ANTI-MALWARE TOOLS & TIPS ©

Jim McKnight *www.jimopi.net* *ANTIMALWARE_Tips.lwp* *revised 10-1-2017*

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

CONTENTS:

ANTI-MALWARE TOOLS

MY FAVORITE (Go-To) MALWARE REMOVAL TOOLS (alphabetically):

- **AdwCleaner** (cleans Adware, junk toolbars etc) Free: http://www.bleepingcomputer.com/download/adwcleaner/
- **BitDefender Ransomware Recognition Tool:** https://labs.bitdefender.com/category/free-tools/
- **ESET (NOD32) Online Scanner**: http://www.eset.com/us/online-scanner
  (Downloads & installs an ActiveX add-on for Internet Explorer. In Windows 7, IE must be "Run as Administrator")
- **Kaspersky Virus Removal Tool** - Free http://www.kaspersky.com/antivirus-removal-tool?form=1
  If the link fails, go here and find it on the list: http://support.kaspersky.com/viruses/utility
- **MBAM-Malwarebytes Anti-Malware** - 2000/XP/Vista/Win7 (Free, but no free Resident Shield):
  http://www.download.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html?tag=mncol
- **SAS-SUPERAntispyware** (XP/Vista/7) - Free: http://www.superantispyware.com/superantispywarefreevspro.html
- **SAS-SUPERAntispyware Portable** (Portable Scanner for infected PC's): http://www.superantispyware.com/onlinescan.html
- **Spybot S&D version (1.6.2 only) - Free:** http://filehippo.com/download_spybot_search_destroy/5168/
  NOTE: I do not use or recommend version 2.0 of Spybot S&D.
- **TDSS Killer** from Kaspersky (Rootkit remover) - Free: http://support.kaspersky.com/downloads/utils/tdsskiller.zip
- **See also the "BOOTABLE RESCUE CD's" below.**

MY FAVORITE "STANDALONE" MALWARE REMOVAL TOOLS (PORTABLE or ONLINE):

- **SUPER ANTISPYWARE "On-line" scan**: (Download & run) - Free: http://www.superantispyware.com/onlinescan.html
- **ESET NOD32 Online Scanner:** http://www.eset.com/online-scanner
- **MBAR - Malwarebytes Anti-ROOTKIT -** http://downloads.malwarebytes.org/file/mbar
- Microsoft Safety Scanner (downloadable Scanner tool) -Free: http://www.microsoft.com/security/scanner/en-us/default.aspx

BOOTABLE RESCUE CD's (ISO Images to create a Bootable CD):

- Overview of Rescue CD's http://blogs.techrepublic.com.com/security/?p=3803&tag=content;leftCol
- **HitmanPro-Kickstart** (bootable USB) Free: http://www.surfright.nl/en/kickstart
- AVG - Rescue CD: http://www.avg.com/us-en/download-file-cd-arl-iso

- AVIRA RESCUE CD or Anti-Rootkit Tool - Free http://www.avira.com/en/support/support_downloads.html
  (This CD does not update the signature files. You have to download it just before running for the latest files)
- Kasperksy Rescue CD (ISO Image) - Free: http://devbuilds.kaspersky-labs.com/devbuilds/RescueDisk10/kav_rescue_10.iso
  ✓Set to "Prompt on Completion" or it will stop on every issue found. (2011 version not available ????)
- Katana Portable Security suite - Free: http://www.hackfromacave.com/katana.html
- **Windows Defender Offline** - Free: http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline
  AKA - Microsoft System Sweeper http://connect.microsoft.com/systemsweeper NOTE: WDO requires at least 768 MB of RAM, preferably 1 GB. Otherwise it will fail with a 0x80508007 low memory error.
- Norton Bootable Recovery Tool: http://security.symantec.com/nbrt/nbrt.asp?lcid=1033&origin=default
- SHARDANA Rescue CD builder Utility http://www.sarducd.it/downloads.html
- Trinity Rescue Kit = Free: http://trinityhome.org/Home/index.php?wpid=1&front_id=12
- Ultimate Boot CD for Windows (UBCD4WIN.COM) See my UTILITY PROGRAMS sheet for details.

