HOW TO REMOVE MALWARE FROM YOUR PC ©

Jim McKnight www.jimopi.net RemoveMW.lwp revised 6-8-2020

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

These Step-by-Step procedures should remove malware from an infected PC, but are not for the faint of heart. These tools have a risk of crashing the system and making it unbootable, especially with the COMBOFIX and ROOTKIT TOOLS, so this process is best done by an experienced technician.

Understand that the only way to be 100% assured that a system is fully cleaned is to do the "**NUKE & PAVE**" process discussed at the end of this sheet. Any malware removal process other than a format and clean re-install always leaves the risk that something is still hidden for later attack.

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 malware removal is different.

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 malware is really gone.

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 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 malware 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 INFECTED PC.**

BACK UP FIREFOX BOOKMARKS AND IE FAVORITES.

- If possible, backup browser bookmarks and favorites before starting any removals.

START:

a. BOOT FAILS: Try these tips:

1) Go to the safe-mode boot screen *(F8, F8, F8),* & select boot to "Last Known Good Configuration".

2) If you still cannot boot the system, boot a UBCD4WIN CD and try restoring the System to an earlier time with the EZPCFIX Utility. If you do not have this CD, continue on.

3) Boot a Windows Repair CD or a Windows Install CD so you can run chkdsk /r. *(Note:The file sytem may be corrupted from the user messing with things trying to remove the malware). See my "TROUBLESHOOTING XP" or "TROUBLESHOOTING WINDOWS "sheet for other "fail to boot" suggestions.*

4) If you still cannot boot the system, or the system boots OK but is non-responsive, burn *(on another PC)* a HITMANPRO "KICKSTART" Bootable Flash Drive, or a KASPERSKY RESCUE DISK or AVG RESCUE DISK. Boot the CD/FLASH drive and run scans against the system's hard-drive. *If you need to know if the system is 32-bit or 64-bit, boot from a standalone CD of any sort and look at the drive C:\ . If there is a "C:\Program files (x86 folder)" then it is a 64-bit System).* Boot the Flash drive or CD and scan the system's hard-drive.

5) If you are short on Support Tools, you can install the hard-drive as a slave drive in a good PC and run anti-malware scans on it from there. ***WARNING: This is risky & can spread the infection!***

b. IF THE PC IS LOCKED BY FBI, DOJ, POLICE, OR ANY OTHER RANSOMWARE:

1) Try booting into Safe-Mode. If Safe-Mode works, continue with MBAM and other malware scans.

2) If Safe-Mode is also locked:
   a) Try burning (on another PC) a HITMANPRO "KICKSTART" Bootable Flash Drive or other bootable Malware Rescue Disk. Boot from the CD/FLASH and run scans against the system's hard-drive.
   b) Try booting to a KASPERSKY RESCUE DISK, click the K (graphic) button in the bottom right corner of the screen, select TERMINAL (on the Start menu of Kaspersky) and type

WINDOWSUNLOCKER, Then reboot and run your virus scans as you normally would. For details: http://support.kaspersky.com/8005?el=88446

c) Startup Password Removal:
Http://triplescomputers.com/blog/casestudies/solution-this-is-microsoft-support-telephone-scam-computer-ransom-lockout/

c. PC BOOTS OK, BUT DOES NOT RESPOND OR WILL NOT RUN ANY PROGRAMS:

1) Try running in Safe-Mode. If Safe-Mode works, go to step "g. POWER SETTINGS" & continue on.

2) If your programs will not run in Safe-Mode, try steps "a. 4)" and "a. 5)" above.

3) If many programs/scans pause, stop, freeze, or hang, run D or Windows Repair Toolbox or other Windows Repair Utilities)

d. IF THE PC SHUTS DOWN AND/OR REBOOTS ON ITS OWN BEFORE YOU CAN TROUBLESHOOT, try this: (This can be the result of a rootkit). If you get a shutdown warning, quickly do a *(Start > Run > enter: shutdown -a then click "OK")*. This will abort the shutdown and give you time to continue with this list.

e. DESKTOP BACKGROUND IMAGE: If the image looks normal, find and record the location of the image. *(Many malware removal activities can remove the desktop image):* _____

f. SAFE-MODE: If desired, you can boot into Safe-mode before continuing. *Pwr On, F8, F8, F8* . Note: that some programs like MBAM and TDSS Killer are best tried in a normal boot first. If PC boots normally, but you cannot get into safe-mode, run MSCONFIG and set the Boot option to Safe Boot.

g. POWER SETTINGS: Once the PC can boot, set the Power options to "ALWAYS ON" so the PC will not go into standby or hibernate while scans are running.

h. 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.

