Published on *Maximum PC* (http://www.maximumpc.com)

Ultimate Malware Removal Guide -- Purge Your PC of Junk Files!
Created *01/29/2009 - 7:00am*
Maximum IT


- Renting Data Centers is the Latest Fad in IT
- IBM Turns Up the Heat in New Data Center to Cut Back Energy Bill
- Trend Micro Invests Millions into Cloud Computing Subsidiary

SEE MORE MAXIMUM IT
News

- AMD to Expand Graphics Business to Mainstream Servers
- Watch The Nexus One Get "Shock" Tested
- Haleron Launches a $149 Mini Tablet, Does This Prove Apple is Overcharging?
- Rumor: Samsung to Debut Transparent Screen Laptop this Year
- eSATA is Still Faster Than USB 3.0

SEE MORE NEWS
How-Tos


# Ultimate Malware Removal Guide -- Purge Your PC of Junk Files!

Posted 01/29/09 at 09:00:00 AM by Josh Kampschmidt

Comments Print Email

Malware is everywhere. You can't browse on any Internet tech forum without someone mentioning this word (with disdain), usually in search of a remedy after being infected with spyware. No matter how careful you are, we're guessing that many of you have had malware inadvertently installed on your system and may have even ended up reformatting your computer as a last resort. While that may have been the most thorough solution, it is in a sense admitting defeat. Or worse yet, you took your computer to get cleaned and was charged anywhere from $50-300 -- a high price for humiliation. But don't fret, because you can actually purge your system of malicious software for free! Just follow our comprehensive guide.

**Time = About 4 hours**

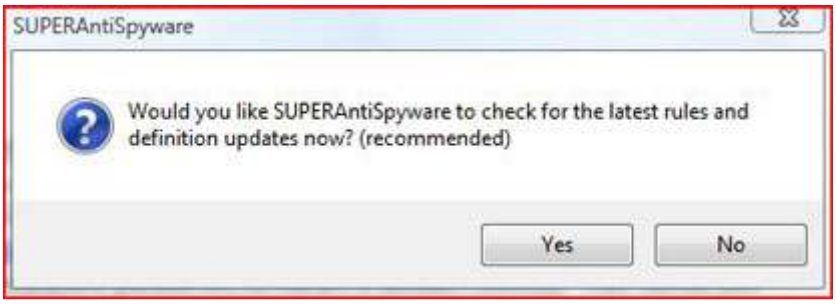
## 1. Scrub your system with SUPERAntiSpyware

### What You Need:

- SUPERAntiSpyware
  Free, http://www.superantispyware.com
- Malwarebytes Anti-Malware
  Free, http://www.download.com
- Combofix
  Free, http://www.combofix.org/
- Panda Activescan 2.0
  Free. http://www.pandasecurity.com
- Pocket Killbox
  Free, http://www.bleepingcomputer.com
- CCleaner
  Free, http://www.ccleaner.com/
- Comodo Registry Cleaner
  Free, http://registry-cleaner.comodo.com

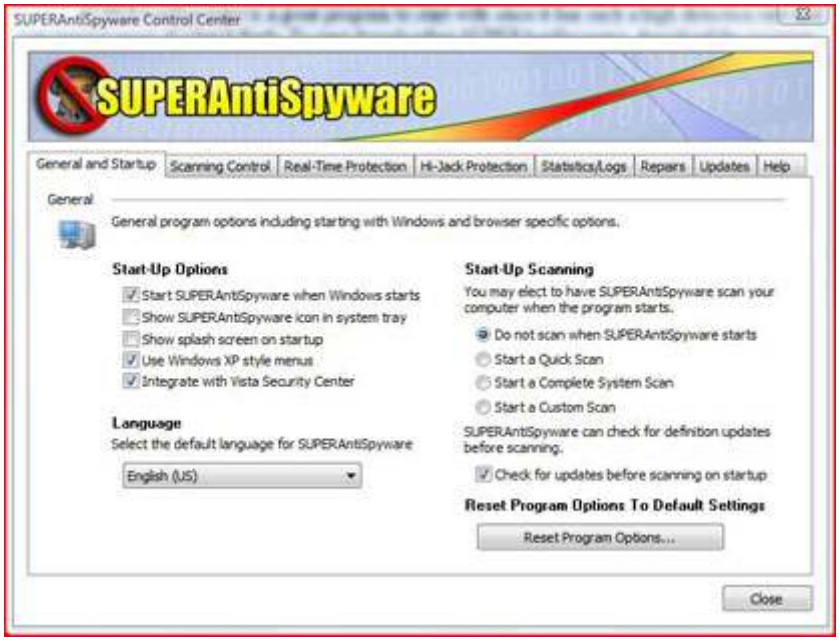
SUPERAntiSpyware is a great program to start with since it has such a high detection rate and can remove most of what it finds. Depending on how infected your computer is, you may want to run this program in Safe Mode.