WINDOWS REPAIR TOOLS (For after the Infections are cleaned) *(All free)*

- CleanUp! (by Steven Gould) - free http://www.stevengould.org/index.php?option=com_content&task=view&id=29&Itemid=72
- **COMPLETE INTERNET REPAIR** Utility (RIZONE): http://www.rizonesoft.com/2011/complete-internet-repair/
- **D7** (REPAIR TOOLS & malware remove assistance): http://sites.google.com/a/obxcompguy.com/foolish-it/d7
- **OTC** by Oldtimer (cleans up PC after malware removal): http://oldtimer.geekstogo.com/OTC.exe
- SUPERAntiSpyware REPAIR TOOLS (part of the Super Antispyware program)
- **Windows_Repair_ALL_IN_ONE** http://www.tweaking.com/content/page/windows_repair_all_in_one.html
- **FARBAR SERVICE SCANNER**: http://download.bleepingcomputer.com/farbar/FSS.exe
  Helps repair connectivity after a malware cleaning: http://www.bleepingcomputer.com/forums/topic441075.html
- FIX IE (Fixes IE settings after a malware attack - IE7, IE8): http://www.thewindowsclub.com/downloads/Fix%20IE.zip

MY FAVORITE PROTECTION TOOLS

- **Microsoft Security Essentials (Windows 7)** - Free: http://www.microsoft.com/security_essentials/
- **AVIRA AntiVir Personal Free (XP/Win7/Win8)** (Click "Download latest version") http://filehippo.com/download_antivir/
- **SpyBot Search & Destroy** (**ver 1.6.2 only**) - Free: http://filehippo.com/download_spybot_search_destroy/
  (Uncheck TeaTimer & IE Helper during install) ***NOTE: I do not like or use version 2.0 of SpyBot S&D.***
- **SANDBOXIE** - Free http://www.sandboxie.com/index.php?DownloadSandboxie
  See the writeup on SANDBOXIE at www.jimopi.net under MALWARE TOPICS

OTHER USEFUL TOOLS:

- AVG Free 9 Anti-malware Suite (2000/XP/VISTA/Win7) - Free: http://www.filehippo.com/download_avg_antivirus/
  Here is the AVG feature comparison chart (Free vs Paid versions): http://free.avg.com/download-avg-anti-virus-free-edition
  ✓AVG - Manual Virus Removal Tools: http://www.avg-antivirus.com.au/avg_virus_removal.htm
  ✓AVG - LinkScanner (Separate browser add-on from AVG)
  http://download.cnet.com/AVG-LinkScanner/3000-2162_4-10610872.html?tag=mncol
- AVIRA AntiVir Personal - (2000/XP/Vista/Win7. Click "Download latest version") Free: http://filehippo.com/download_antivir/
- Ad-Aware (I no longer recommend Adaware) *(Note: It may have problems with AVG & Spybot S&D)*
- A-Squared Free - 3.5 Scan& removal 98/XP http://www.emsisoft.com/en/software/download/
- Aries Rootkit Remover (for Sony Rootkit) http://lavasoft.com/support/securitycenter/aries_rootkit_remover.php
- Avast! (Supports XP/Vista/Win7) see my notes; http://filehippo.com/download_avast_antivirus/
- Avast: "ASW MBR" MBR Rootkit Remover: http://public.avast.com/~gmerek/aswMBR.htm
- ComboFix - Free (Vista & Windows 7 only Use the Tutorial)
  Http://www.bleepingcomputer.com/combofix/how-to-use-combofix
  ✓See the tips in this sheet.
- Comodo Cleaning Essentials - Free: http://www.comodo.com/business-security/network-protection/cleaning_essentials.php

