PenguinBlog.com

NOTE: You may have gotten here via a mirror, but you should bookmark the page HERE.

Please visit my Blog for more useful tech info.

I'm an IT Tech with my own computer consultation business. I'm also a moderator at PC Abusers Forums and answer a lot of technical questions there (my forum nick is FlyingPenguin). PCAbusers is a great place to post technical questions. There's a nice bunch of people there who are happy and eager to help.

FLYING PENGUIN'S D.I.Y. SPYWARE/MALWARE REMOVAL

Updated 4/06/10: Added ComboFix which seems to be the only anti-spyware scanner that reliably removes many of the worst rogueware/fakeware trojans.

I first posted this page in 2005 and since then we've seen the emergence of organized crime-grade trojans which are nearly undetectable and un-removable. People no longer infect your computer for fun, it's now for profit... BIG profit. Organized crime reportedly makes billions (yes BILLIONS with a "B") from spyware trojans every year.

Modern malware is designed to steal your personal information to be used for identity theft, steal you user account logins, and turn your computer into a member of large "Botnet" networks of hundreds of thousands of computers controlled by organized crime syndicates and used primarily for sending SPAM and launching Denial of Service attacks.

This Spyware removal procedure will remove most of your run-of-the-mill spyware,

adware, fakeware and malware but may not work on the really hardcore organized crime-grade trojans. Honestly, there's really no hope if you have a seriously hardcore trojan on your system. REMEMBER, once your system is compromised there is NO WAY to be certain if it's ever clean again unless you wipe the drive.

If you suspect your system is still compromised after performing this procedure, I strongly recommend you backup your data (and scan that data with a virus scanner on an uncompromised computer), do a security erase of the hard drive using DBAN (single pass is enough) to eliminate any boot sector trojans (these are rare but they DO exist), and perform a clean install of your operating system. If that is too technical for you, go find a mom & pop computer store. Stay away from major retail stores. TRUST me, the office supply store has no clue how to remove a trojan, no matter what they say. They sell staplers and paperclips.

FAIR WARNING:

These instructions assume you're at least some-what technically inclined concerning Windows (you should know how to boot into safe mode, do file searches, how to make a system restore point, be familiar with altering the registry). If you feel any of this is over your head, I strongly urge you to take your computer to a professional.

I in no way take any responsibility for any harm caused to your operating system if you follow these instructions. Removal of spyware and viruses can be VERY tricky, and you could possibly render the operating system unbootable, requiring a re-install of Windows and possibly losing all data on the hard drive. PROCEED AT YOUR OWN RISK! Make sure to backup any important data before proceeding.

REMOVAL PROCEDURE:

1) Make a Restore Point if you can, or make sure a restore point was made recently. There are MANY ways that attempting to remove malware can trash your operating system so before doing ANYTHING, make a System Restore point using Windows System Restore. If something goes wrong, you can at least put things back the way they were when you started.

NOTE: Some of my colleagues recommend disabling System Restore (thereby nuking all the restore point files) BEFORE you start performing a spyware removal because spyware can hide backup copies in there. While that's true, I still think there's more benefit in using System Restore than nuking it. It's easy to damage the registry, your TCP/IP stack or something else while performing a spyware removal, and you want to be able to use System Restore to put the OS back the way it was before you started - especially the registry - if something goes terribly wrong (yes, it'll still be infected, but at least functional like it was before). Then you can try to clean it again. Modern spyware scanners can find and remove malware inside the System Restore folders just fine nowadays anyway. However at the END of my procedure, once you've removed the malware, I do recommend you nuke the system restore points.

It also wouldn't hurt to make an image of your boot drive using Norton Ghost, Acronis True Image, Drive Snapshot, or some other drive imaging software and save it to an external hard drive. System Restore is not perfect, but a drive imaging program takes a complete "snapshot" of your hard drive and thus you can always put things back exactly as they were before you started.

I also like to backup the entire registry before doing anything. I like to use ERUNT: http://www.majorgeeks.com/download1267.html

2) UNINSTALL your Anti-Virus. Yes uninstall it and you can re-install it later when you're done. Your AV program will only interfere with the spyware scanners you're going to run, and it will also slow them down dramatically. Some of these scanners you're going to run act as rootkits themselves (a necessity in order to remove malicious rootkits) and if your AV app is running it's going to go nuts and block it.

Also, if your system is badly infected then most likely your anti-virus is compromised anyway and you should re-install it once your system is clean.

If it's not possible to uninstall your AV app (because Add/Remove programs is not working properly for instance), then you need to at least disable it. Open your AV program's main window and and find a setting to disable "Background" or "Realtime" or "Resident" virus scanning. In AVG you double-click on the "Resident Shield" icon and uncheck "Resident Shield Active". In Norton and McAfee you usually have to go into the Advanced settings and disable real-time scanning. Avira Antivir lets you right click on the Avira icon in the taskbar and disable it. If you're asked how long to disable it for, choose "permanently" or the longest possible option. You can turn it back on later.