To start downloading SUPERAntiSpyware, download the program from their official website. Download the file to your Desktop or wherever you choose. Keep all the default installation parameters to ensure it installs correctly. Just click the next button along the installation wizard. Choose your language, English is normally the default. After this screen, a new definitions window will pop up click Yes to download the updates.

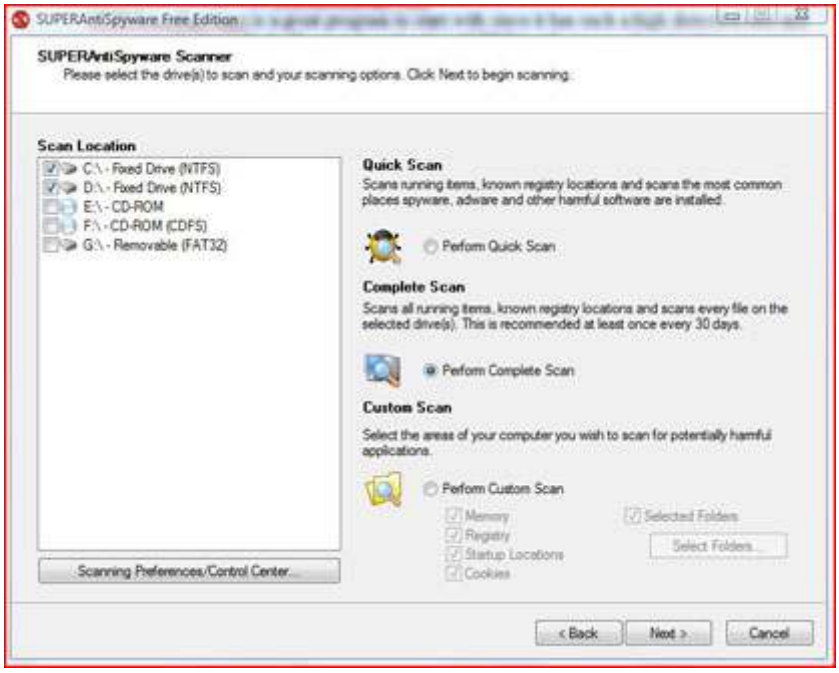



On the initial setup window, click next. You don't need to enter your e-mail address on the next screen since you aren't purchasing this program, but on the screen that asks if you want to automatically check for updates, make sure you leave that box checked. Having the program automatically scan for updates saves you time in the future. Do not send a diagnostic report to the company, so uncheck the box. Eventually you will be presented with a window wanting to protect your homepage.


If it is your homepage, click Protect Home Page, otherwise, don't. When the program opens, click Preferences. Make sure your Preferences matches the following screenshot and select Close.




Click the Scan Your Computer button and then start a Complete System Scan of all your fixed drives. Remove everything that is found.




## 2. Scrub your system with Malwarebytes Anti-Malware

Similar to SUPERAntiSpyware, Malwarebytes Anti-Malware is a great scanning utility with excellent removal capability. You might also need to run this program in Safe Mode.

Download Malwarebytes Anti-Malware from this site. Save the file to your Desktop. Installation is relatively simple, just follow the installation prompts. At the end of the installation, you will be presented with a Finish window. Uncheck Launch Malwarebytes Anti-Malware.