ANTI-MALWARE TOOLS & TIPS ©

- D7 (malware remove assistance) http://sites.google.com/a/obxcompguy.com/foolish-it/d7
- Dial-a-fix (for experts only, XP only) - Free http://wiki.lunarsoft.net/wiki/Dial-a-fix
- ESET ROGUE APPLICATION REMOVER: http://kb.eset.com/esetkb/index?page=content&id=SOLN3035&locale=en_US
- Fake Anti-Virus Removal Tool (Trend Micro) - Free: http://esupport.trendmicro.com/solution/en-us/1056510.aspx
- GMER Rootkit Remover - Free http://www.gmer.net/files.php
- HijackThis *(see writeup below)* - Free www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis
- Hitman Pro - Second opinion scanner - Free? http://www.surfright.nl/en/downloads
- KillBox - Free http://killbox.net/
- Malicious Software Removal Tool (Start, Run, mrt.exe) - Free www.microsoft.com/security/malwareremove/default.mspx
- McAfee Rootkit Detective - Free http://www.pcworld.com/downloads/file/fid,67387-page,1-c,privacysecurity/description.html
- Microsoft Safety Scanner (downloadable Scanner tool) -Free: http://www.microsoft.com/security/scanner/en-us/default.aspx
- Microsoft Security Awareness Training: http://msdn.microsoft.com/en-us/security/cc165442
- Norton Scan & Clean - Free http://www.softpedia.com/get/Antivirus/Norton-Security-Scan.shtml
- OTL from OLDTIMER:: http://www.geekstogo.com/forum/topic/2852-malware-and-spyware-cleaning-guide/
  "How-To" video from Britec09: http://www.youtube.com/watch?v=2KsVWmHKCT8
- QUICK FIX PLUS (Portable tools by LeeLu Soft)
  - ✓For XP http://download.cnet.com/XP-Quick-Fix-Plus/3000-2094_4-10976875.html?tag=mncol
  - ✓For Win7: http://download.cnet.com/7-Quick-Fix/3000-2094_4-75024066.html?part=dl-10055425&subj=dl&tag=button
- RKILL (four versions) - Free. Try the first version that works on the infected PC.
  1. Rkill.exe: http://download.bleepingcomputer.com/grinler/rkill.exe
  2. Rkill.com: http://download.bleepingcomputer.com/grinler/rkill.com
  3. Rkill.scr: http://download.bleepingcomputer.com/grinler/rkill.scr
  4. Rkill - Others: http://www.bleepingcomputer.com/download/rkill/
- "Remove Fake Antivirus" - Free: http://www.softpedia.com/get/Antivirus/Remove-Fake-Antivirus.shtml
- RogueKiller (Select 32bit or 64bit) http://www.adlice.com/softwares/roguekiller/
- RRT AV Toolkit (XP/Vista/Win7 32 bit) http://www.sergiwa.com/modules/mydownloads/singlefile.php?cid=2&lid=1
- RUBotted (Trend) - Free www.trendsecure.com/portal/en-US/tools/security_tools/rubotted
- SANDBOXIE - Browsing protection Free: http://www.sandboxie.com/index.php?DownloadSandboxie
  - See the writeup on SANDBOXIE at www.jimopi.net under MALWARE TOPICS.
- SmitFraudFix - Free http://siri.geekstogo.com/SmitfraudFix.php
- SOPHOS Rootkit remover - Free: http://www.snapfiles.com/downloads/sophosantiroot/dlsophosantiroot.html
- SOPHOS Virus Removal Tool - Free: http://www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx
- Spyware Doctor Starter Ed.- Free http://www.download.com/Spyware-Doctor-Starter-Edition/3000-8022_4-10704508.html
  (Caution: May install unwanted Toolbars)
- Secunia PSI - Free (see my UTILITY PROGRAMS sheet.
- SUPERFISH REMOVAL TOOL - Free: http://support.lenovo.com/us/en/product_security/superfish_uninstall
- Symantec Malware Manual Removal Tools: http://www.symantec.com/business/security_response/removaltools.jsp
- TFC Temp File Cleaner (cleans out temp files for all users at once) http://software.addpcs.com/tfc/index.php
- ThreatFire Anti-virus - Free: http://www.threatfire.com/?utm_source=download.com&utm_medium=frontdoor
- Trojan Remover ($34.00, 30 day free trial): http://www.download.com/Trojan-Remover/3000-8022_4-10038982.html?tag=mncol
- UNHIDE.EXE (Restore missing files and folders after an infection) -free: http://download.bleepingcomputer.com/grinler/unhide.exe
- VIPRE PC Rescue Program - portable: Free http://live.sunbeltsoftware.com/
- VundoFix: Scans & Fixes Trojans. http://vundofix.atribune.org/

- Virus Test: Test your A/V Program (RISKY!) - Free: http://www.eicar.org/anti_virus_test_file.htm.
- Virus Effect Remover - Free: http://download.cnet.com/Virus-Effect-Remover/3000-2239_4-10920269.html
- X-rayPc Spyware Remover & Analyzer - Free: http://www.x-raypc.com/