i. USER FILES ACCESS PERMISSIONS: If possible, look in the "C:\Users\" folder and make sure you have full access permissions to each User's folders and files. The D, or UVK Utilities can help restore permissions**.**

j. REMOVE SCHEDULED TASKS: Remove any Tasks that you do not understand. Figuring out unwanted tasks in Windows 10 is a challenge, so I use the CCLEANER PROGRAM. Be careful.

k. 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.*** .

l. STOP ALL STARTUPS: If possible install and run CCLEANER. Stop any "unusual" programs, processes, or services from automatically starting during boot, then reboot (preferably back into safe-mode. *(Do not stop any "Microsoft Services".) For a list of known undesired startups, see: http://www.bleepingcomputer.com/startups/*

m. .EXE FILES WILL NOT RUN? Download and run FixNCR.reg: http://download.bleepingcomputer.com/reg/FixNCR.reg . Then run the RKILL tool, then try the malware scans without rebooting.

n. STOP ANY ROGUES *(that are interfering with your Malware Removal Tools)*:

1) You can download and run the RKILL TOOL which helps stop active malware processes from interfering with your Malware Removal Tools. Do not reboot after running RKILL or the malware will start up again. *TIP: You may have to try RKILL a few times to get it to "Take".*

2) ESET ROGUE APPLICATION REMOVER: Try downloading and running this tool, then try your regular tools.

o. MALWARE REMOVAL PROGRAMS: USE A "FRESH INSTALL" OF ALL THESE PROGRAMS! ANY CURRENTLY INSTALLED ANTI-MALWARE PROGRAMS COULD BE CRIPPLED BY THE MALWARE. *(If possible, do all the scans below, then continue on).* If the malware prevents the installation or running of these programs, re-boot the machine, then try renaming the .exe file to something different. If they still will not run, be sure you are in Safe-mode. *(NOTE: You should download these programs using another PC and then put them onto a CD or write protected*

Flash-drive. Otherwise you can spread the infection). (Links to all these programs are in my "ANTI-MALWARE TOOLS & TIPS" sheet).

1) **First, DISABLE the real-time protection** of any currently "installed" AV programs.

2) **TDSS KILLER TOOL** (From Kaspersky): From a file protected flash-drive, install & run the latest version of the TDSS Killer Tool. First, click Additional Options, then select ☑ Verify Driver Digital Signatures and ☑ Detect TDFLS File System. *(If for some reason this tool does not work, try the "aswMBR" Rootkit Tool from Avast).* Continue with the next step whether this runs successfully or not,

3) **MBAM:**
   a) From a CD or write-protected flash-drive, install & run the latest available MalwareBytes' Anti-Malware Program. Run CUSTOM Scan all Drives, and "Scan for Rootkits". *NOTE: Since you are not yet on the internet, either run MBAM without any updates or use the separate downloadable MBAM update file to update it.*
   b) Continue with the next step whether this runs successfully or not.

4) **SAS**: Run Super AntiSpyware scan. Continue with the next step whether this runs successfully or not.

5) **MICROSOFT SAFETY SCANNER**. From a CD or write-protected flash-drive, drag the latest version of the Microsoft Safety Scanner program file (msert.exe 32 or 64 bit) to the Desktop and run it. *(Note: This tool does not need to be installed).* Continue with the next step whether this runs successfully or not.

6) **KASPERSKY VIRUS REMOVAL TOOL**: From a file protected flash-drive, drag the latest version of the Kaspersky Virus Removal Tool Install File to the desktop. Double-click the file to install it. Select options and run a scan. Let it uninstall itself when done. Continue with the next step whether this runs successfully or not.

7) **ZEMANA SCAN:** Run a full scan.

8) **HITMAN PRO 3.x**: Install Hitman Pro and run a free scan. *(Note: If malware is found, Removal is free, but starts a 30 day free trial).* Continue with the next step whether this runs successfully or not. *(See video for Force Breach Mode: http://www.youtube.com/watch?v=Kw956FtGcs&feature=em-uploademail)*

9) **D Malware Scans or UVK (Ultimate Virus Killer)**. A good follow-up to the above manual scans.

