

# HOW TO REMOVE MALWARE FROM YOUR PC

Jim McKnight

www.jimopi.net

RemoveMW.lwp

revised 2-20-2012

**\*\*\* 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. There is a risk of crashing the system with some of the tools and making it unbootable, especially with COMBOFIX and the ROOTKIT TOOLS, so this process is best done by an experienced technician.

Understand that the only way to be 100% assured a system is fully cleaned is the "Nuke & Pave" process discussed at the end of this sheet under "Last Resort" Options. Any malware removal process other than a 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 next steps. **BE SURE TO COMPLETE ALL STEPS SHOWN IN BOLD** to help make sure the malware is really gone.

For links to the various recommended malware removal tools, see my sheet called "ANTI-MALWARE TOOLS & TIPS" at [www.jimopi.net](http://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/>

## IMAGE BACKUP:

- Before starting this process, I suggest you first make a full image backup of the entire main hard-drive using a standalone bootable **Rescue CD** of Acronis True Image or some other good image backup program. Then, if anything goes wrong, you can recover data or even put everything back the way it was before you started and then you can all 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.**

## 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 UBCD4WIN or a Windows Install CD so you can run `chkdsk /r`. (*Note: The file system may be corrupted from the user messing with things trying to remove the malware*). See my "TROUBLESHOOTING XP" or "TROUBLESHOOTING WINDOWS 7" sheet for other "fail to boot" suggestions.
  - 4) Look for "0 kb" FILES: Using a CD bootable operating system like UBCD4WIN or LINUX, inspect the `C:\Windows\System 32\` folder for any files that are 0 kb in size and delete them or move them to a backup folder for safekeeping in case they are needed.
  - 5) If you still cannot boot the system, or the system boots OK but is non-responsive, then download the latest WINDOWS DEFENDER OFFLINE SCANNER (AKA - Microsoft Standalone System Sweeper) on another PC (32-bit or 64-bit). *NOTE: If there is a "C:\Program files (x86 folder)" then it is a 64-bit System*). Install it to a Flash drive or CD, then boot it and scan the system's hard-drive.
  - 6) Also you can also burn a KASPERSKY RESCUE DISK or AVG RESCUE DISK on another PC. Boot the CD and run scans against the system's hard-drive. (*NOTE: Kaspersky is not updated regularly and needs network access to on-line updates from the infected system after it is booted*).
  - 7) 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. PC BOOTS OK, BUT EITHER DOES NOT RESPOND OR WILL NOT RUN ANY PROGRAMS:
  - 1) Try running in Safe-Mode. If Safe-Mode works, go to step "d. POWER SETTINGS" & continue on.
  - 2) If you programs will not run in Safe-Mode, try steps 5 and 6 above.
  - 3) For XP, if strange messages come up when trying to run programs, try the registry fix for the type of file that will not run: [http://www.dougknox.com/xp/file\\_assoc.htm](http://www.dougknox.com/xp/file_assoc.htm) Then continue on.
  - 4) If many programs/scans pause, stop, freeze, or hang, run COMBOFIX. If COMBOFIX hangs, try rerunning it (*An infected regedit.exe can cause this. Read about the SirCam Worm*)
- c. 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 run "COMBOFIX", then continue with this list.
- d. **DESKTOP BACKGROUND IMAGE:** If the image looks normal, find and record the location of the image, since many malware removal activities can remove the desktop image\_\_\_\_\_
- e. **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.
- f. **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.
- g. **TRY SYSTEM RESTORE:** If the system boots OK into Normal or Safe-Mode, try doing a System Restore to get the system back to where the malware is not active. *Note: This has its risks.*
- 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. **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 here is the path: (*Win7: Control Panel > Administrative Tools > Task Scheduler*). Be careful.
- j. **TEMP FILE CLEANER:** (TFC.EXE) If this utility will load and run, use it now to cleanup all the temp folders for all users. **WARNING:** *It will do an auto-reboot at the end to finish.* If TFC will not run, try it in Safe-Mode. If it will still not run, skip this step and continue to the next step.
- k. **STOP ALL STARTUPS:** If possible install and run the CODESTUFF STARTER utility or use MSCONFIG. 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/>*
- l. **.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.
- m. **RKILL TOOL:** You can also 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".*
- n. **MALWARE REMOVAL PROGRAMS:** USE A "FRESH INSTALL" OF ALL THESE PROGRAMS! THE CURRENT INSTALLATION 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 rename the ".exe" file of the desired program and try running it again. 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) **SAS:** From a CD or write-protected flash-drive, drag the latest version of the SUPER ANTISPYWARE PORTABLE SCANNER file to the Desktop. Double-click to run it. *(Note: This tool does not need to be installed).* Continue with the next step whether this runs successfully or not.
- 4) **MBAM:**
  - a) From a CD or write-protected flash-drive, install & run the latest available MalwareBytes' Anti-Malware Program. *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) Chameleon. If MBAM will not run, go to *(Start > All Programs > Malwarebytes'Anti-Malware > Tools > MBAM Chameleon)*. If you cannot get to Chameleon via the start Menu, go to: *(C:\Program Files\Malwarebytes' Anti-Malware\Chameleon)* and open chameleon.chm. Click each "Test Now" button until you find one that works. *(for 64-bit machines, use C:\ProgramFiles(x86)\Malwarebytes..)*
  - c) 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) **HITMAN PRO 3.5:** 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.
- 8) **D7 Malware Scans or UVK (Ultimate Virus Killer).** A good follow-up to the above manual scans.
- 9) 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.
- o. **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" entry. *(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>
- p. **CLEAN "TEMP" FILES AGAIN:** You can use CCleaner for this step or the TFC.EXE utility again now if desired. For Ccleaner, run for EVERY User Account on the PC.
  - 1) LIST ALL USER ACCOUNTS: From any "Administrator " level Account make a list of all User Accounts on the PC: *(XP: Right-click My Computer > Properties > Advanced tab > User Profiles "Settings" button)* *(Win7: Right-click Computer > Properties > Advanced system settings > User Profiles "Settings" button).* .
  - 2) TFC: Run Temp File Cleaner again.
  - 3) CLEAN EACH USER ACCOUNT: Log on to each User Account (including the "administrator" account) and run the following items:
    - a) TEMP FOLDER: Click Start, run: %temp% and delete all the files listed that are not in use.
    - b) CCLEANER:
      - i) FILE CLEAN: Run the CCleaner Utility (with all boxes checked) to clean out more temp files.

