Security & Maintenance PC & laptop (Windows based)

Istart websearches removal & other malware

Good Rule of thumb with installs: Often the only thing that is free is cheese in a mouse trap!

A few months ago, I was asked to remove Istart.websearches for someone. It had taken over his browser. Dealing with malware is a major issue. As a result, I wrote the following instructions. These instructions are useful for individuals and also as a lab for A+ software students or to use in a networking class.

For specific step-by-step-instructions to get rid of Istart.websearches I will refer to the following link I found: http://malwaretips.com/blogs/istart-webssearches-com-removal/ I followed these step-by-step instructions and successfully removed this malware.

Webbsearches is an example of malware software which cannot be removed in the traditional manner using the **Control Panel>Programs>Uninstall a Program**. You can install instead a different program, **Revo Uninstaller**, a more robust 3rd party utility, in case a program can't be removed through Windows Control Panel.
(Direct link: http://www.revouninstaller.com/revo_uninstaller_free_download.html)

Malware tends to hide itself inside the browser (Internet Explorer, Google Chrome, Mozilla, etc.)

It is important to be very careful with downloading software and freeware. Even with legitimate applications, such as (or in particular) **Adobe Reader**, be very careful: frequently malware is attached and unintentionally downloaded and installed by the user together with the legitimate software. This also frequently happens when using search engines such as **Ask.com**.

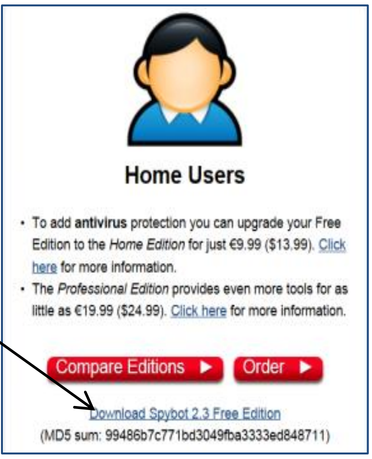
Solutions to deal with malware:

Antivirus programs:

1. **ESET Smart Security** www.eset.com (robust antivirus, Dutch site).
2. **Kaspersky Pure or Internet Security** (also includes a firewall) (For both Kaspersky & ESET a 30 day trial is available). Both are good antivirus software).
3. Norton and MacAfee are not very effective, Trend Micro is weak, and Microsoft Security Essentials is quite poor.
4. If you install a free anti-virus such as **AVG** it is difficult to uninstall, almost like virus itself: If you have this issue: (Using AVG removal as an example)
   a. Go to the Registry: In run box click: **Regedit>H_KEY local machine>software** look for the product: **Right mouse click** and **delete**. Go also to **HKEY_Current User>Software** and look for **AVG**. If you cannot find it: Highlight **Computer**> **Go to Find>Edit**: Type in **AVG** and let registry search for it. Remove the occurrences.
   Note: ***If you are not familiar with the registry, be very careful going in the Windows Registry!***
   b. Use a removal tool from their web site: for example: The following link has useful instructions how to: http://techdows.com/2009/04/download-avg-removal-tool.html but you need to be careful that it does *not download* other stuff along with the removal tool. *When you do this it is best to not multi task (don't do other things simultaneously) put pay attention to where you click and make sure to uncheck*

automatic includes in the prompts!

5. **SpyBot Search and Destroy:** Only download at this *legitimate* site: [safer-networking.org]() (type in the address bar without the www!)



Home Users

- To add **antivirus** protection you can upgrade your Free Edition to the *Home Edition* for just €9.99 ($13.99). Click here for more information.
- The *Professional Edition* provides even more tools for as little as €19.99 ($24.99). Click here for more information.