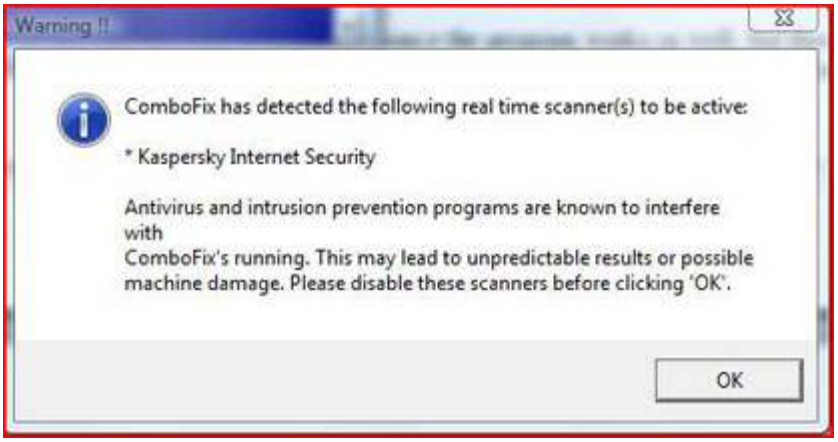
The program will update and not launch until you request it to do so. Launching the program directly after the update could temporarily crash the program because of the malware present on the system. Double-click the Malwarebytes Anti-Malware icon on your Desktop. Set the program to do a full scan and press the Scan button. Malwarebytes Anti-Malware may look like it froze, but do not do anything, just let it scan.


---

## 3. Combofix the malware

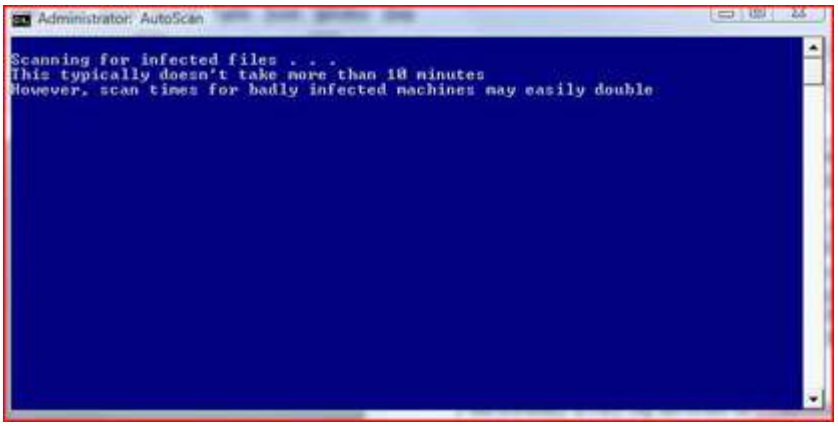
We are normally a very big advocates of Combofix since the program works so well, but there is a possibility that the program can cause damage to your computer. Download Combofix from the following link and save it to your Desktop.

You may be requested to update the program when you open Combofix, please do so. After the update, the program will restart. Don't restart the program yourself. On the next start you may get a warning if you have active security software on your system <insert Combofix_Warning.jpg> disable your antivirus or other security protection since it may interfere with Combofix.



