HOW TO REMOVE NASTY JUNKWARE & UNWANTED TOOLBARS FROM YOUR PC

Jim McKnight www.jimopi.net RemoveMW.lwp revised 1-29-2014

****** ALWAYS USE THE LATEST REVISION OF THIS CHECKLIST ******

These Step-by-Step procedures should remove most of the junkware from a PC, including many browser hijackers and unwanted Toolbars. Most of the typical Junkware programs, Adware type toolbars, and many PUPs (Potentially Unwanted Programs) are not detected by Anti-malware scans. Someway, somehow, the user gave permissions for the crap to be installed.

Before you start, I suggest you read through this entire sheet to see what you are in for. I did my best to present the material in a logical sequence, but every junkware removal is different. For an introductory video from britec09, see this youtube.com video: http://www.youtube.com/watch?v=dvnGAjWNSuk

It is a good idea to first go through my "HOW TO REMOVE MALWARE" checklist first to make sure any infections are cleaned up. Malware removal tools have a risk of crashing the system and making it unbootable, so this process is best done by an experienced technician.

If you cannot complete a specific step, continue on with the following steps. **BE SURE TO COMPLETE EVERY STEP SHOWN IN BOLD** to help make sure the junkware is really gone.

LIST OF COMMON ADWARE / JUNKWARE / PUPs

PUPs are Possibly Unwanted Programs. Here is some of the crapware that I have removed from PC's that cause multiple Toolbars, pop-ups, and ads that can drive you crazy. It also can track your movements on the internet and steal your identity:

- ★ Aartemis
- ★ Ask Toolbar
- ★ Babylon
- ★ BFlix Toolbar (BFlix gadget/BFlix Updater)
- ★ Browser Manager
- ★ Claro / iSearch
- ★ Conduit (Any Conduit products)
- ★ Coupon Printer for Windows
- ★ CoupScanner
- ★ Crossrider
- ★ DealPly
- ★ DMuninstaller
- ★ Facemoods / Funmoods
- ★ FLVM Player/ FLV Media Player *(install VLC Player instead)*
- ★ Free Download Manager
- ★ Highlightly
- ★ IB Updater (Incredibar)
- ★ iLivid
- ★ Iminent
- ★ IncrediBar (IB Updater)
- ★ Jollywallet
- ★ Maps Galaxy
- ★ Mobogenie
- ★ MyPCBackup
- ★ MyWebSearch
- ★ Online Vault
- ★ Power Speed
- ★ Plus-HD
- ★ PricePeep
- ★ Radio Rage Toolbar
- ★ ReMarKit
- ★ ScorpionSaver
- ★ Searchqu
- ★ Search Protect
- ★ Search Results Toolbar
- ★ Severe Weather Alerts
- ★ Shopathome Toolbar (Shop At Home Helper)
- ★ ShoppingChip
- ★ Snap.Do
- ★ Storimbo
- ★ Sweetpaks,
- ★ Torch
- ★ VideoPlayer *(Install VLC Player instead)*
- ★ VisualBee
- ★ Wajam
- ★ WeatherBlink
- ★ Web Assistant
- ★ WiseConvert Toolbar (Conduit)
- ★ WPM

IMAGE BACKUP FIRST:

- Before starting this process, I strongly suggest you first make a full image backup of the entire main hard-drive (all partitions) using a standalone bootable **Rescue CD** of Acronis True Image or some other good image backup program. Then, if anything goes wrong during malware removal, you can put everything back the way it was before you started, and then start over from scratch. Some junkware removal activities can make a PC unbootable. This way you have a path to recovery.
- **AFTER THE IMAGE BACKUP, BE SURE TO REMOVE THE EXTERNAL HARD-DRIVE AND/OR ANY NETWORK CABLES BEFORE BOOTING THE PC.**

START:

a. **REMOVE SCHEDULED TASKS**: Remove any Tasks that you do not understand. *(XP: Control Panel > Scheduled Tasks.).* Figuring out unwanted tasks in Windows 7 is a major challenge, but is much easier if you use the Tool in CCleaner. Here is the manual path: *(Win7: Control Panel > Administrative Tools > Task Scheduler)*. Be careful. *(CCleaner = Tools > Startup > Scheduled Tasks tab).*

b. **ATTEMPT TO REMOVE ALL THE LISTED JUNKWARE POSSIBLE using REVO UNINSTALLER or ADD/REMOVE PROGRAMS (For Windows 7 see PROGRAMS and FEATURES).** Some will remove cleanly and some will not. Most will leave remnants scattered around the system. Also, in the Start > All programs Menu there is sometimes a shortcut to remove the desired program.

