

## HOW TO CLEAN AN INFECTED COMPUTER

Posted by: [rdsok](#) - Moderator (IP Logged)

Date: March 15, 2005 05:56PM

### How To Clean An Infected Computer

by Randy D. Stafford  
November 26, 2004

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 parasites since that word seems to best describe them. I find it best to use a multi-pronged approach to fighting parasites, 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 these parasites.

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 a harder time catching them. Finally 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 parasites than before but they will need to be redesigned and start using multiple methods if they are ever going to be effective against all parasites.

Spyware isn't a new breed of parasite. 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 parasite, so when it comes to trojans and some worms, AS software is much better equipped to fight these than the AV software is.

A new variant 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.

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 98 & later (CWS - Windows 98SE & later - Vista?)

- **CWS**hredder - You can find it at [\[www.trendmicro.com\]](http://www.trendmicro.com) Latest version is v2.19
- **Spybot S&D** - You can find it at [\[www.spybot.info\]](http://www.spybot.info) Latest version is v1.5

##### For Windows 2000, Windows XP ( inc. 64bit version ) only

- **Lavasoft's Ad-Aware** - You can find it at [\[www.lavasoftusa.com\]](http://www.lavasoftusa.com) Latest version is v2007 7.0.1.6

**Note :- Ad-Aware Personal 1.06r1 to suit earlier Windows versions is still available thro' Google search.**

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

- **RogueRemover** - You can find it at [\[www.malwarebytes.org\]](http://www.malwarebytes.org) Latest version is v1.22

##### For Windows 2000, Windows XP & Vista ( inc. 64bit versions ) only

- **AVG AntiSpyware** - You can find it at [\[free.grisoft.com\]](http://free.grisoft.com) / [\[www.ewido.net\]](http://www.ewido.net) Latest version is v7.5.1.43

#### Anti-Virus Software

##### For Windows 98 & later

- **Grisoft AVG Free** - You can find it at [\[free.grisoft.com\]](http://free.grisoft.com) Latest version is v7.5.503

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. There is one small exception: CWSredder is a stand-alone program that doesn't need to be installed, but you do need to have it check for an update to ensure that you have the latest version. 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. Spybot S&D

/ Lavasoft's Ad-Aware detections are usually updated at least once a week whereas AVG AV can be daily.

Since spyware is a bigger problem today than viruses, and spyware is typically harder to find and get rid of, I suggest to start looking for spyware first. 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 parasites in mind, and often it can't tell the difference between an infected file and a good file, so it might automatically restore an infected file also if it had been in a protected area, effectively re-infecting your computer. 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.

### **Carefully Look at Windows Add/Remove programs for suspicious programs**

- Many of the spyware threats actually install into your system like a program. Many appear to be utilities that you may think are helpful but in reality aren't. Look for add-on 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 don't come with spyware themselves are a security risk that may lead to your system being infected or to spread infections like these. Remove all suspicious programs, if you are wrong, 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 be 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 CWS shredder**

- This specialized util is made for detecting and cleaning of the infamous CoolWebSearch exploits. Currently there are about 40 types of these, each with up to 4 variants and growing. These are some of the toughest ones to get rid of and while they aren't seen as often as they used to be, this is still a good place to start.

### **Run RogueRemover**

- This is another specialized util that targets Rogue spyware. This currently targets about 360+ rogue applications and counting. 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 antispysware utils, update this before each use to help give you the edge in fighting these malware.

**Run Ad-Aware Next *Windows 2000 and newer use v2007, for older versions of Windows use v1.06r1.***  
***See Note above...***

- This handles the next types that weren't covered by the specialized utils earlier. When it finally presents you with the list of parasites it has found, put a check mark in the box next to the ones you want to get rid of, I suggest checking them all. If you want to select all, just right-click your mouse on the boxes to get the options menu, and left-click on Select All. If it says it can't get rid of a problem right now, it will ask if you want to run it again after you restart your computer, answer yes and restart your computer so it may test again.

### **Run Spybot Next**

- When you run it, it will automatically select all the spyware that it finds, if there is something you don't want to get rid of for some reason, deselect it and then let Spybot fix all of the rest of the problems that it finds. This program

also will ask to restart your computer so it can test again if it has problems removing something, so let it.

If you had Windows 2000, Windows XP & Vista ( inc. 64bit versions ) you also have this option...

### Run AVG AntiSpyware Next

- This is a part of a new breed of antispysware utils and probably one of the best I've worked with. The only down side is that only certain versions of Windows can run it at this time. When you run it, it will prompt you to select to remove or keep each item or you can select to have it remove all that it finds.

### Now Run The AVG Program

- All 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 from just executable files to all files.

- To change AVG's settings, open AVG's Test Center.

Click the Tests menu then in both of the tests labelled **Complete Test Settings** and **Selected Area Test Settings** select **Scan all Files** and click the Ok button.

- 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.

- Have it scan for the remaining parasites that the others may have missed. If you found any parasites, you need to restart your computer so you can test everything again. There are times that after cleaning certain parasites, you will need to test again because something may have been hidden earlier by the infection. So **repeat this process** of testing and restarting until you find no more parasites.

- Run the scans again in Safe Mode. This will keep many of the parasites from loading and being able to hide from your protection software. To access Safe Mode on most versions of Windows, start tapping the [F8] key after you first start or restart your system, start tapping it before you ever see a Windows Splash Screen and continue until you get the Menu where you may select it from the list. On WinNT, this is called VGA mode and on Win2k you actually start tapping just after the first splash screen shows. For Detailed instructions see [Restarting Your Computer in Safe Mode](#)

These procedures should have cleaned most cases of infection that you will find. Yes I said MOST because there are some infections that are very hard to detect and remove. Generally, if you have one of these, you will need the assistance of an expert to help you get rid of it.

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 extensions 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 extensions for known file types

disable - Hide protected operating system files (WinME and WinXP only)

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

### How to find an embedded infection

AVG 7 Free now 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 separates 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.