COPS Guide - Virus/Malware Removal (Windows)

contributors: shaun@	*updated: 25-JUN-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
  - xxx

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)
  - 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
  - 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**"