Bhuvaneshwar-Naidu Update Exp_9_Process_Explorer.md 9ddb462 · now

149 lines (109 loc) · 4.97 KB

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

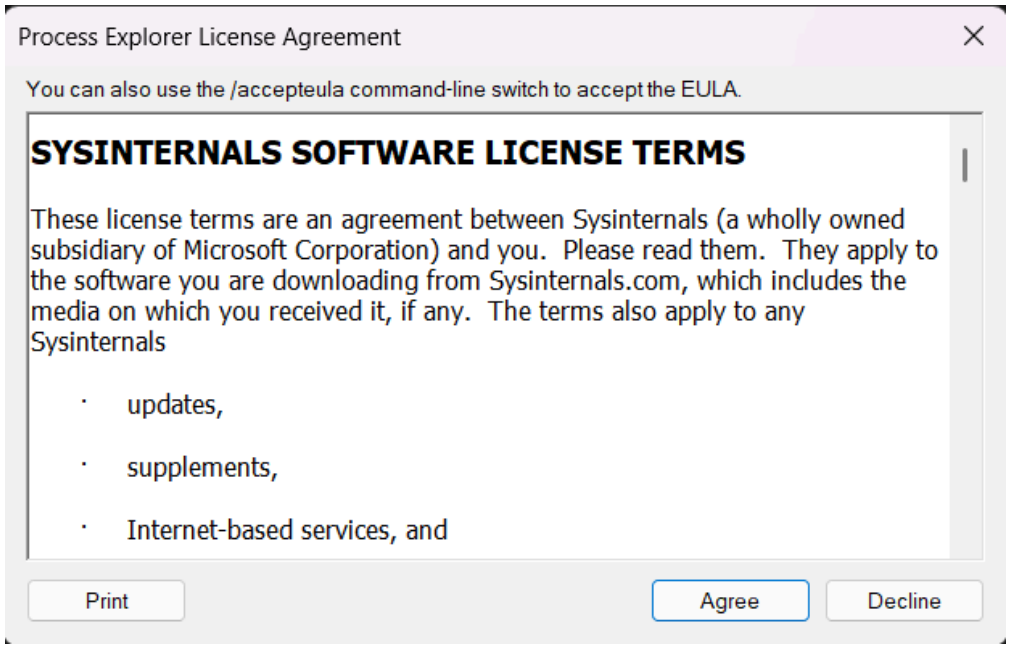
Aim

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

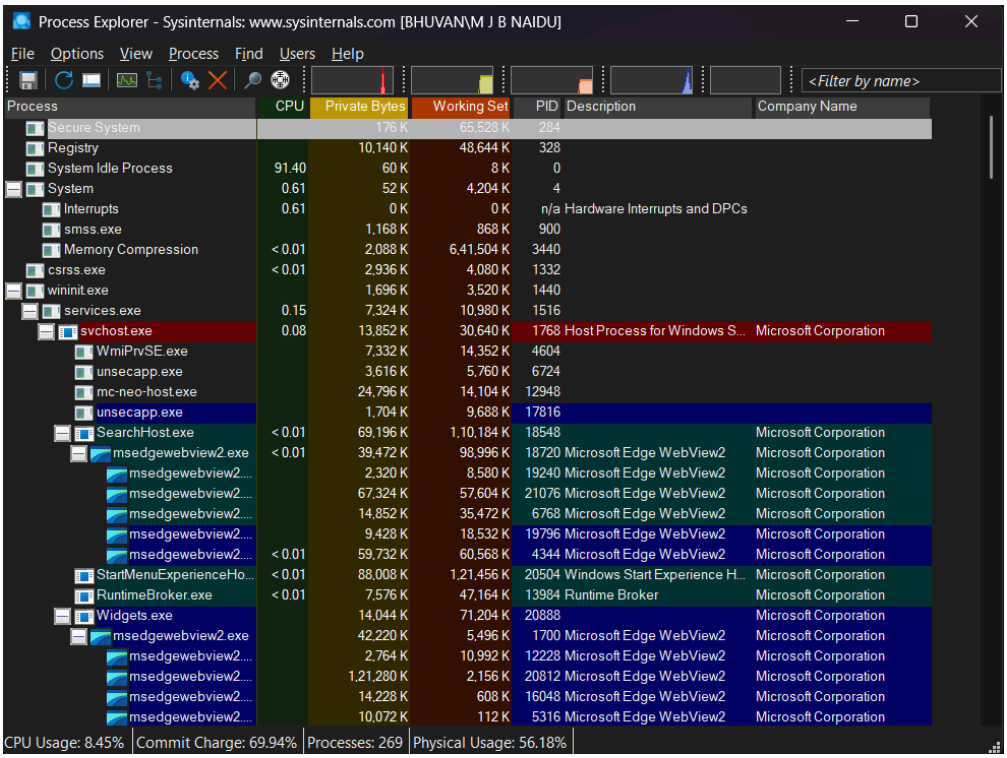
- Observe CPU, Memory, and Disk columns.
- Abnormally high or fluctuating usage could signal malware.