ONLINE SCANNING TOOLS

- **ESET NOD32 Online Scanner:** http://www.eset.com/online-scanner
- Kaspersky Online scanner: http://download.cnet.com/Kaspersky-Online-Virus-Scanner/3000-8022_4-10723401.html?tag=mncol
- JOTTI (Scans an individual file online) http://virusscan.jotti.org/en
- Trend Micro House Call - Free malware scan: http://housecall.trendmicro.com/.
- Panda Cloud Antivirus - Free http://filehippo.com/download_cloud_antivirus/
- Shields Up! Open Port Scanner: http://www.grc.com/x/ne.dll?bh0bkyd2
- WEBSITES TO UPLOAD AND SCAN A SUSPICIOUS FILE FOR MALWARE:
  - Jotti: http://virusscan.jotti.org/en
  - VirusTotal: http://www.virustotal.com/
- WEBSITES TO SCAN A SUSPICIOUS WEBSITE FOR MALWARE *(SCAN A URL)*:
  - VirusTotal: http://https://www.virustotal.com/en/#url
  - SUCURI http://sitecheck.sucuri.net/scanner/
  - GOTMLS for WORDPRESS SITES: http://gotmls.net/

AD-AWARE: (Note: I no longer recommend Ad-Aware. I experienced too many conflicts with other programs, plus other issues.)

AUTOPLAY~AUTORUN DISABLE: Autoplay~Autorun is a big PC vulnerability: Since Autoplay allows code to be immediately executed upon insertion of the media (CD/DVD, FLASH drive, EXT-HDD, FLOPPY, etc), malware can infect your PC before any action can be taken. Autoplay should be disabled for all removable devices:

- **Windows 7:** See my sheet called WINDOWS 7 TIPS".
- **Windows XP**: See my sheet called "XP TIPS"

AVAST! FREE ANTIVIRUS

- You have to register with Avast once a year to keep it running.
- Download from: http://filehippo.com/search?q=avast
- For me, Avast! Does NOT play well with Sandboxie so I do not use it.

AVG FREE: **NOT RECOMMENDED**: I have had too many issues with later versions of AVG and no longer recommend it. For free tools, I recommend MSE, Malwarebytes Anti-malware, SuperAntispyware, and SpyBot Search and Destroy. For browser protection, I recommend the "WOT" addon (Web Of Trust). If you really must have a paid antivirus, I suggest KASPERSKY or ESET NOD32. (4-2011)

AVIRA ANTIVIR PERSONAL Free - TIPS (re: version 14.x)

- INSTALL: Note: By default, Avira runs a resident shield and auto updates every 6 hours, and is set up to do a scheduled Quick System Scan every 168 hours.
- AVIRA plays well with SANDBOXIE.
- UPDATES: By default, Avira will check for Updates every 6 hours. You can change it if you want. After you first install Avira, click the "Start Update" button
- SCHEDULED SCANS: After first installing Avira, open Avira and click on Scheduler.
  1) The default setting is a Quick Scan every 168 hours.
  2) In addition to the default scan, you can add a Scan Job and make it scan daily, weekly, monthly and pick the day of the week and time of day too. Quick Scan, Complete System Scan, Scan for rootkits, and Active Malware & Rootkit scan, etc.

- "GUEST" USER ACCOUNT: Warning: Avira does NOT run in Guest user accounts. The recommended solution is to manually create a limited or Standard User account and call it Visitor or Guest2, instead of using the built-in "Guest" account.

AVOIDING MALWARE INFECTIONS:

- See the "A STRESS FREE PC" article on my website at www.jimopi.net for ideas to help secure your PC.
- See my separate sheet called: "MY ADVICE FOR AVOIDING MALWARE INFECTIONS" at www.jijmopi.net

BROWSER PROTECTION

- SANDBOXIE - Free: http://www.sandboxie.com/index.php?DownloadSandboxie

COMBOFIX Notes:

- COMBOFIX can crash a PC and should only be used by experienced Techs.
- For Vista and Windows 7, you must disable UAC before running COMBOFIX.
- Using the Console with Combofix: http://www.bleepingcomputer.com/combofix/how-to-use-combofix
- Using the Windows Recovery Console: http://support.microsoft.com/kb/314058/
- Obtaining the XP Recovery Console from Microsoft: http://support.microsoft.com/kb/310994
- For more user tips, see: http://www.bleepingcomputer.com/forums/topic273628.html
- To remove the Recovery console from the Boot screen after using COMBOFIX, see: http://support.microsoft.com/kb/555032