10) If the PC is still infected or re-infects after a reboot, run a standalone bootable scanner like WINDOWS DEFENDER OFFLINE, KASPERSKY RESCUE DISK, or AVG RESCUE DISK.

p. USER FILES ACCESS PERMISSIONS - AGAIN: If you were unable to do this before, run the D or UVK, Utility to restore permissions and policies.

q. CLEAN THE "HOSTS" FILE: For XP and Win:
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 "12.0.0.1 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

r. CLEAN "TEMP" FILES AGAIN: You can use CCleaner for this step orfor Win only run the TFC.EXE utility again now if desired. Run the TFC Temp File Cleaner from Oldtimer and be sure to reboot afterwards. ***NEVER RUN TFC ON WINDOWS 10!***

s. CLEAN THE "DOWNLOADS" FOLDER for every User. *(Many malware install files can be there)*. Especially remove any .exe files from the Downloads folder.

t. SCHEDULED TASKS: Using Ccleaner; Check again for any that do not belong.

u. FIREFOX:
1) Set Connection Settings to: "No proxy" *(Firefox: Tools > Options > General tab > Network proxy settings).* Connection settings Window. Click to check the button either for "No proxy" or "Use system proxy settings")
2) Check that Bookmarks are all still there. If not, restore them from backup.

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

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

2) RESET IE: *(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: *(Control Panel > Internet Options > Connections tab > LAN settings).* The Proxy Server box should NOT be checked, but "Automatically Detect settings" should be checked.

w. NETWORK CONNECTIONS: *(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.

x. CONNECT THE SYSTEM TO THE INTERNET and TEST INTERNET EXPLORER. If it does not work correctly, first restore the Advanced Settings again: *(Control Panel > Internet Options > Advanced tab > click "Restore Advanced Settings").* If IE still does not work, run the "Fix IE" Utility program, then try D, or Windows Repair Toolbox.

y. COMPLETE THE FOLLOWING TASKS:

1) RE-SCAN WITH LATEST SAS AND MBAM (FRESHLY INSTALLED & UPDATED: Again, run full-scans of SAS and MBAM. Also update and run your preferred (and updated) Anti-virus, any other desired Programs (even if you have already run them) *(see my "ANTI-MALWARE TOOLS & TIPS" sheet for details)*. Any previously installed Anti-malware programs may still be crippled and may have to be reinstalled.

2) ESET ON-LINE SCAN: Do a free on-line scan from ESET.COM. *NOTE: These scans runs a long, long time.*

3) MSE/WINDOWS DEFENDER: Update and run a full scan.

4) If things seem OK, skip to Section "POST INFECTION CLEAN-UP TASKS".

STILL HAVING PROBLEMS?

a. SAFE-MODE: If the PC is still infected and you were unable to complete the above tasks and you have not already tried them in safe-mode, go into Safe-Mode now and try all the above steps again. *(You can get to Safe-Mode by pressing F8 (many times) when you first turn on the PC*). If PC boots normally, but you cannot get into Safe-mode, run MSCONFIG and set the Boot option to Safe Boot

b. STILL INFECTED, BUT NO INFECTIONS FOUND? Newer malware is better at hiding. If the tools will not run or if they ran OK and did not find any malware, try running the WINDOWS DEFENDER OFFLINE SCANNER and/or COMBOFIX (see the tips in a later section). *(Also, if you know the name of the infection, go to www.bleepingcomputer.com, read about it in their Manual Removal Guides, and try a manual removal)*. Continue on with this guide.

c. INFECTION CLEANS OK, BUT THEN REINFECTS AFTER A BOOT: This is probably caused by an infected MBR/Track 0. Sometimes the malware can wait hours or even days before re-infecting the PC. Others re-infect after a certain number of boots. Try some of the bootable scanners like "WINDOWS DEFENDER OFFLINE". KASPERSKY RESCUE DISK, or the AVG RESCUE DISK, but at this point you will probably end up doing a Nuke and Pave *(Reformat and re-install Windows from CD/DVD)*. Run MBAR and see my "LAST RESORT" Notes on the last page of this Guide.

d. ON-LINE SOLUTIONS FOR MALWARE REMOVAL:

1) If malware is detected, but cannot be removed, write down the exact name (and syntax) of the malware detected. Then search Google using the keyword "removal" plus the specific name of the malware for ideas on how to remove it *(I always first search at bleepingcomputer.com).* Also, the Manufacturer sites for the most well known commercial anti-malware suites all have individual removal tools available for specific infections. (Usually for free). You should use only these reliable sites to get a removal tool or you may end up downloading a new infection.

2) WARNING #2: Use caution when googling the name of a virus. Lots of fake removal tools show up. Make sure the "**WOT**" add-on is installed on any browser used for researching malware.

e. If there is still suspected malware on the PC or if none of the removal tools will run, try other tools listed in my ANTI-MALWARE TOOLS & TIPS sheet. *Again, you may have to rename the ".exe" program files to get them to run.*

f. Try the "HijackThis" Utility from Trend Micro. The Trend Micro site tells you how to download and use the program. Also, see the "HijackThis Overview" in my "ANTI-MALWARE TOOLS & TIPS". Also, see this alternative called OTL: http://www.geekstogo.com/forum/topic/2852-malware-and-spyware-cleaning-guide/

g. UNALLOCATED HARD-DRIVE SPACE: Malware can hide in unallocated space *(not in hidden partitions which are for System Recovery).* Make sure all hard-drive space is fully allocated into partitions. You can verify: *(Right-click My Computer > Manage > Disk Management).* To fix this, I prefer the free EASEUS Partition Manager to avoid losing data.

h. If the PC seems to be clean of malware, continue to the POST INFECTION CLEAN-UP TASKS.