3) Download and run HostsXpert: http://www.majorgeeks.com/Hoster_d4626.html
Unzip it to a folder on your hard drive, open that folder and double click on the "HostsXpert.exe" executable. Click the "Restore MS HOSTS File" button and then click on the "Make ReadOnly" button. Close the program.

NOTE: You can skip step 4 if you feel this is too technical for you and proceed directly to step 5. The spyware removal utilities you'll run after step 4 will probably do the job just fine, but if possible it's nice to give them a head start by using HiJackThis to get rid of the crap that's running in the background first.

4) Download the latest version of HiJackThis: http://www.majorgeeks.com/Trend_Micro_HijackThis_d5554.html

Run HijackThis with the default setting. When it finishes it will generate a text file and open it in Notepad. Copy all the text in the notepad file and paste the into the HijackThis Online Analyzer located here: http://www.hijackthis.de/en. Then click on the "Analyze" button at the bottom of the page.

NOTE: This website is sometimes VERY slow to respond - especially in the morning - due to heavy use. Also it may tell you that it's too busy and to try again later.

Scrutinize anything that the analyzer thinks is suspicious. The analyzer is NOT perfect though. There are lots of things that will trigger a yellow caution or even a red X that's legit. You can usually ignore any green checkmarks with a warning that the file is in the wrong location. Anything with a red X should be looked at carefully though. It's up to you to decide if an entry is legit or not. Read the description and filename carefully. If you don't know what it is then delete it. Make sure you don't delete something that's required by your printer or scanner (most HP printer files and services start with the letter HP for instance). You can always type the name of the file or service into Google to find more detailed information on it.

Place a checkmark next to any item you want to remove and click the "Fix Checked" button.

I recommend removing ALL BHO's except Acrobat, the Java Helper and the Google toolbar. Most people don't need any other BHOs and a lot of malware is found in Toolbar BHOs (if you use the Firefox browser instead of IE, which you should, then you don't need ANY BHOs - BHOs are unique to Internet Explorer).

HijackThis saves a backup of any registry entries it deletes in a folder in the HiJackThis folder.

5) Download the following programs:

- ComboFix: http://www.bleepingcomputer.com/combofix/how-to-use-combofix. Save this file somewhere you can find it, like the desktop. You will run it later.

- Trojan Remover 30 day trial: http://www.simplysup.com/tremover/download.html When prompted after the install, allow it to check for and install database updates.

- Malewarebytes Anti-Malware Free Edition: http://www.malwarebytes.org/mbam.php
  When prompted, allow it to download and install the latest definition updates.

- Microsoft Malicious Software Removal Tool (MSRT): http://www.microsoft.com/security/malwareremove/default.mspx

There are no updates required for this program.

6) Reboot the computer into **Safe Mode with Networking** (if you don't know how to get into Safe Mode then you shouldn't be attempting this). We're going to run all our spyware scanners in Safe Mode because there's a better chance of them succeeding. If you can't get into Safe Mode it's okay, then run it in Normal Mode. Some malware will prevent you from booting into Safe Mode. However it would be much better if you can run in safe mode.

NOTE: The reason we're booting into "Safe Mode with Networking" is so we'll have access to the Internet. Combofix requires Internet access to work. You need to be connected to a network directly via a network cable (Wifi doesn't work in Safe Mode).

7a) Run ComboFix. ComboFix should run immediately. If nothing happens for a minute or two then the trojan on your system is preventing ComboFix from running which is not uncommon. The trojan in the rogueware app "Personal AntiVirus" does this for instance. The way to get around this is to rename the COMBOFIX.EXE installer file to FIX.COM and then run it. You also have a better chance of running it from Safe Mode.

ComboFix will ask for permission to install the Windows Recovery Console. Go ahead and allow it. Basically follow the instructions it gives you and allow it to do whatever it wants. Go get a beer. Combo Fix can take anywhere from 30 - 60 minutes depending on the speed of your computer, and how badly it's infected. ComboFix will reboot your PC at least once during the process.

NOTE: ComboFix must have Internet access in order to work. If you do not have internet access because the trojan is blocking the Internet, then skip to the next step.

7a) Run Trojan Remover, click the Continue button, and then click the Scan button. Let it nuke anything it finds. This will only take a few minutes. Close the program when it's done.

7b) Run the Microsoft Malicious Software Removal Tool (MSRT). Select the Quick Scan option. Go have a beer. This program could take anywhere from 15 - 60 minutes to scan your drive.

8) Run Malwarebytes AntiMalware. Click the Scan button (the default Quick Scan is fine for now. You can run the much slower full scan later if you want to).

Go have another beer or two and watch some TV. This could take anywhere from 10 minutes to 2 hours depending on the speed of your system and the size of the drive.

When it's finished, let it nuke anything it finds.

9) Reboot the computer and turn your Anti-Virus program back on, or re-install it if you removed it in step 2.

10) Try browsing the Internet. Don't just go to your homepage. Browse to CNN.COM and click on some news stories. Make sure Internet access is working and you're not just loading cached pages.