CRYPTOLOCKER: *(UNLOCK ENCRYPTED FILES):*

- FREE:
- See this site: http://krebsonsecurity.com/2014/08/new-site-recovers-files-locked-by-cryptolocker-ransomware/
- And this site: http://https://decryptcryptolocker.com/

FIREFOX ADD-ONS for enhanced security:

- **WOT** for Firefox http://www.mywot.com/en/download/ff
- LinkExtend http://https://addons.mozilla.org/en-US/firefox/addon/10777
  LinkExtend help http://www.linkextend.com/help/ *See my Firefox Tips for details*
- NoScript http://https://addons.mozilla.org/en-US/firefox/addon/722

KASPERSKY

- If you feel you need to pay for your anti-malware protection, Kaspersky Internet Security or Kaspersky Antivirus is a good one. Be forwarned that Kaspersky is very difficult to remove once you install it. Also, Kaspersky has given me problems causing errors with SANDBOXIE.
- KASPERSKY RESCUE CD.
  - Note: If a PC is locked by FBI or Police Ransomeware. Try booting to a Kaspersky Rescue CD, go to TERMINAL (on the Start menu of Kaspersky) and type WINDOWSUNLOCKER, Then reboot and run your virus scans as you normally would.

MBAM: (MalwareBytes Anti-Malware):

- MBAM Free is a great malware scanner, but does not have real-time protection. Only the Paid "MBAM Pro" version does. *See below.*
- On a severely infected PC, the MBAM.EXE file may have to be renamed in order to run. IE: bonbon.exe
- If MBAM results in any error messages, check the Help file's list of error codes within its program folder: MBAM.CHM
- If you are unable to get online updates for MBAM on an infected PC, you can download them on another PC as a separate file from: http://data.mbamupdates.com/tools/mbam-rules.exe . Put the file on the infected PC and double-click it. It will install the new rules.
- When installing the latest version of MBAM, a new window pops up asking to either "Decline" or "Start Trial". Be sure you click "Decline" so you are not tricked into paying for MBAM. If you did start the trial and it expires, you will be asked to pay for MBAM. If you are expired, you should be able to click a button called "End Trial". If that does not work, you will have to remove MBAM, reinstall it, and then click Decline to use the free version.
- FREEZES DURING A SCAN: Run MBAM in Safe-Mode.

- **MBAM PRO**:
  - ✓ If you buy the paid version (A one-user license is about $25.00), the license is lifetime, no renewals. Includes automatic updates, real-time protection, and allows set-up of a scheduled scan.
  - ✓ If you paid for MBAM Pro and want to run the full-time protection alongside MSE, go to the following tutorial to set exclusions for MSE and MBAM to avoid conflicts. *(See Section "**I**")*:
    http://forums.malwarebytes.org/index.php?showtopic=10138&st=0&p=497675&#entry497675
  - ✓ To set up a scheduled scan, use the same tutorial page as above. *(See Section "**O**")*

MICROSOFT SAFETY SCANNER - See my sheet called "FREE ANTI-MALWARE TOOLS FROM MICROSOFT" for details on this scanner.

MICROSOFT SECURITY ESSENTIALS (MSE)

As of 4.8.2014, MSE IS NO LONGER SUPPORTED FOR XP PC's. I recommend using AVIRA for your XP machine. Microsoft Security Essentials (MSE) offers real-time protection, automatic updates, and scheduled scans. MSE works with Vista, and Windows 7.