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.



STEP 4 — Perform Online Verification

Actions

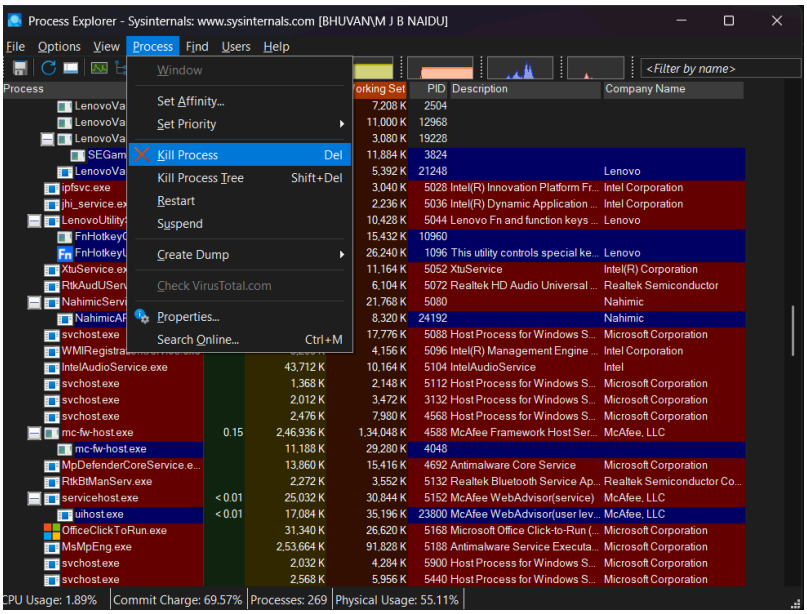
- Perform a quick Google search using the suspicious process name (e.g., `randomname.exe`).
- Cross-check the process in malware databases like:
  - VirusTotal
  - ProcessLibrary

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.

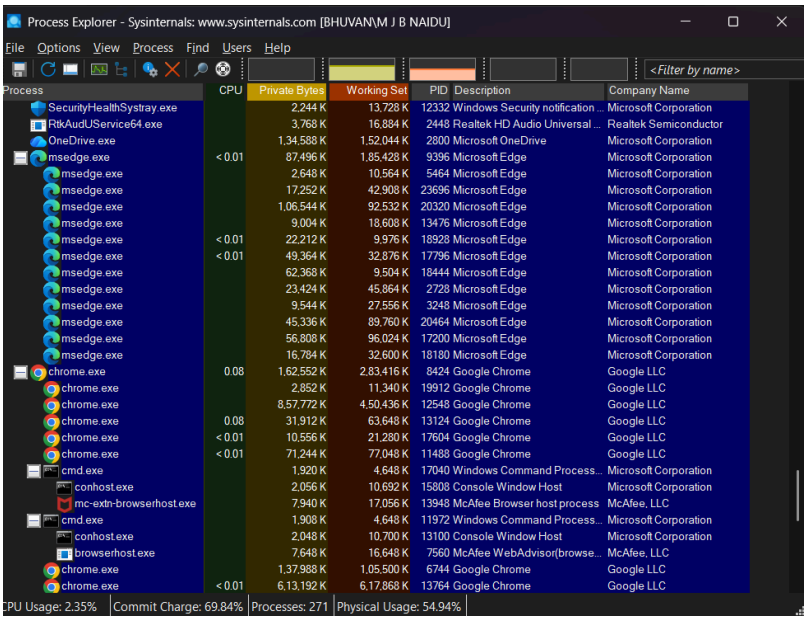
> *Note:* Some malware prevents termination. In such cases, reboot into **Safe Mode** or use antivirus tools.



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.