POST INFECTION CLEAN-UP TASKS

a. RESTORE ANY MISSING FILES, FOLDERS, OR ICONS: If any of the user's stuff is missing, try the free UNHIDE.EXE utility from bleepingcomputer: http://download.bleepingcomputer.com/grinler/unhide.exe **. Warning**: If the missing folders and files are set as "System" protected files, UNHIDE may not help and a manual fix is required using the DOS Prompt: IE: If the files are in a folder called C:\WORK, then this command would correct the attributes for all the files: attrib -H -S C:\WORK*.* /S /D

b. JUNKWARE REMOVAL: Run ADWCleaner and JRT (Junk Removal Tool) to clean up ads and popups. *(See my separate sheet on Junkware removal)*

c. RESET UAC (USER ACCOUNT CONTROL) (Windows , 8 & 10): Verify that UAC is turned on and set to "Always notify". *(Control Panel > Action Center), (for Vista: Control Panel > Security Center > Other Security settings)*

d. WINDOWS SERVICES REPAIR: Restore Windows Services back to their Default State with the ESET Services Repair tool. http://kb.eset.com/library/ESET/KB%20Team%20Only/Malware/ServicesRepair.exe

e. WINDOWS UPDATES: Make sure Windows Update works and all Updates are installed, including those for all Microsoft Products.

f. FIX WINDOWS FUNCTIONALITY PROBLEMS: If you have strange problems after the malware removal is done: Try **D**, **or SuperAntiSpyware (repair tools),** or Windows-Repair-All-In-One *(from www.tweaking.com)*, or "COMPLETE INTERNET REPAIR*" (rizonesoft.com).* Try running the FARBAR Service Scanner to repair corrupted or missing Windows Services.

g. DESKTOP ICONS: Make sure all Desktop Icons open properly and have not been hijacked.

h. 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 allows you to clear the history: (Win: Control Panel > System > System protection > select drive C > "Configure" > "Delete".)*

i. 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.

j. POWER SETTINGS: Set the Power options back to their original settings.

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

l. PC TUNEUP: At this point I normally continue with my 10 page "TUNEUP CHECKLIST".

"NUKE & PAVE" OPTION:

If none of the above tools removed the malware, you have only one choice, the Nuke & Pave process. This involves wiping the hard-drive, re-partitioning the hard-drive, reformatting the hard-drive, and reinstalling Windows from a Windows Install CD/DVD or the Recovery Disks. Note: Merely reformatting Partition "C" is no longer adequate as malware has been found hiding in the Master Boot Record and in unallocated drive space. For details, see my writeup: "NUKE and PAVE CHECKLIST FOR INFECTED PC's".

NOTES & MORE TOOLS:

- *For links to the various recommended malware 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*
- For more ideas, see the Malware Removal Guides from majorgeeks.com and gemstatecomputers.com. Help is also available from bleepingcomputers.com:
  http://forums.majorgeeks.com/showthread.php?t=3540 and from
  Http://docs.google.com/Doc?docid=0AaqZNZywWLNIZGc1cHZjZ2NfMGc0N2ZucWNw&hl=en
  http://www.geekstogo.com/forum/topic/2852-malware-and-spyware-cleaning-guide/
- For a virus removal tutorial, see the video podcast at: http://www.technibble.com/categories/video-podcasts/
- Also, see these Malware Removal VIDEO's from Microsoft's Mark Russinovitch:
  http://www.youtube.com/watch?v=fXFcU_DKi_c NOTE: This is an 8-part video. The link is for part 1 of 8. Watch them all. There is also a writeup on his procedure starting on page 9 of this document:
  http://download.microsoft.com/download/0/3/3/033166E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_1_1_English.pdf
- ROOTKIT REMOVAL: See this article from www.technibble.com:
  http://www.technibble.com/how-to-remove-a-rootkit-from-a-windows-system/
- BLEEPING COMPUTER TOOLS:
  - ✓ How to use Inherit.exe and MiniToolBox: http://www.bleepingcomputer.com/forums/topic442232.html
  - ✓ Also see Bleepingcomputer.com for more ideas: Go to the Search box, select "Search BC" and then enter the name of the malware you are trying to remove in the search box.