- **GENERAL INFO:**
  1. An Overview of MSE can be found in my sheet called "FREE ANTI-MALWARE TOOLS FROM MICROSOFT" at http://www.jimopi.net .
  2. Get the free download of MSE and read more about it at: http://www.microsoft.com/security_essentials/
- **DOWNLOAD MSE**:
  1. On the Microsoft Security Essentials Home page, click the <Download Now> button.
  2. Click the <Download> button and save the "mse installer" file.
  3. Close your Browser.
- **INSTALL MSE**:
  1. Double-click the downloaded "mse installer" .exe file. Click <Next>, Then <Validate>. If you are not a pirate or a criminal, you will be at the License Agreement screen.
  2. Click **"I accept the terms...."**, then click <Next>.
  3. Click **"Complete"**. Click <Next>, then click <Install>.
  4. You can choose to "Check for definitions and run a quick scan now" or not. Your choice. Click <Finish>.
- **CONFIGURE MSE**:
  1. The default setup is an Automated Weekly scan. To change this; *(Settings tab > click Scheduled scan).* Then set up your Automatic Scanning as desired.
  2. Unless you are an expert, leave all the other settings at default. Click <Save changes> to exit.
- **REMOVE MSE**: (If Add/Remove Programs will not work)
  1. Make sure the installer file is in the system root. Start > Run > mssefullinstall-x86fre-en-us-xp.exe /U

ON-LINE PROTECTION SCANS.

- On-line scanners use an ActiveX add-on for Internet Explorer. Some of the On-line scanners allow you to use Firefox and Chrome *(using JAVA).*
- ESET Online scanner is my preferred online scanner. You can check a box to tell it to either remove any found malware or just scan. *I usually uncheck the box for "Remove found threats". I always check the box to "Scan Archives". I also click on Advanced Settings, then check the boxes for "Scan for potentially unwanted applications (PUP's)", and "Scan for potentially unsafe applications".*
- See my list of ONLINE SCANNING TOOLS (above) for a list of more on-line scanners.

SECUNIA PSI - See my "UTILITY PROGRAMS" sheet for details.

SPYBOT SEARCH & DESTROY VERSION 1.6.2 TIPS

- ***NOTE: I do not use or recommend the new Version 2.0 of Spybot S&D.***
- Version 1.6.2 is available from filehippo.com: http://filehippo.com/download_spybot_search_destroy/5168/
- To stop those nagging messages to "approve or deny Registry changes", turn off "TeaTimer" by doing the following:
  1. First, you should be running Spybot version 1.6.2. If not, remove Spybot and install this version.
  2. Open Spybot, then click: *Mode > Advanced mode. Then click Tools (in LH column) > Resident (in LH Column*). In the "Resident" window, UNCHECK both: "☐ Resident SDHelper" and "☐ Resident TeaTimer"

3. If desired, you can go back to basic mode by clicking *(Mode > Default mode).*
4. Close SpyBot.

- With both VISTA and WINDOWS 7, Spybot must be run in "Administrator mode".
- IE8: When IE 8 first came out, users experienced slow startup problems caused by SpyBot immunizations. Microsoft fixed this with Update KB969897 released in June 2009 for XP and Vista. If you choose to use both IE8 and Spybot, and IE8 is very slow to start up, make sure this update is installed. (It has been superceded by even newer updates for IE8). I never had any problems with IE8 and SpyBot running under Windows 7.

SUPERAntispyware Notes:

- This program is a great scanner, but the free version does not have real time protection.
- SYSTEM & BROWSER REPAIR TOOLS: *Click Preferences > Repairs tab > Select item > click Perform Repair.*
- ON-LINE SCAN: This is actually a downloadable standalone scanner that does not need to be installed on the infected system. If the infected system can go on the internet, download the latest version of the "SAS_nnnnnn.exe" file and run it. If not on the internet, then download it to another PC and burn to a CD or write protectable flashdrive. Run it from that. *Note: Each time you download it, the file name is different. This is to confuse the hackers*. http://www.superantispyware.com/onlinescan.html
- UBCD4WIN: SUPERAntispyware is included in the UBCD4WIN CD package and can be updated before scanning if you have Networking enabled.

WINDOWS DEFENDER: See my sheet called "FREE ANTI-MALWARE TOOLS FROM MICROSOFT" at: at http://www.jimopi.net .

