KEYLOGGER INVESTIGATION ON WINDOWS:

Objective:

To investigate potential keylogger activity on a Windows machine.

Introduction:

Keylogging is a serious security threat where keystrokes are secretly recorded, capturing sensitive information such as passwords and financial details. This stolen data can be used for malicious purposes, including identity theft and fraud. Keyloggers can be hardware- or software-based, making detection challenging.

This report outlines a structured approach to identifying potential keyloggers on a Windows system.

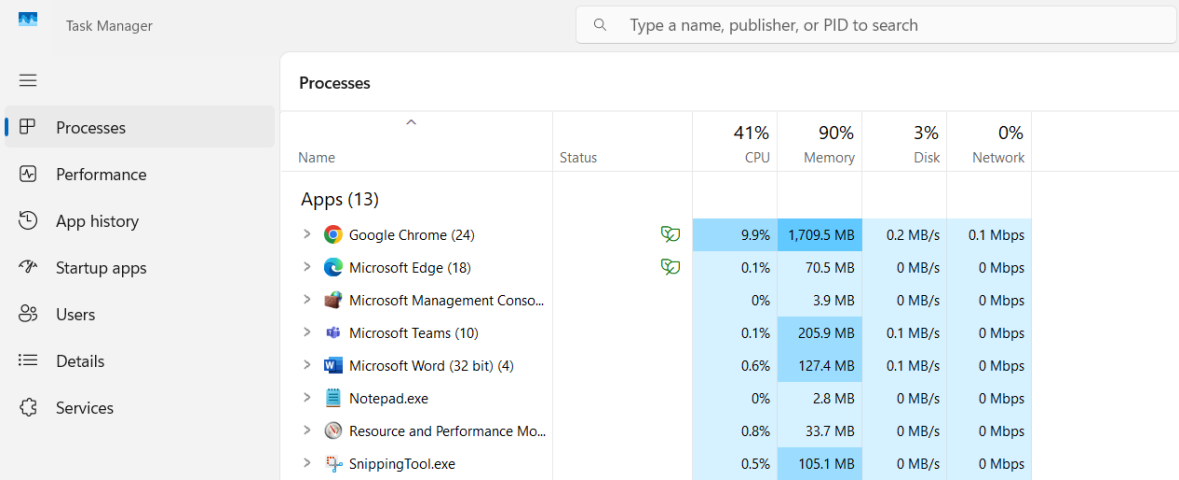
Methodology

Detecting a keylogger in Windows involves checking for suspicious processes, unusual network activity, and unauthorized software. Below are the steps taken to investigate keylogging activity:

1. **Check for Suspicious Processes in Task Manager**

Steps:

i. Open Task Manager (Ctrl + Shift + Esc).
ii. Navigate to the Processes tab and look for unfamiliar or suspicious processes.
iii. Right-click a suspicious process → Open File Location.
iv. If the file is stored in an unusual directory (e.g., %TEMP% or C:\Users\Public\), it may be a keylogger.



2. **Review Installed Programs**

Steps:

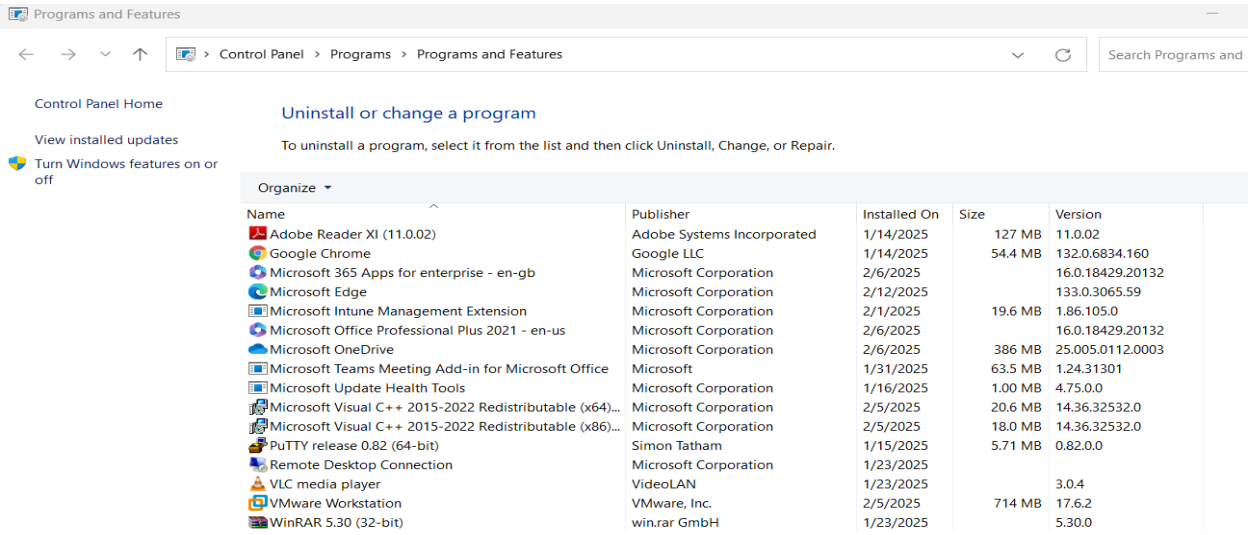
i. Press Win + R, type appwiz.cpl, and press Enter.