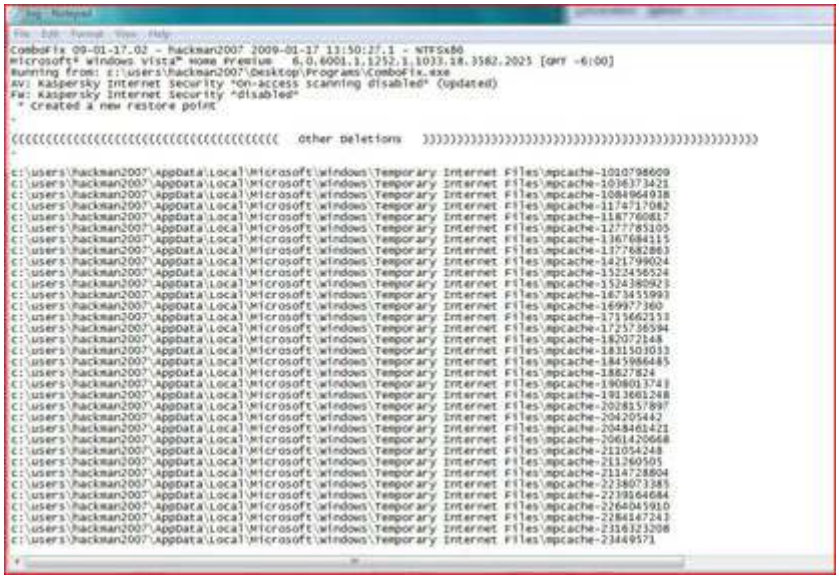

You will get an EULA pop-up from Combofix. This EULA explains the basic terms and conditions of using the program. Make sure you read this and understand the terms and conditions.

Combofix will now create a system restore point and start scanning, don't move the program window. Your taskbar may disappear several times as it goes through the various stages and you may lose network connectivity temporarily. If it asks if you want to clean the registry, please allow it to do so.




The program will try to generate a logfile. Do not move or close the window.

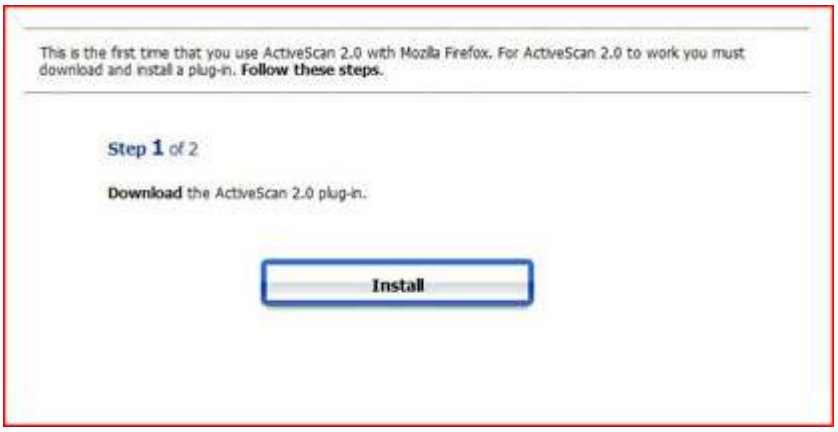
After the reboot, if necessary, a logfile will have opened automatically on your screen. Please close the logfile. Altering any files that Combofix displays could cause serious, irreversible damage to your system if you don't know what you are doing.



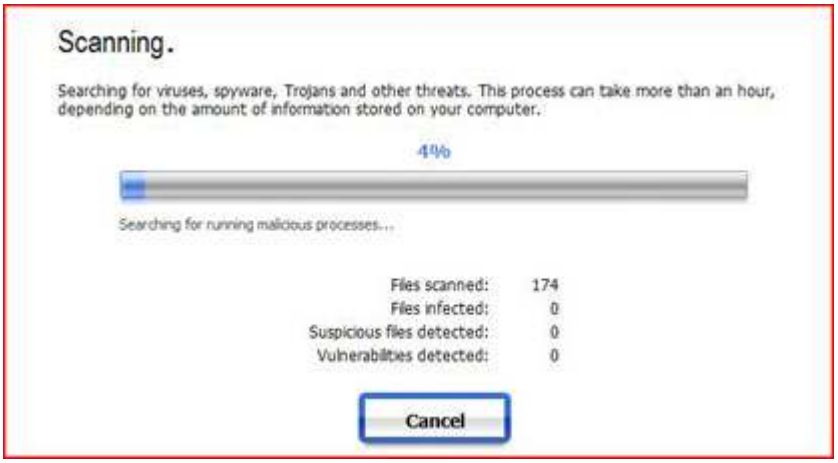

## 4. Get a second opinion with Panda Activescan 2.0

Panda Activescan 2.0 is a general malware scanner, but runs through a web browser instead of natively on your hard drive. It has a good detection rate, but does not remove the malware it finds, so you will have to do this yourself. This scanner is primarily used with Internet Explorer, but also works with Firefox.