Certain spyware trojans alter your TCP/IP stack and it's possible that when a spyware scanner removes the trojan, it may damage your TCP/IP stack and render your computer incapable of accessing the Internet. There's a utility called WinsockXPFix.exe that can repair it (this fix is ONLY for Windows XP). You can get it here: http://www.majorgeeks.com/WinSock_XP_Fix_d4372.html DO NOT run this fix unless you can't browse the Internet after removing spyware.

11) Once you're finished and you're ABSOLUTELY CERTAIN you won't need to go back to an earlier restore point, you need to NUKE all your System Restore files. WHY? Because your restore points contain backup copies of all the spyware and trojans you've just labored so hard to remove, so you need to get rid of them.

Just disable System Restore and click Apply. Windows automatically deletes all your restore points. Then enable System Restore and Windows makes one new restore point at that moment.

Instructions here: http://www.pchell.com/virus/systemrestore.shtml

12) OPTIONAL:

-Uninstall TrojanRemover. It expires after 30 days anyway. If you uninstall it now then it won't expire the next time you need it. Trojan Remover also runs a scan every time you boot (FASTSCAN) which can be annoying, although it can be disabled from the menu.

- Delete the contents of the IE browser cache and the temp folder. A simple way to do this is to use CCLeaner. It also wouldn't hurt to run the registry cleaner in CCLeaner: http://majorgeeks.com/download4191.html

- Defrag your hard drive. We've deleted a lot of files during this procedure, leaving holes that have fragmented the drive.

- If Malwarebytes found a LOT of malware, then it wouldn't be a bad idea to download and run a scan with **SuperAntiSpyware** free Edition as a followup. SAS often detects a few stray registry entries that Malwarebytes misses, and it

also removes bad cookies. You'll want to uninstall it when you're done or disable it from running in the background via it's menu. Get it here: http://www.superantispyware.com/download.html

- Another good followup scanner is **Hitman Pro**. It tends to find a few special things that the other scanners miss. You'll want to either uninstall it when you're done, or disable the "Scan Computer Daily at Startup" setting in the settings. Get it here: http://www.surfright.nl/en/hitmanpro

WHAT TO DO AFTERWARDS:

- **Don't rely on your anti-virus program to protect you!** There is always an exposure "window" between the time a new threat is released and the anti-virus vendors release an update for it. You are exposed during that time. Also a lot of spyware and adware is PERFECTLY LEGAL (believe it or not, as long as they follow certain guidelines and you "voluntarily" installed it).

- Follow safe browsing practices. I have a guide posted here courtesy of GetNetWise.org: http://soldcentralfl.com/flyingpenguin/spyware/spyware_help.html

- Be aware that organized crime-grade malware is almost impossible to detect and remove. Even if your system seems to be rid of spyware after this procedure, be wary. Keep an eye out for suspicious activity (large memory usage, network traffic when there shouldn't be, disk access when there shouldn't be, advertising popups when you don't have a web browser open, notices from your ISP that you may have a virus because they've detected SPAM coming from your IP address, etc.)

- Use the Firefox web browser instead of Internet Explorer (IE). Doing this will do more to protect you from malicious infection from websites than anything else. Firefox is a much safer browser than IE because it does not support ActiveX scripting. Firefox will not replace IE and once installed you can use either browser, so try it - there's nothing to lose. It will even import all your favorites, passwords and cookies: http://firefox.com

I also STRONGLY recommend you install the NoScript plugin for Firefox. For ease of use you can set NoScript to allow scripts globally, but even with that setting NoScript automatically blocks cross-site scripting and click-jacking attempts: http://noscript.net/

- If you insist on using Internet Explorer then make sure you're running IE7 or IE8. IE6 is technically obsolete and very insecure.

- Turn off your cable or DSL modem at night when you're not using the PC, if convenient and practical. Remember, if your PC is infected with organized crime-grade malware it may be part of a Botnet, and this is hard to detect. You may think it isn't bothering you if your computer is otherwise running fine, but

your computer may be a member of a network of hundreds of thousands of other computers polluting the Internet with SPAM. You ever wonder where all that junk e-mail comes from? It comes from infected Botnet PCs. Moreover, once a PC is part of a Botnet it's OWNED by someone else. That person controlling the Botnet can make your computer do anything he wants. He can easily monitor everything you type into your computer, or make it download illegal content for him like copyrighted music and child pornography. More information about Botnets here: http://en.wikipedia.org/wiki/Botnet

NOTE: BE CAREFUL where you download the utilities mentioned in this article. There's lots of fakes (also known as Fakeware or Rogueware) out there that may not be what they claim to be! Only download them from the author's homepage, or from a known safe download site.

You can download all the tools I mentioned above from http://MajorGeeks.com which is a secure source I can highly recommend.

BEWARE of sites that have fake, and possibly virus infected versions of these programs!

Feel free to contact me via this contact form.

(352) 750-0845
Toll Free Pager: (888) 210-9108

- By Appointment Only -

24 Hour Emergency Service

Doing business in
Lady Lake since January 2002

Homepage