HOW TO CLEAN AN INFECTED COMPUTER....(REVISED 30/08/08)

Posted by: **rdsok - Moderator** (IP Logged)
Date: March 15, 2005 05:56PM

How To Clean An Infected Computer....(Revised 30/08/08)

by Randy D. Stafford
November 26, 2004
Revised August 30, 2008

Cleaning an infected computer today has become harder than ever. To effectively clean your system you must first learn a little about what you are trying to get rid of and what tools you need to get the job done. I'm going to try to give you some of the background, followed by the basics of getting rid of these pests.

Today there are a variety of things that can infect your computer such as viruses, worms, trojans and spyware. I refer to all of them as malware since that word seems to best describe them and covers both viral and spyware related issues. I find it best to use a multi-pronged approach to fighting malware, so I use several software programs to find and get rid of them. Hopefully, by giving you a little of the background, you will be able to learn what tools to use and when to use them so that you may clean your computer of the malware you may encounter.

Viruses were the first computer bugs, and anti-virus (AV) software was made specifically to detect and get rid of these. Worms are a little different than viruses, which is one reason why AV software has had a harder time catching them. Next came trojan horses, usually just called trojans. These are very different than both viruses and worms. They actually take advantage of the weaknesses that are inherent in AV software. For one, most trojans actually try to hide from being detected by AV software. They also work "smarter" by creating hidden copies of themselves so that when they do get detected and cleaned, they can re-infect the computer with the hidden copy right after the AV software cleans the original infection. Basically, trojans are AV software's worst nightmare simply because AV software wasn't designed to specifically go after this type of threat. Today, AV software is much better at detecting all types of malware. With the release of AVG 8.x.xxx... it now combines both an antivirus with an antispyware scan to help users fight both viral and spyware related issues.

Spyware isn't a new breed of malware. It is simply a combination of various computer exploits and they utilize various combinations of scripts, trojans and worms. Currently they take advantage of trojans the most since they are harder to detect and clean properly. Anti-spyware (AS) software was created specifically for detecting and cleaning this type of malware, so when it comes to trojans and some worms, AS or a combined AV/AS software is much better equipped to fight these than the AV only types of software such as the earlier versions of AVG.

A new varient of spyware is the Rogue type of malware software. This type of software pretends to be useful utils like antispyware, antivirus, hard drive and/or registry cleaning utilities but really their only goal is to sell you their useless software or to install other spyware onto your system. They do this by falsely stating you are infected by something or have other issues that could affect the performance of your system. They usually are installed using the "drive by installation" method that happens when you may visit various malicious websites, often installing without your knowledge.

There is also another type of detection that AVG and most good AS softwares will detect and they are only detected because of their potential security risk if a user was unaware of their existance. AVG calls this type of software Potentially Unwanted Programs (PUPs)... others may refer to them as hacktools, riskware, or simply "not-a-virus". These are normally very useful utilities.. but since they can also be used for harm, AVG and other utils will detect them so the user is aware of their existance. Examples of these are utilities to recover forgotten passwords, forgotten software keys (like the Windows install key), IP scanners, remote control software and a variety of similar utils. If you have any of these installed or on your system, you will want to exclude them from detection with whichever utility you are scanning for malware with... or at the very least do not have them removed when you are cleaning the system up. Remember that these are not malware and do not do damage to your system BUT if you are unaware of their existance, it could be a sign that a hacker may have placed them on your system to do harm. A quick rule of thumb, if you are aware of their existance leave them on your system... if not quarantine them and check out what they really are later.

I suppose I should also cover one last subject before moving on to the cleanup steps... Tracking Cookies. AVG as well as most antispyware utils do detect these and each has a specific but different list of the ones they will find. These ARE NOT MALWARE.. they can do no harm or damage to your system. They do however represent a potential invasion of your privacy since they can be used to track your internet browsing habits. So unless you have setup your browser to block them or use a specialized utility to do that... you will always find these detected. So do not be alarmed by their presence.. clear them if you want (I always clear mine)... but also understand that they will likely return the next time you happen to visit a website that may use them.