To start scanning with Panda Activescan 2.0, go to their official site. Click the big Scan Now button. If you are using Mozilla Firefox, you need to download the appropriate plug-in to run the scanner.




Let the program update and install temporary files to your computer. The temporary files allow Panda to scan your computer's hard drive. Panda should start automatically scanning your computer's physical hard drives.



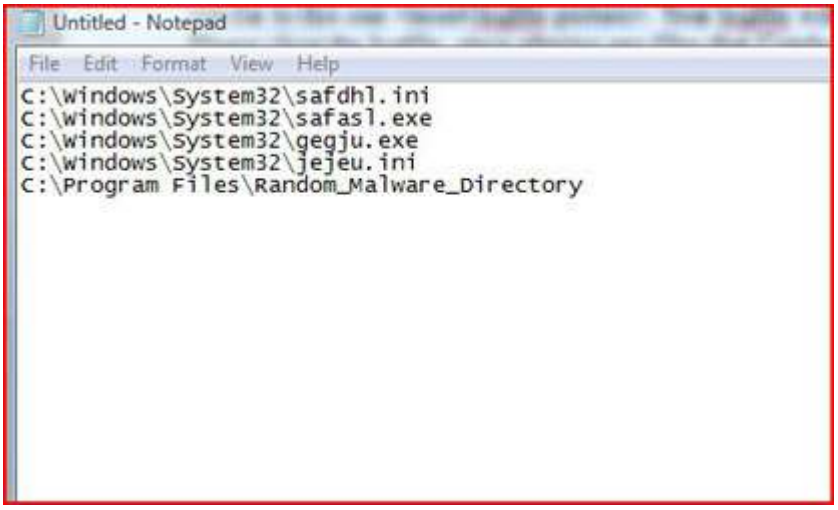

If malware is detected, it will alert you and allow you to see a logfile. Save this logfile, you will need it later. You can close Panda Activescan 2.0 after you save the logfile.

## 5. Delete files with Pocket Killbox

In order to get these malware files off of your computer, you need to delete them yourself. Since Panda is a pay program, it won't be able to remove these for free.

Open the Panda Activescan 2.0 logfile. Locate the full pathway. A pathway looks similar to C:\Windows\System32\sdfhl.exe. Copy and paste that entire line starting with the "C:" from your logfile and paste in a new Notepad file. Please do this for every file or directory that has been identified as malicious.

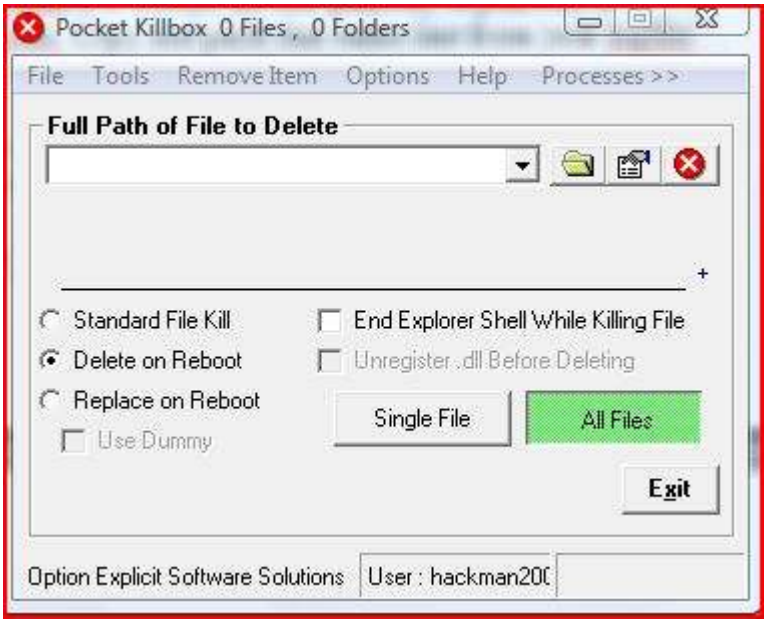
When you are done, you should have a list of files and directories. Do not close this list of files.