ii. Review installed programs for unknown or suspicious applications.

iii. If found, uninstall them and delete their associated folders from C:\Program Files.

Tip:

Many keyloggers disguise themselves with generic names, such as "System Optimizer" or "Windows Update Helper."



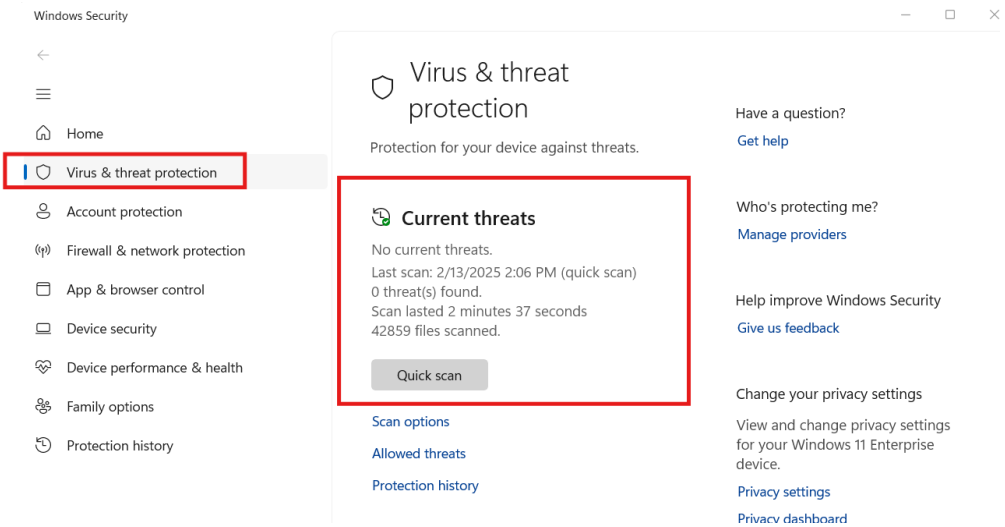
3. **Scan for Keyloggers with Windows Defender or Antivirus**