c. **RUN ADWCLEANER:** Make sure PC reboots OK afterwards. If not, restore from image and start over**.** Once ADW Cleaner has cleaned everything, it is a good idea to run it again until it runs clean.

d. **RUN JRT:** The Junkware Removal Tool has the ability to remove much of the junkware. Make sure PC reboots OK afterwards. If not, restore from image and start over. *(NOTE: May not work on 64-bit systems).*

e. **RUN CCLEANER:**
   1) **Run the Temp file Clean.**
   2) **Run the Registry Clean until it runs clear with nothing found.**

f. **TURN OFF SYSTEM RESTORE:** Now is the time to TURN OFF *SYSTEM RESTORE (this deletes all the System Restore history files)*. Continue with the next steps

g. **RUN SPYBOT S&D (Use only Version 1.6.2 from filehippo.com. NOT version 2.x)**

h. **RUN SAS (Super Anti Spyware):**

i. **RUN MBAM (MalwareBytes Anti Malware):**

j. **RUN MBAR (MalwareBytes Anti Rootkit):** .

k. **RUN OTL (by Oldtimer) If Necessary: If you have any difficult to remove Files or Registry Keys, run an OTL scan.** http://www.geekstogo.com/1888/otl-by-oldtimer-a-modern-replacement-for-hijackthis/

l. **CLEAN THE "HOSTS" FILE**: For XP and Win7:
   1) Click START, RUN, and type in: C:\windows\system32\drivers\etc\hosts , then click <OK>
   2) When prompted, choose to open the HOSTS file with either Notepad or Wordpad.
   3) Delete all the lines of IP addresses in this text file except for the "127.0.0.1 localhost" and the " ::1 " entries. *(Also, you can leave all lines that begin with # as they are just comments)*.
   4) Save the file. Also see this site for an optional Hosts file: http://www.mvps.org/winhelp2002/hosts.htm

m. **TEMP FILE CLEANING:** ***WARNING: New Malwares are hiding good user files in temp folders. Deleting temp files before you get the sysem back to normal can ruin any chance of a successful recovery. Better have a full image backup of the PC before continuing.***

1) Run **TFC TEMP FILE CLEANER** (by oldtimer). If this utility will load and run, you can use it now to cleanup all the temp folders for all users. *It will do an auto-reboot at the end to finish*. If it will still not run, skip this step and continue to the next step

2) Run **CCLEANER AGAIN** for each user.

n. **CLEAN THE "DOWNLOADS" FOLDER for every User.** *(Many junkware installer files can be there)***.** _

o. **SCHEDULED TASKS**: Check <u>again</u> for any that do not belong: *(XP: Control Panel > Scheduled Tasks)*.

p. **FIREFOX (Options = Set "No" PROXY)**: *(Firefox: Tools > Options > Advanced tab > Network tab > Connection settings)*. Check the button for "No Proxy" or "Use system proxy settings")

q. **INTERNET OPTIONS:** Clear and Reset IE. *(Do these steps for each user):*

1) TRUSTED SITES: *(XP & Win7: Control Panel > Internet Options > Security tab > Trusted Sites > Sites)*. Delete all Trusted Sites.

2) RESET IE: *(XP & Win7: Control Panel > Internet Options > Advanced tab. Click "Restore advanced settings", then "Apply", then click "Reset.." (WARNING: The Home page/s may be lost)*

3) "No" PROXY: Check that the Connections are NOT using a Proxy: *(XP & Win7: Control Panel > Internet Options > Connections tab > LAN settings).* The Proxy Server box should NOT be checked, but "Automatically Detect settings" should be checked.

r. **NETWORK CONNECTIONS:** *(XP: Control Panel > Network Connections, then right-click the desired adapter > Properties > then TCPIP > Properties). (Win7: Control Panel > Network & sharing center > Change adapter settings, then right-click the desired adapter > Properties > then TCPIP/IPv4 > Properties).* Make sure all Network Adapters are set to "Obtain an IP Address Automatically" and "Obtain a DNS server address Automatically.