Download Pocket Killbox from the following link. Extract the files to your Desktop or wherever you choose.

Double-click the Killbox red Killbox file. Go back to your list of files and highlight all the pathways and copy them to your clipboard.

Set the program to Delete on Reboot and make sure it is set to All Files. If it is set to Single File, it will only delete the first file in the list and leave the rest.



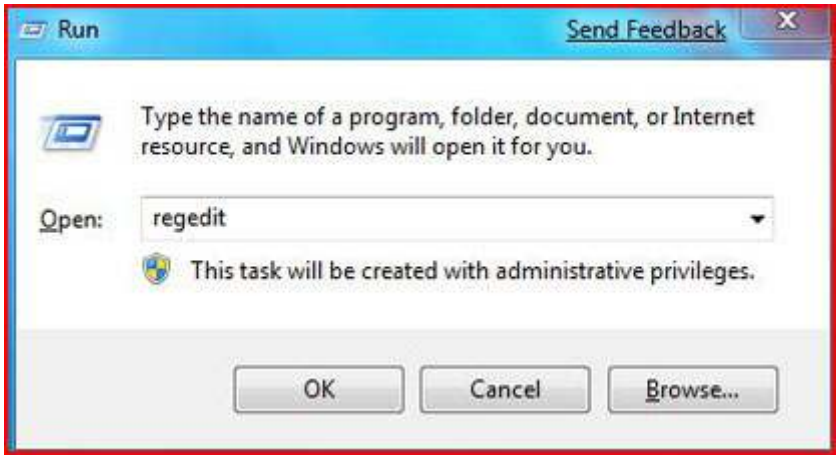

Now click File and select Paste from Clipboard. If no text appeared in the Full Path of File to delete, then try again. Click the Red X. Pocket Killbox will automatically restart your computer.

---

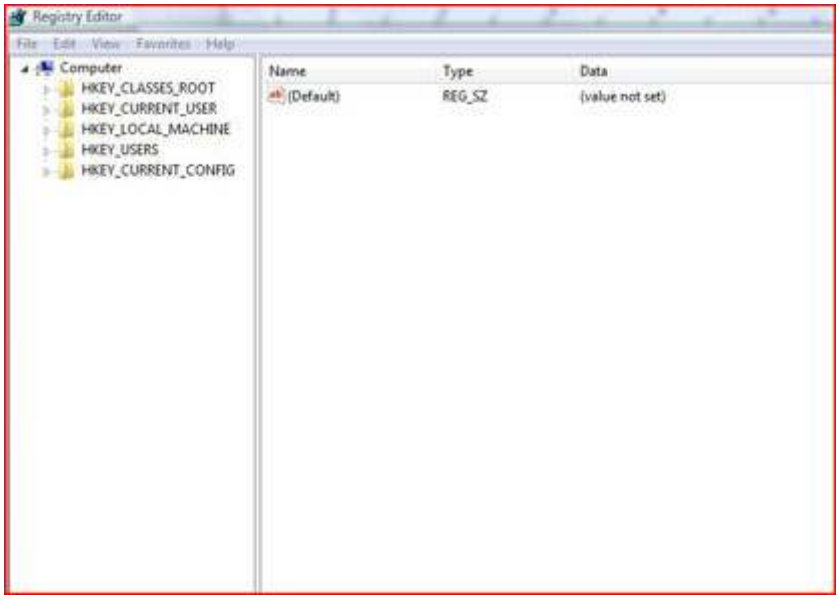
## 6. Advanced Registry Editing

If you happened to luck out and get a list of registry entries that were infected, then you can go through this more advanced step. This particular step is not required as long as the computer is mostly disinfected since the entries will only be remnant registry entries. When we do the final cleanup, it should also get rid of most of the entries. But if the entries are causing problems right now, then you can remove them here.

