COPS Guide - Virus/Malware Removal (Windows)

contributors: shaun@	*updated: 08-JUL-2024*

PRE

- [**IMPORTANT**] Air Gap Device
  > *Ensure device is disconnected from all networks before RKill is run successfully and RATs (Remote Access Tools) removed, to ensure malicious actors do not re-connect to the device while it's still compromised*
- Enable System Restore (set to 7% allocation if enough free disk space)
- [OPTIONAL] Create a new System Restore point "**COPS - Pre Virus/Malware Removal**"
  > *This System Restore point will be wiped out in a later step (post-virus/malware removal), as malware can persist in old System Restore points*
- Restart Windows
  > *Force Restart Windows (`shutdown -r -f -t 00`) now to provide a clean slate for proceeding*
- Create COPS Folder
- Add COPS Folder to installed antivirus exclusions list(s)
- Copy Rkill folder from USB Tool to "%SYSTEMDRIVE%\COPS" (RKill can't run from a write-blocked drive)
- Run an Rkill executable as Administrator
- Move Rkill.txt from "%USERPROFILE%\Desktop" to "%SYSTEMDRIVE%\COPS"
- Revo Uninstaller
  - xxx
- Disk Cleanup
  - Run `Win+R : cleanmgr /sageset:10`
    > *This will open the Disk Cleanup utility to create settings for Profile 10*
  - Click `Clean up system files`
  - Select all checkboxes except for the two **System error** options
    > *`System error memory dump files + System error minidump files >`*
    > *(you can click on an option, and then use the UP + DOWN Arrows + Space Bar to quickly check or uncheck options)*
  - Click `OK`
  - Run `Win+R : cleanmgr /sagerun:10`
    > *This will run the Disk Cleanup utility to using Profile 10's settings`*

MAIN

- Connect to Internet
- [OPTIONAL] AdwCleaner
  > *AdwCleaner crashes out of UVK's automation, so run it now instead if you want to use it*
- [OPTIONAL] Spybot - Search & Destroy
  > *Spybot is a thorough malware removal tool, but it can take a very long time to complete it's scans*
- [OPTIONAL] Windows Defender Offline Scan
- [OPTIONAL] Create a new System Restore point "**COPS - Pre Virus/Malware Removal**"
- Ultra Virus Killer (UVK)
  - Install UVK
  - Open UVK
    - Do not disable Hybrid Shutdown if asked when opening UVK
    - Do Update UVK if asked when opening UVK
  - Click System Repair

- Select the following repair actions: *(left menu)*

  (you can click on an option, and then use the UP + DOWN Arrows + Space Bar to quickly check or uncheck options)

  - Pre-Repair Actions
    1. Set technician power settings
    2. Kill all non system processes
    3. Delete all restore points
    4. Create a system restore point
    5. Free physical memory
    6. Backup the registry
    7. Un-immunize all areas
    8. Disable the User Account Control
    9. Enable the legacy (F8) boot menu
    10. Enable Windows Recovery Environment
    11. Prevent rebooting until all is done - Third-Party Built-in Apps
    12. Ultra Adware Killer scan
    13. MalwareBytes AntiMalware scan
    14. Super AntiSpyware scan
    15. RogueKiller scan
    16. Kaspersky TDSSKiller scan
    17. Avast! Browser Cleanup - Reset Actions
    18. Reset the DNS cache
    19. Reset the Windows Store
    20. Reset all print jobs
  - Fixes for Common Windows Problems

    n/a
  - File System Related Actions
    21. Rebuild icon cache
  - Essential Installes/Updates

    [If Google Chrome is installed:]

    22. Insall/Update Chrome
    23. Install uBlock Origin for Chrome

    [If Mozilla Firefox is installed:]

    24. Install/Update Firefox
    25. Install uBlock Origin for Firefox
    26. Install uBlock Origin for Edge
    27. PatchMyPC - Update all apps - Privacy Cleanup
    28. Clear all browsers history (all users)
    29. Delete browsers cookies (all users)
  - Maintenance Actions
    30. Empty all users temp folders
    31. Empty browsers cache (all users)
    32. Unattended disk cleanup
  - System Repair and Optimization

    n/a
  - Windows Troubleshooters

    n/a
  - Post-Repair Actions
    33. Restore the previous UAC state
    34. Restore previous immunization
    35. Delete all restore points (post repair)
    36. Create restore point (post repair)
    37. Reset power settings
    38. Uninstall Malwarebytes Antimalware
    39. Uninstall Super AntiSpyware
    40. Uinstall RogueKiller
    41. Uninstall this application
    42. Restore normal boot

    - Select the following loadout settings: *(right menu)*
        1. Third party full scans
        2. Use unattended mode

    - Click `Run selected fixes/apps`

POST

- [OPTIONAL] Create a new System Restore point "**COPS - Pre Windows Update**"
- Update Windows (no preview updates)
- Update Apps via Microsoft Store
- Update Apps via Windows Package Manager (winget)

  > *You can queue up multiple commands using PowerShell by pressing `Shift+Enter` to add a new line before pressing `Enter` to executre the commands*

    - winget source update
    - winget upgrade --all --silent
- [OPTIONAL] Create a new System Restore point "**COPS - Pre Driver Update**"
- Update Drivers (SDIO)
- Verify Drivers (verifier)
    - **Turn On Windows Verifier:**
        - Run `Win+R : verifier`
        - Select `Create standard settings`
        - Click `Next`
        - Select `Automatically select all drivers on this computer`
        - Click `Finish`
        - Restart Windows (`shutdown -r -f -t 00`)

          > *Windows Verifier works by stressing out drivers as they're loaded (it is expected that the computer's performance will be impacted while verifier is enabled)*
          > *If Windows loads into the desktop OK and does not crash with verifier enabled, then all is good and you can proceed to turn it off*

    - **Turn Off Windows Verifier:**
        - Run `Win+R : verifier`
        - Select `Delete existing settings`
        - Click `Finish`
        - Restart Windows (`shutdown -r -f -t 00`)
- System Maintenance/Repair

  > *You can queue up multiple commands using PowerShell by pressing `Shift+Enter` to add a new line before pressing `Enter` to executre the commands*

    - sfc /scannow
    - dism /online /cleanup-image /startcomponenetcleanup /resetbase
    - dism /online /cleanup-image /restorehealth
    - sfc /scannow
    - chkdsk /r /scan /perf
- Create a new System Restore point "**COPS - Post Virus/Malware Removal**"