First, you will need to get some software programs to help you. The following programs are what I use personally. Not only do I trust them, but they are also free for personal use. The companies that provide the free software, also provide software that they sell for use in a commercial environment. Usually, the free versions are just as good but simply don't have as many of the extra features which make the commercial versions even more attractive to use.

Anti-Spyware Software

For Windows 2000, Windows NT, Windows XP & Vista only

- **MalwareByte's Anti-Malware** - You can find it at [www.malwarebytes.org]

Anti-Virus Software

For Windows 2000, Windows XP (inc. 64bit version) & Vista (inc. 64bit version)

• **AVG Technologies Free Edition** - You can find it at [free.grisoft.com] - English version, [gratis.avg.it] - Italian version, [free.avg.de] - German version, [gratuit.avg.fr] - French version, [free.avg.com] - Japanese version, [free.avg.com] - Brazilian Portuguese version, [free.avg.com] - Dutch version, [free.avg.com] - Latin America Spanish version & [free.avg.com] - Polish version

First you will want to download each of the above programs and then install them. After you install them, you **MUST** update them so you will have the latest protection. If you don't update these programs and you are infected with the latest parasites, you will not be able to effectively detect and clean them from your computer, so remember to update, update, update. Most if not all of the definition files for these utils are now updated daily.

Now that you have downloaded, installed and updated all of the above utils... Print this article so you can refer to it later and disconnect your computer from the internet. This is an important step and will remove one way that a malware may use to re-infect your computer.

With the release of AVG 8.x now combining both antivirus and antispyware into one product, I have now switched from scanning with it last, to scanning with it first since it now detects more malware than any of the others. I also use the different AS software packages in a specific order so that I go after the tougher problems first and the easiest ones last.

Turn off System Restore

• WinME and WinXP have a cool feature called System Restore. It is used to restore your computer to an earlier configuration in case of a problem. The only problem is that it wasn't made with malware in mind, and often it can't tell the difference between an infected file and a good file, so it can as easily restore an infected file if it had been in a protected area, effectively re-infecting your computer right after you have cleaned it. Because of this, it is recommended to turn off System Restore before you test, and when you're done, turn it back on so you are still protected from standard computer problems.

• For WindowsME

Click Start, Settings, and then click Control Panel.
Double-click the System icon. The System Properties dialog box appears.

NOTE: If the System icon is not visible, click "View all Control Panel options" to display it.

Click the Performance tab, and then click File System.
Click the Troubleshooting tab, and then check Disable System Restore.
Click OK. Click Yes, when you are prompted to restart Windows.

• For WindowsXP

Click Start.
Right-click the My Computer icon, and then click Properties.
Click the System Restore tab.
Check "Turn off System Restore" or "Turn off System Restore on all drives."
Click Apply.
When turning off System Restore, the existing restore points will be deleted. Click Yes to do this.
Click OK.

• For Win Vista

1. Open System by clicking the Start button , clicking Control Panel, clicking System and Maintenance, and then clicking System.
2. In the left pane, click System Protection. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. To turn on System Protection for a hard disk, select the check box next to the disk, and then click OK.

Carefully Look at Windows Add/Remove programs for suspicious programs

• Many of the spyware threats actually install into your system just like a regular program. Many may appear to be utilities that you may think are helpful but in reality aren't. Look for add-an toolbars, while toolbars like those provided by Google, MSN, Yahoo and other are great utils, there are many more that aren't and if in doubt check it out to see if ones you have are parasitic. Another common exploit are the Search helpers, WinTools, Gator products, IE Helper, Comet Cursor and many others just to name a very few. Peer-to-Peer (P2P) programs are another common source for these and even the ones that doesn't come with spyware themselves are a high security risk that may lead to your system being infected or to spread infections like these. Remove all suspicious programs, if you accidentaly remove the wrong item, you may always re-install them later.

Run Disk Clean-Up

• This actually comes with Windows and has been installed by default since Windows 98. You can find it by clicking the Start Button and then going to Programs / Accessories / System Tools / Disk Clean-up. I recommend selecting all of its options except the ones for Office Setup Files and Compress Old Files if you have them. While you may select those if you wish, they aren't as important. This will clean up all of the temporary files so your testing will go faster, and may also delete any spyware that may hiding there if the spyware isn't already running. To clear systems that have System Restore you will need to select the second tab and click the button for clearing this.