Launch the Registry Editor. You can do this by pressing the Windows Key and then pressing r simultaneously. Type regedit into the run window and press Enter.




You should get a list of five registry hives to the left of your screen. Each hive is similar to a pathway on your hard drive, such as C:\Program Files\Microsoft Office. In this example, you would double-click C, then double-click Program Files, and then find the Microsoft Office directory. The same process works in the registry editor. The only difference is you are not working with files and directories. You navigate through the left pane of the screen.




Navigate through the tree of entries until you find the exact one you are looking for. Make sure you select the right entry because many of them look similar. Then delete that entry from the left side of the window. Don't touch the right side, since that side just contains information related to that key. You may also use .reg files to do this, which may be simpler. If you are interested in this, see this Microsoft KB article.

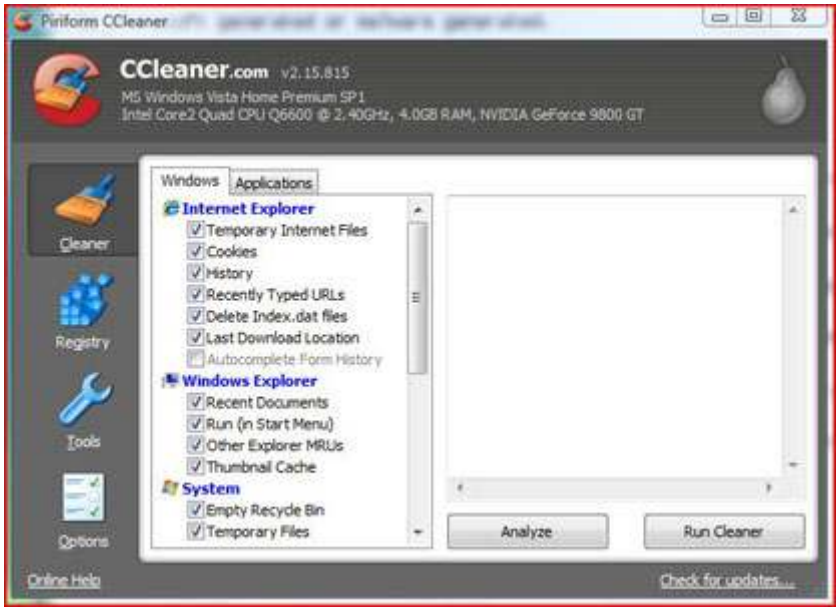
## 7. Cleaning up the computer

Often-times malware removal leaves the computer with some junk files (.dat, .txt, etc) on the hard drive and some invalid registry entries which may produce errors. There are two programs you can run, CCleaner and Comodo Registry Cleaner. CCleaner will get rid of temporary files and Comodo Registry Cleaner will get rid of the registry entries.

Download CCleaner from the following link. Save the file to your Desktop.

Install the program like any other program; make sure to keep the default settings.

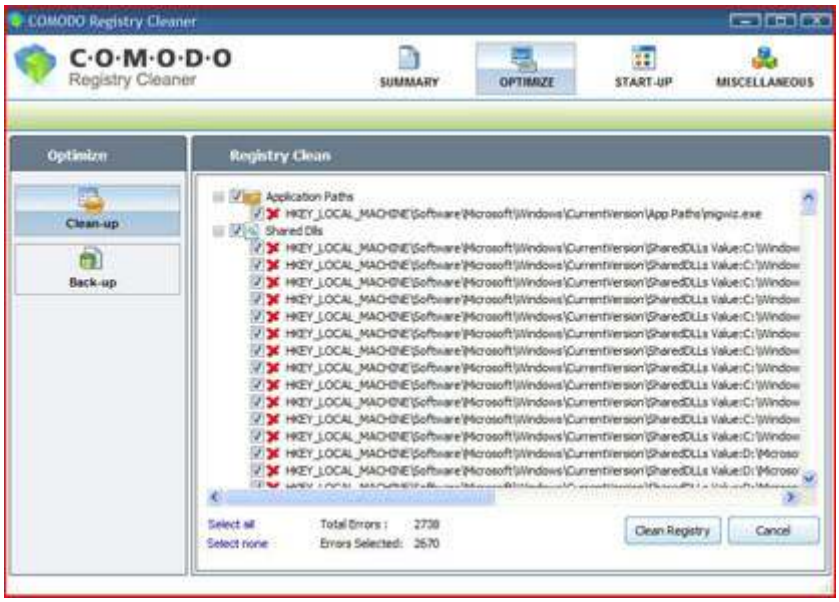
Double-click the CCleaner file on your Desktop and click the Analyze button and then the Run Cleaner button. Close the program.