REMOVING COMMERCIAL ANTI-MALWARE SUITES

- ESET AV REMOVER: Pick 32 or 64-bit http://support.eset.com/kb3527/#removable
- APPREMOVER (from OPSWAT.COM) http://www.opswat.com/appremover/AppRemover.exe
- AVAST! UNINSTALL UTILITY http://www.avast.com/uninstall-utility
- AVG REMOVER (avgremover.exe) : http://www.avg.com/ww-en/utilities
- AVIRA REGISTRY CLEANER http://www.avira.com/en/downloads#tools
- CA (Computer Assoc's): Go to http://support.ca.com/irj/portal/anonymous and search for TEC481327
- CA: eTrust Antivirus 7.x http://supportconnect.ca.com/sc/kb/techdetail.jsp?searchID=TEC436187&docid=436187&bypass=yes&fromscreen=kbresults
- Kaspersky Products Removal: http://support.kaspersky.com/faq/?qid=208279463
  NOTE: For me, use of this tool caused Microsoft Office 2007 to fail on 6-4-2012 Backup before running it.
- MBAM - MalwareBytesAntiMalware http://www.malwarebytes.org/mbam-clean.exe
- McAfee Consumer Removal Tool = MCRT: http://service.mcafee.com/FAQDocument.aspx?id=TS100507 or http://download.mcafee.com/products/licensed/cust_support_patches/MCPR.exe
- Microsoft MSI cleanup utility: http://support.microsoft.com/kb/290301.
- Microsoft OneCare Cleanup Tool (including MSE): http:// http://go.microsoft.com/fwlink/?linkid=81699
- Norton Removal Tool = NRT: After removing all Norton Products from Add/Remove Programs, download and run the NRT. http://service1.symantec.com/Support/tsgeninfo.nsf/docid/2005033108162039
  Note: If you are unable to remove Norton because you need a password, download the "Cleanwipe" Utility. Use caution.
- SUPERAntispyware: http://www.superantispyware.com/downloads/SASUNINST.EXE
- Threatfire Removal tool: YOU MUST COPY AND PASTE THIS LINK. Do not click it:
  http://www.threatfire.com/files/RemoveThreatFire(3.0).zip
- Trend Micro or PC-cillin: Don't miss all the links at the end of the following webpage:
  http://esupport.trendmicro.com/Pages/How-do-I-remove-old-or-new-versions-of-Trend-Micro-products-in-my-comp.aspx
  Also see PCCTool.exe at: http://esupport.trendmicro.com/9/Uninstalling-Trend-Micro-PC-cillin-Internet-Security-2007.aspx
- If you do not find the tool you need here, try this site:
  Http://answers.microsoft.com/en-us/protect/forum/protect_start/list-of-anti-malware-program-cleanupuninstall/407bf6da-c05d-4546-8788-0aa4c25a1f91
- If you still do not find the tools you need, try this site:
  http://www.askvg.com/ultimate-collection-of-uninstallers-removal-tools-for-all-popular-anti-virus-software/

HIJACKTHIS (overview)

- HijackThis is a Utility that scans your PC and creates a report listing important information about settings and processes running in your computer.

- Experts are available in online Forums to help you interpret & analyze the report. Hopefully they can help you find & remove the malware in your computer.
- This is the last resort before formatting your hard-drive and re-installing Windows from scratch. It is assumed that all you have tried all other Utilities to remove the malware.
- Removing malware this way is very complex and should only be done on advice from knowledgable people.
- If you Google "HijackThis", you will find many, many resources to help you.
- Trend Micro bought this Utility in 2007 and continues to make it available for free, but they do not help you analyze the results of a scan or guide you on what action to take.
- The Trend site does give instructions on downloading and using HijackThis. *See the section above on "Virus, Spyware & Rootkit Tools" for the link to trendsecure.*
- After creating your Report/Log, go to: http://www.hijackthis.de/ , then copy/paste the log into the box and click Analyze. It will tell you what Files and Reg entries are bad.
- If you are still stuck, Google: "hijackthis forum" (no quotes) to find people to help you. Log into some of the forums that turn up and ask for help. Here are a few example Forum sites: http://www.bleepingcomputer.com/ or http://www.castlecops.com/ or http://help.lockergnome.com/general/HijackThis-Logs-forum-48.html or http://hjt.networktechs.com/

HOW TO REMOVE MALWARE FROM YOUR PC

This is not for the faint of heart and should be done by an experienced technician. See the separate sheet “HOW TO REMOVE MALWARE FROM YOUR PC” for a "step by step" guide.

HOW TO REMOVE JUNKWARE FROM YOUR PC

This is not for the faint of heart and should be done by an experienced technician. See the separate sheet “HOW TO REMOVE JUNKWARE FROM YOUR PC” for a "step by step" guide.