- ii) **REGISTRY CLEAN:** If you want, run the Registry cleaner portion of CCleaner. (*Glary Utilities is also a good program for this*). *Warning: Problems can arise if you clean the Registry on Windows 7.*
- q. **CLEAN THE “DOWNLOADS” FOLDER for every User.** (*Many malware install files can be there*). \_
- r. **SCHEDULED TASKS:** Check again for any that do not belong: (*XP: Control Panel > Scheduled Tasks*).
- s. **FIREFOX (“No” PROXY):** (*Firefox: Tools > Options > Advanced tab > Network tab > Connection settings*). Check the button for “No Proxy” or “Use system proxy settings”
- t. **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.
- u. **NETWORK CONNECTIONS:** (*XP: Control Panel > Network Connections, then right-click the desired adapter > Properties > then TCP/IP > Properties*). (*Win7: Control Panel > Network & sharing center > Change adapter settings, then right-click the desired adapter > Properties > then TCP/IP/IPv4 > Properties*). Make sure all Network Adapters are set to “Obtain an IP Address Automatically” and “Obtain a DNS server address Automatically.
- v. **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 DIAL-A-FIX
- w. **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) **SPYBOT SEARCH & DESTROY:** Install, update, and run a full scan. Also, do the IMMUNIZE Function. (*This will clean up and insert good entries in the HOSTS file*).
  - 3) **ESET ON-LINE SCAN:** Do a free on-line scan from ESET.COM, Kaspersky (*available soon*), Trend, or Panda). *NOTE: These scans runs a long, long time.*
  - 4) **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.*
  - 5) **MSE:** If MSE is installed on the system, update and run a full scan.
  - 6) **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*).
- 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](http://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*). See my "LAST RESORT" Notes on the last page of this Guide.

