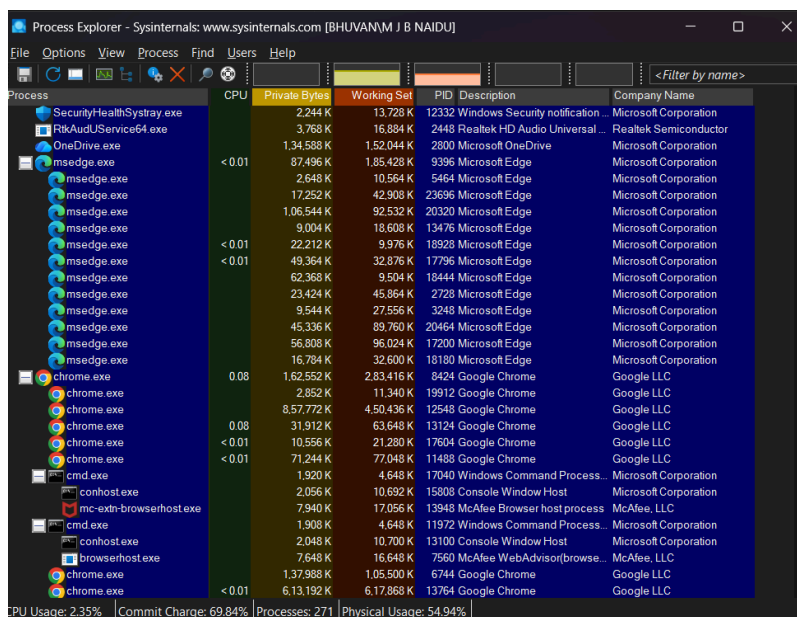
Note: Some malware prevents termination. In such cases, reboot into **Safe Mode** or use antivirus tools.



STEP 6 — System Cleanup and Scan

Recommendations

- Perform a full antivirus scan using tools like:
 - Windows Defender
 - Malwarebytes Anti-Malware
- Remove quarantined threats and restart the system.



Example — Identifying a Malicious Process

Action Taken

- Suspended → Killed the process
- Removed file from directory
- Performed full malware scan

Result: Confirmed as malicious software and successfully removed.

Rubrics

Criteria	Mark Allotted	Mark Awarded
1. GitHub Activity & Submission Regularity	3	
2. Application of Forensic Tools & Practical Execution	3	
3. Documentation & Reporting	2	
4. Engagement, Problem-Solving & Team Collaboration	2	
Total	10	

Result

Successfully utilized **Process Explorer** to monitor and analyze system processes, identify suspicious activities, and mitigate potential malware threats.