s. **CONNECT THE SYSTEM TO THE INTERNET and TEST INTERNET EXPLORER**. If it does not work correctly, first restore the Advanced Settings again: *(XP & Win7: Control Panel > Internet Options > Advanced tab > click "Restore Advanced Settings").* If IE still does not work, run the "Fix IE" Utility program, then try COMBOFIX, WINSOCK XP FIX, or "COMPLETE INTERNET REPAIR" or the FARBAR SERVICE SCANNER.

t. **COMPLETE THE FOLLOWING TASKS:**

1) **ESET ON-LINE SCAN**: Do a free on-line scan from ESET.COM, Kaspersky *(available soon)*, Trend, or Panda*)*. *NOTE: These scans can run a <u>long, long</u> time.*

2) **MSRT**: Verify the latest version is installed and run a FULL SCAN. *(Start > Run > MRT) Note: You can verify the Tool's version Month and year on the program's title bar.*

3) **MSE:** If MSE is installed on the system, update and run a full scan.

4) **If things seem OK, continue to CLEAN-UP**.

CLEAN-UP:

a. **WINDOWS UPDATES:** Make sure ALL the Windows Updates are installed, including those for all Microsoft Products. To fix Windows Update problems: For XP try **DIAL-A-FIX**, or see Microsoft KB 971058. For Windows 7 try this fix-it button: http://support.microsoft.com/kb/971058 or try the FixWU.exe download or the Windows_Repair_All_In_One program *(XP/Vista/Win7)*.

b. **FIX WINDOWS FUNCTIONALITY PROBLEMS:** If you have strange problems after the malware removal is done: Try **D7** *(XP or Win7),* **or SuperAntiSpyware (repair tools),** or Windows-Repair-All-In-One *(from www.tweaking.com. XP or Win7)*, or "COMPLETE INTERNET

REPAIR*" (rizonesoft.com).* Try running the FARBAR Service Scanner to repair corrupted or missing Windows Services.

c. **FIXDAMAGE: (From the MBAR Toolkit):** The Malwarebytes Rootkit removal tool folder has another tool called FIXDAMAGE *(MBAR folder > Plugins > fixdamage.exe)*

d. **TURN "SYSTEM RESTORE" BACK ON for Drive C:**. At this point, turn System Restore/System Protection back on. If it is already on, be sure clear all the history. For XP, you must turn it off and then turn it back on. *Windows 7 allows you to clear the history: (Win7: Control Panel > System > System protection > select drive C > "Configure" > "Delete".)*

e. **BROWSER SECURITY:**

1) Make sure the "**WOT**" (Web Of Trust) Add-On is installed on all Browsers and for all User Accounts. Make sure it is functioning to help the user browse more safely.

2) Install **SANDBOXIE** for all User Accounts and show the User how to browse with it.

f. **SECUNIA PSI**: Once all is back to normal, check your system for program vulnerabilities by downloading, installing, and running the "Secunia PSI" program *(For a link, see my "UTILITY PROGRAMS" sheet at www.jimopi.net).*

g. **ADVISE THE OWNER TO CHANGE ANY PASSWORDS USED FOR ONLINE BANKING OR FINANCIALS OF ANY KIND.**

h. **PC TUNEUP: At this point I normally continue to my "XP TUNEUP CHECKLIST" or my "WINDOWS 7 TUNEUP CHECKLIST"**.

NOTES & MORE TOOLS:

- *For links to the various recommended junkware removal tools, see my sheet called "ANTI-MALWARE TOOLS & TIPS" at www.jimopi.net. Also, information on the latest popular "Fake AntiMalware" & "Fake System Tools", and techniques for their removal can be found at: http://www.bleepingcomputer.com/ and at http://siri-urz.blogspot.com/ For lots of good videos, see http://www.youtube.com/britec09*

- GEEKS TO GO TUTORIAL
  - ✓ Http://www.geekstogo.com/forum/topic/2852-malware-and-spyware-cleaning-guide/

- BLEEPING COMPUTER TOOLS:
  - ✓ How to use Inherit.exe and MiniToolBox: http://www.bleepingcomputer.com/forums/