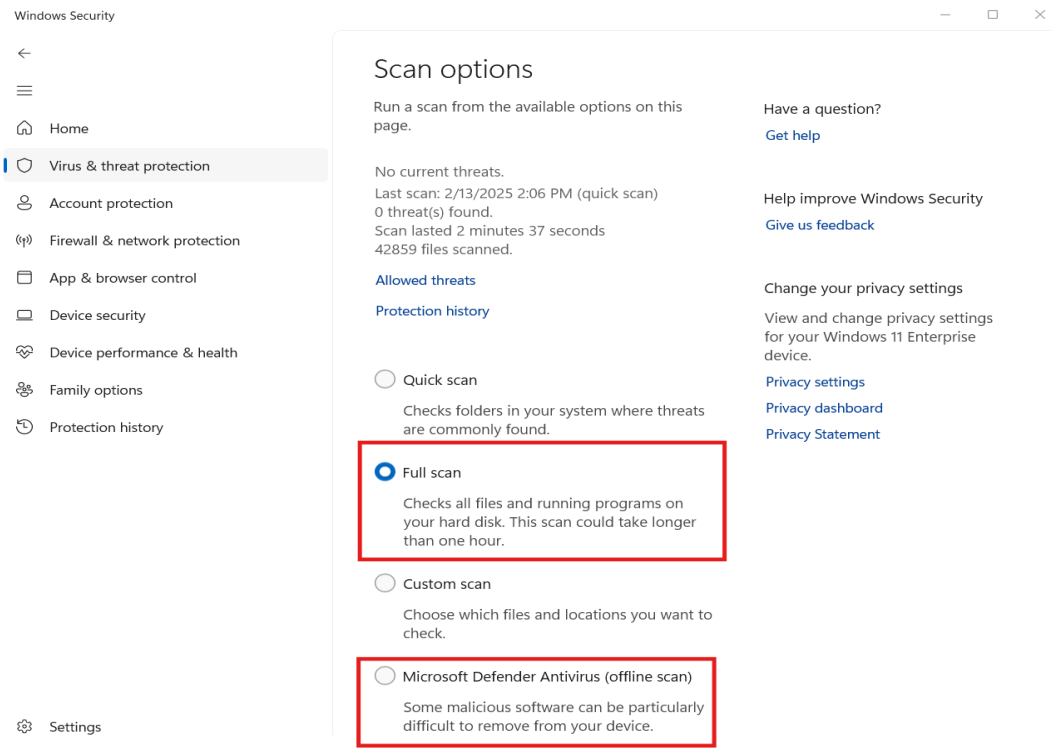
Steps:

i. Open Windows Security (Win + S, search for "Windows Security").

ii. Navigate to Virus & Threat Protection → Click Quick Scan.

iii. For a more thorough check, choose Full Scan or Microsoft Defender Offline Scan under Scan options.



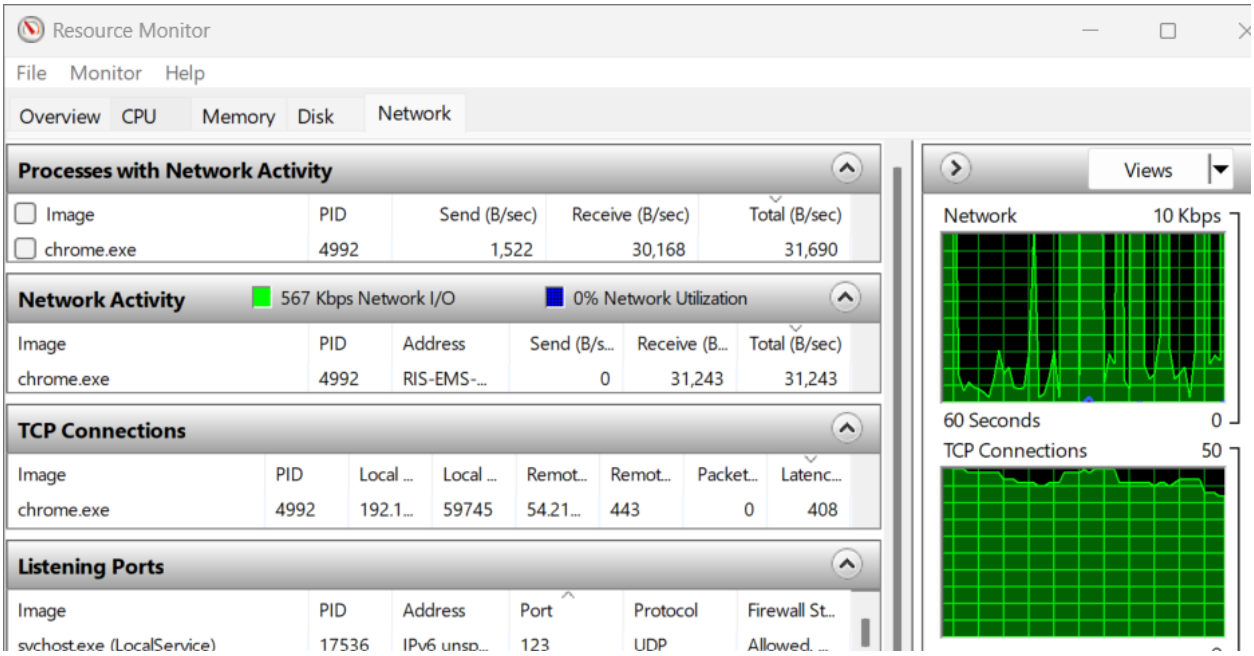


4. **Monitor Network Traffic for Suspicious Activity**

Steps:

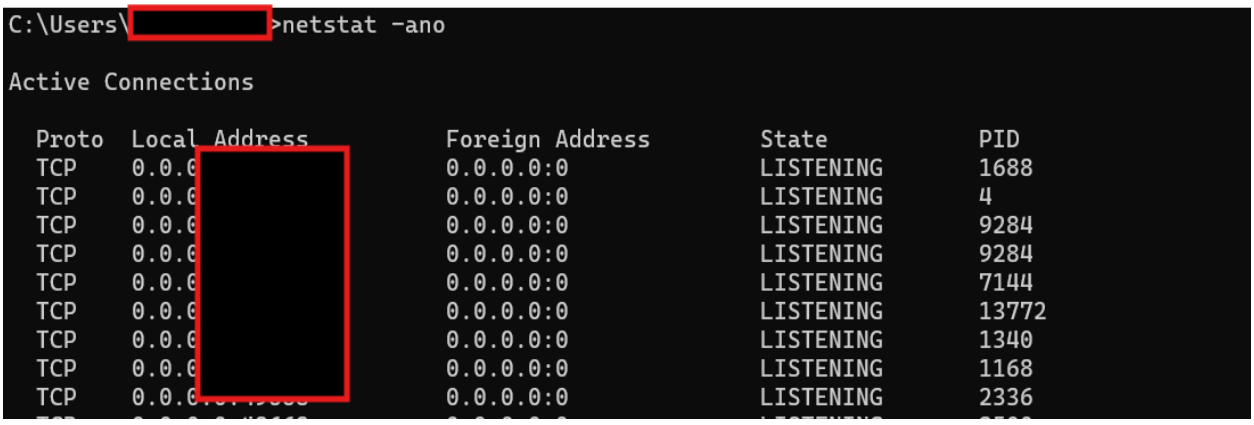
i. Open Task Manager, go to the Performance tab → Click Open Resource Monitor → Switch to the Network tab.

ii. Look for unknown programs actively transmitting data to external IP addresses



On Command Prompt, you can use netstat command to check active connections

- netstat -ano



From the listed active connections, check for unusual ports being used and the state of the ports.

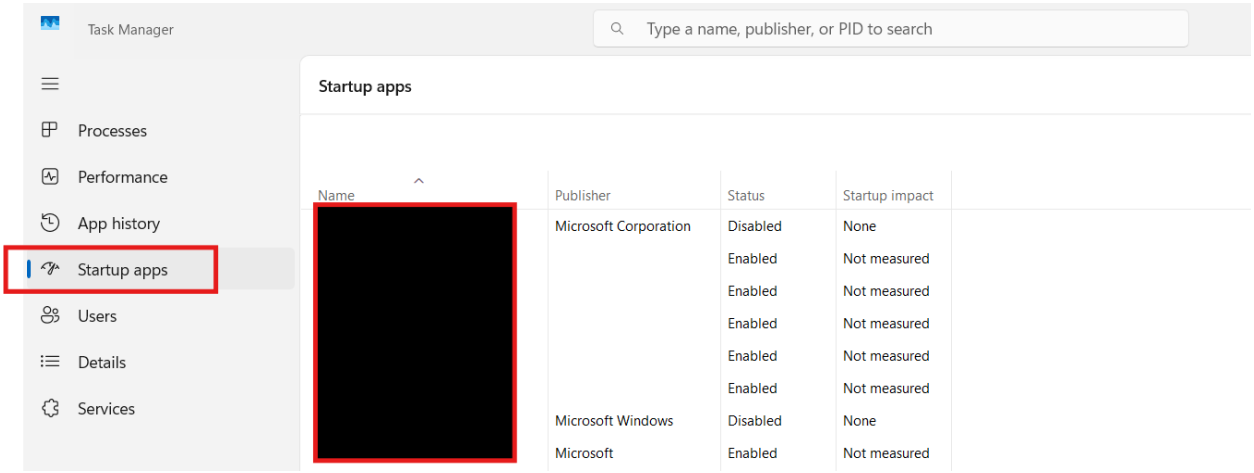
5. **Check Startup Programs**

Steps:

i. Open Task Manager, go to the Startup tab.

ii. Identify unfamiliar applications that launch at startup.

iii. Disable any suspicious programs from running automatically.