Download the Comodo Registry Cleaner from the following link. Save the file to your Desktop.

Install the program like any other program; make sure to keep the default settings.


Click the Scan My Registry button and wait for the results. Click the Clean Registry button.




## 8. Prevention and Concluding Advice

The ultimate goal of malware removal is to prevent it from re-occurring. By following simple steps you can help ensure that you won't be infected again.

- Make sure Windows is up to date; otherwise you will get infected from the exploits that the patches are supposed to fix.

- Run security software. If you don't, you will get a malware attack again. The software you run may not effectively clean the computer after you are infected, but it will stop you from getting infected in the first place.
- Run browser security software. Our favorite extension is WOT, this extension alerts you to risky websites. If you don't want something like this, you can always use McAfee SiteAdvisor. It also warns you of risky websites, but does not block the malicious pages first.
- Remove your old versions of Java. The older versions of Java are heavily exploited by Vundo. When you install a new version of Java you are not removing the old version, it stays on your computer.
- Don't pirate software. Software pirating is a big cause of malware. Many torrent sites secretly have malware downloads waiting for people to download.
- Don't search for porn. Porn websites typically have malware on them since a lot of people browse these types of websites. Not all of them are infected, but if you browse around enough you will get infected.

COMMENTS:60
TAGS: Software, spyware, malware, ccleaner, windows. how-to, combofix, comodo registry cleaner
COMMENTS

- Login or register to post comments

- **DVD Burner**
- **Digital Cameras**
- **Portable Storage**
- **Computer Accessories**
- **Smartphone**
- **Antivirus Software**
- **Sound Cards**
- **Speakers**
- **Computer Systems**
- **Thumb Drives**
- **Video Cameras**
- **Video Card Reviews**
- **Water Cooling**
- **Gadgets**
- Keyboards

- Contact Us
- Advertising
- Privacy Policy
- Terms & Conditions
- RSS Feeds
- TechBlips
- PCHardwareBlips
- Site Map
- Customer Service



---

**Source URL:**
http://www.maximumpc.com/article/howtos/ultimate_malware_removal_guide_purge_your_pc_junk_files

**Links:**
[1] http://www.maximumpc.com/user/hackman2007
[2] http://www.maximumpc.com/article/howtos/ultimate_malware_removal_guide_purge_your_pc_junk_files
[3]

http://www.superantispyware.com/downloadfile.html?productid=SUPERANTISPYWAREFREE
[4] http://www.download.com/Malwarebytes-Anti-Malware/3000-8022_4-10804572.html?part=dl-10804572&subj=dl&tag=button
[5] http://www.combofix.org/
[6] http://www.pandasecurity.com/activescan/index/
[7] http://tinyurl.com/4fjfz9
[8] http://www.bleepingcomputer.com/files/killbox.php
[9] http://www.ccleaner.com/download
[10] http://registry-cleaner.comodo.com/download.html
[11] http://tinyurl.com/3gewgk
[12] http://tinyurl.com/6u6hw
[13] http://tinyurl.com/6o8wb
[14] http://tinyurl.com/3b3qyj
[15] http://tinyurl.com/e7pg2
[16] http://www.maximumpc.com/article/howtos/how_to_diagnose_your_pc_with_a_clean_boot
[17] http://www.maximumpc.com/article/an_easier_way_to_decrapify_your_pc
[18] http://www.maximumpc.com/article/new_year_in_spyware