Run AVG 9.x.xxx

- Most antivirus programs, including AVG, by default have their settings to only scan executable files in an attempt to speed up looking for infections. While most of the time this is just fine, the newest threats that can infect your computer have started getting sneaky on how they hide their files making it easier for them to reinfect your system if your antivirus program detected and removed their executable file. To help also detect these "backup" files that the infection leaves on your system, you should in my opinion, make a couple of changes to what your AVG scans during these tests from just executable files to all files.

- To change AVG's settings during a scan, open AVG's User Interface.
Click the **Computer scanner** tab, then under the **Scan whole computer** area, select **Change scan settings**. Unselect **Scan infectable files only** and select all other checkmarks with the **Automatically heal/remove infections** and **Scan for Tracking Cookies** as options I'll let you decide if you want enabled or not.

- Now AVG will scan all of the files when you scan your computer. This will take longer to complete, but I feel it is a small price to pay for the added security it provides.

Run MalwareByte's Anti-Malware

- Select to perform a Full Scan and then click the Scan button. This is another specialized util that not only targets Rogue spyware but other malware as well. This currently targets malware and rogues from 931+ vendors (the malware authors). The malware that is targeted in this category is very actively being updated by their authors because of the potential they have for making money. As with all antispyware utils, update this often and before each use to help give you the edge in fighting these malware.

When you believe you are finished, remember to turn System Restore back on if you had turned it off.

I recommend testing for parasites as often as you can, probably at least once a month if not more. The sooner you catch them, the less damage they can do to your computer, and the less chance of a hacker finding your sensitive information such as checking account info, passwords, etc.

Windows Tip

Windows itself, by default, hides certain files, system folders or file extentions from the user to make it easier to navigate. If you are having to find an infected file or just one you are looking for, this can cause you to not find it. If you wish you may change this to show all of the files on your computer.

Open your **My Computer** icon (Either from your desktop or the Start Menu)
Click the **Tools** menu and select **Folder Options**(on older systems it may be in the View menu)
Select the **View** tab and scroll through the **Advanced settings**
Enable or disable the following (using a checkmark to enable)

enable - Show hidden files and folders
disable - Hide extentions for known file types
disable - Hide protected operating system files (WinME and WinXP only)

Now click **Apply** and **Ok**

For Win Vista info. see this link [www.howtogeek.com].

How to find an embedded infection

AVG 9 Free detects infections in areas that it was unable to before. The most notable are ones embedded inside of archives. Since AVG can't determine if you created the archive or if it was a parasite that created it, they leave these alone so you may have a chance to recover uninfected files from the archive and then you simply delete the archive when done. Infections that are inside of an archive aren't a direct threat to your system unless the file gets extracted to allow it to run. Grisoft has chose this method because it is safer for your data that the archive may contain.

For someone that is new to looking for these embedded infections, it can be a little confusing with the way that AVG will list the file because it also must include the archive file name that contains it in the full path/filename. The following is an example that I made up to highlight the info so you will know which filename to look for so you may either extract files and or delete the correct file. I will color code these for you, but AVG will not.

AVG will give you a name like...

C:\Windows\Temp\InfectedArchive.cab:\InfectedFile.exe

The location of the file is in C:\Windows\Temp
The archive that contains the infection is InfectedArchive.cab
And the actual infected file inside of the archive is InfectedFile.exe

Note the ":\" that seperates the archive from the file it contains.
After you have recovered any files inside of the archive that you may want to keep (other than the infected one that is) just simple delete the whole archive.. in this example the file to delete would be InfectedArchive.cab

It looks harder than it really is.. just remember the file you want to look for is named just before the last ":\"

Most of the time, you won't have any files to recover inside of the archives. The only time this isn't true is if it is an archive that you had created yourself. If you didn't create it.. just delete and move on.

Edited 113 times. Last edit at 02/04/09 02:36AM by BIG AL 43.