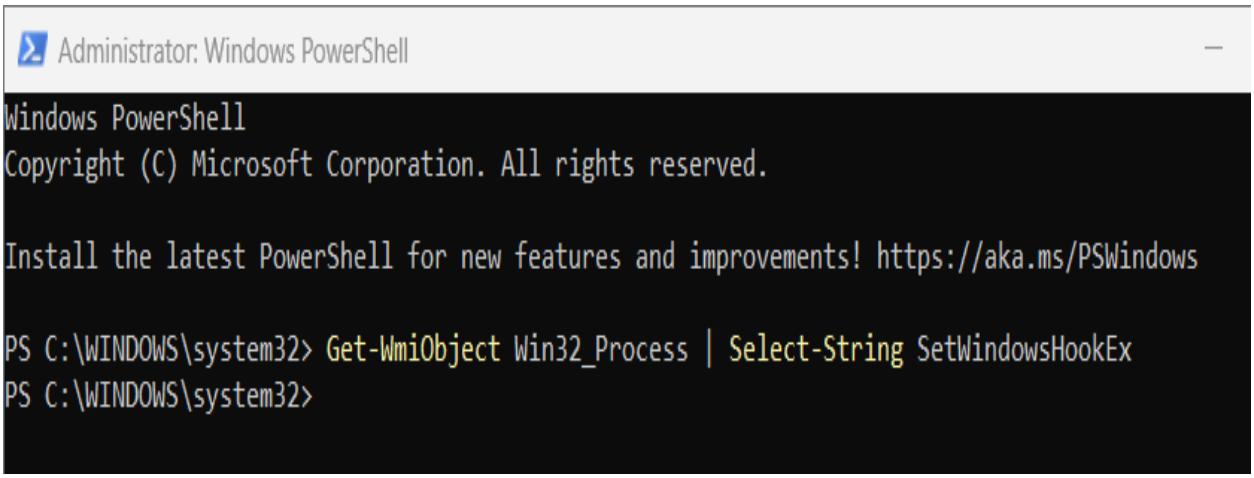
6. **Inspect Keyboard Hooking with PowerShell**

Steps:

i. Open PowerShell (Admin) (Win + X → Windows Terminal (Admin)).

ii. Run the following command to detect programs using keyboard hooks:

➢ *Get-WmiObject Win32_Process | Select-String "SetWindowsHookEx"*



The SetWindowsHookEx function is commonly used by keyloggers to capture keystrokes.

7. **Use Anti-Keylogger Software**

Consider using specialized anti-keylogger tools for additional protection:

a. Zemana AntiLogger – Detects keylogging attempts in realtime.
b. SpyShelter Anti-keylogger – Monitors keystroke activity.
c. Malwarebytes – Scans for keylogger signatures.

8. **Reset the System**

If you suspect an advanced keylogger that isn't detected, consider:

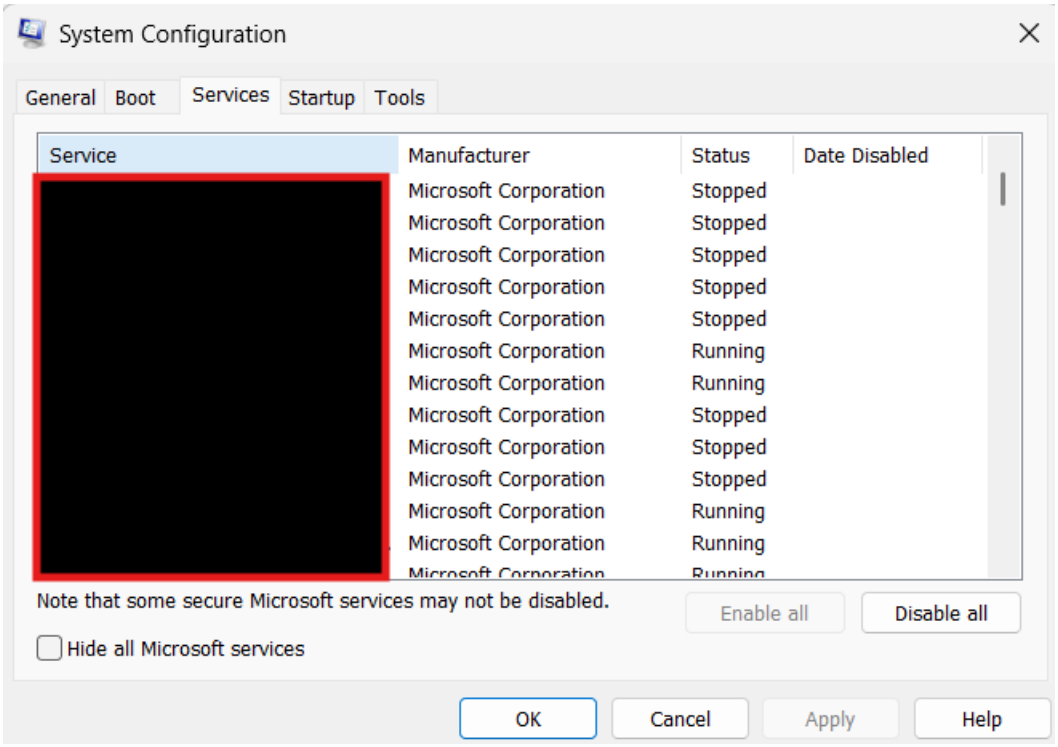
a. Resetting the PC

Go to Systems > Recovery > Reset this PC

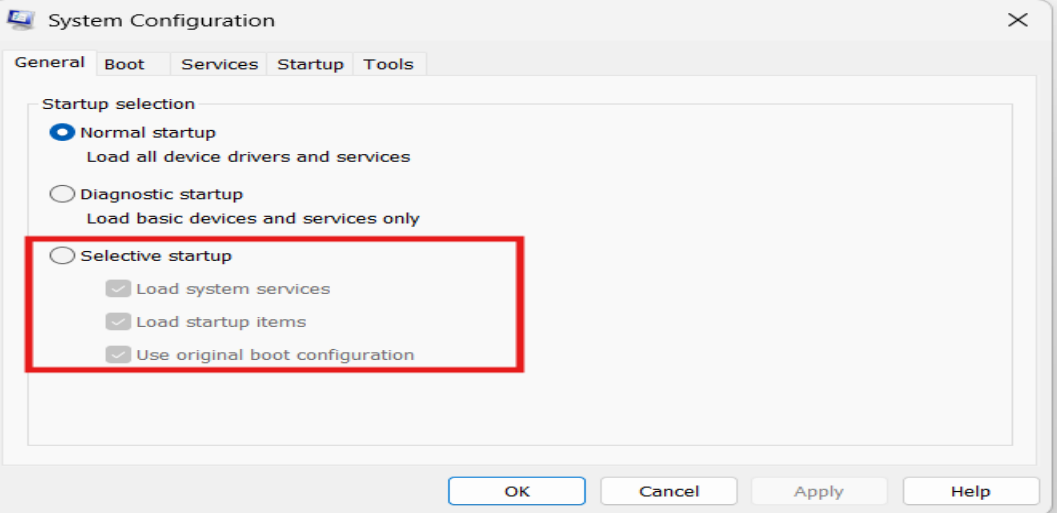
b. Perfoming a clean boot

Steps:

i. Press Win + R, type msconfig, and press Enter.
ii. Under the Services tab, check Hide all Microsoft services and disable unnecessary startup items.



iii. Under General tab, allow Selective startup



Tip:

Enable On-Screen Keyboard (Win + Ctrl + O) when entering sensitive data to prevent keylogging attacks.

Conclusion

Keyloggers are becoming more advanced, especially with the rise of AI-driven attacks, making them increasingly difficult to detect. However, by following the above steps, it is possible to identify and mitigate keylogger activity on a Windows 11 system. Regular security audits, software updates, and cautious online behavior are essential in preventing such threats.