- d. COMBOFIX: Quick Tips before running COMBOFIX:
  - 1) FIRST record the name of the Desktop background image file and the IE Homepage URL/s so they can be restored after running COMBOFIX.
  - 2) Also, first disable any real time anti-malware program processes. For details, see: <http://www.bleepingcomputer.com/forums/topic114351.html>
  - 3) Be sure to download the latest version.
  - 4) For Vista and Windows 7, you must disable UAC before running COMBOFIX. (*Note: COMBOFIX auto-reboots at the end of the run*).
  - 5) WARNING: Make double sure you have an image backup of drive "C" before running COMBOFIX, as it can make a PC unbootable if there are any irregularities with the MBR or Track 0.
- e. 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) Check out [www.download.com](http://www.download.com) to see the ratings of various specific specialty removal programs.
  - 3) WARNING #1: Some programs come with a free trial & will detect for free, but you have to buy it to remove the malware. Most good removal tools are free.
  - 4) 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.
- f. 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.*
- g. Try the "HijackThis" Utility from Trend Micro. The Trendmicro site tells you how to download and use the program. Also, see the "HijackThis Overview" in this document.
- h. UNALLOCATED HARD-DRIVE SPACE: Newer 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: (*XP & Win7: Right-click My Computer > Manage > Disk Management*). To fix this, I prefer the free EASEUS Partition Manager to avoid losing data.
- i. 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>
- b. **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*).
- c. **FIX WINDOWS FUNCTIONALITY PROBLEMS:** If you have strange problems after the malware removal is done: Try **DIAL-A-FIX** (*XP only*), or **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" (*rizonsoft.com*).
- 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](http://www.jimopi.net)*).

g. **CCLEANER - WIPE FREE SPACE:** Now is a good time to run this Ccleaner option on the hard-drive.

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

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

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

## "LAST RESORT" OPTIONS:

If none of the above tools have removed the malware, you have only two choices:

- 1) **IMAGE RESTORE:** Restore your system from a full image backup (**including all partitions and the MBR**) taken prior to the malware infection.
- 2) **NUKE & PAVE:** (Wipe the drive, re-partition the hard-drive, reformat the hard-drive, and re-install Windows) 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. See my "NUKE and PAVE CHECKLIST FOR INFECTED PC's" for details.

For more ideas, see the Malware Removal Guides from [majorgeeks.com](http://majorgeeks.com) and [gemstatecomputers.com](http://gemstatecomputers.com). Help is also available from [bleepingcomputers.com](http://bleepingcomputers.com):

<http://forums.majorgeeks.com/showthread.php?t=35407> and from

<http://docs.google.com/Doc?docid=0AaqZNYwWLNIZGc1cHZjZ2NfMGc0N2ZucWNw&hl=en>

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 Russinovich:

[http://www.youtube.com/watch?v=fXFcU\\_DKi\\_c](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 97 of this document:

[http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft\\_Security\\_Intelligence\\_Report\\_volume\\_11\\_English.pdf](http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf)

**ROOTKIT REMOVAL:** See this article from [www.technibble.com](http://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.

Special thanks to Stephen Cherubino ([www.podnutz.com](http://www.podnutz.com)), Mike Smith ([www.miketechshow.com](http://www.miketechshow.com) and [tech-vets.com](http://tech-vets.com)), Bryce Whitty ([www.technibble.com](http://www.technibble.com)), and the members of the Yahoo group:

"computertechpros" for many ideas that helped me create this guide and keep it current.