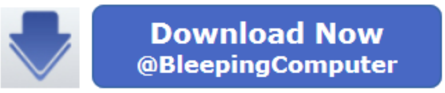
Compare Editions ▶ Order ▶

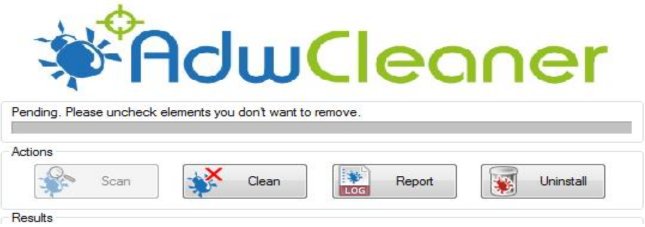
Download Spybot 2.3 Free Edition
(MD5 sum: 99486b7c771bd3049fba3333ed848711)

   a. Select **download** at top menu (to the right of **Home**)
   b. Scroll down just below "Home Users" Click on the hyperlink: download **Spybot 2.4 free edition**
   c. Click under **Ad-free download at Safer-Networking Ltd. Download**
   d. Then hit download again (to the right of donate button) and it will start the download and install
   e. When running the program: **Right click** icon and choose> **Run as administrator**
   f. Program comes up with a menu: follow instructions; then first run **Update** Update to latest version.
   g. Then do **immunization** Immunization to check system: Then run the **System Scan** System Scan and *disable tracking cookies*. **Clean** up the temp files. Then start the scan and wait until it's done.
   h. Then clcik **Fix Selected** and after that go to menu and open **Quarantine** and select everything in quarantine and purge all selected.

6. **Adware Cleaner** = small executable file. It is *not harmful* even though you may get the warning! Go to: Bleepingcomputer.com by:Typing in the address bar:: (*without* typing the www!) **bleepingcomputer.com** then on the download tab click on the left and scroll down where it says AdWareCleaner or you can also click on link [http://www.bleepingcomputer.com/download/adwcleaner/]()

7. ignore all free download info but click on the **blue** Download Now @bleepingcomputer. There are numerous redirects to ignore. Wait after one click few seconds and save to download folder or run and you have option to make short cut. It runs as a standalone program. It is an extremely effective malware killer. Double click and hit scan and then when done scanning hit Clean.



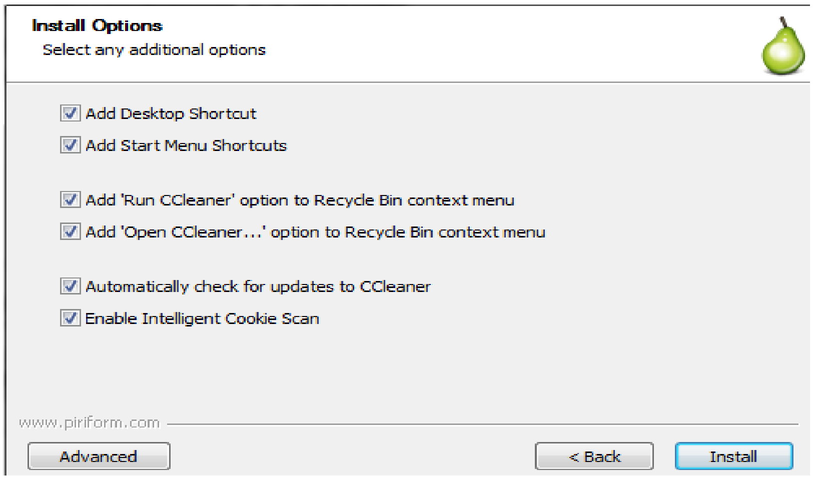


Pending. Please uncheck elements you dont want to remove.

   a. For example a very poor site that attracts a lot of malware is **Ask.com** and this site is very difficult to remove from system: Registry removal does not work, and Control Panel, but **Adware Cleaner** removes it.

8. **CCleaner (latest version 5.04)** is a utility that does not actually install on your computer. You can get the latest version from its native site Piriform: [https://www.piriform.com/ccleaner]() click on the download link and choose the free version.

You can leave all options checked when installing:



Install Options

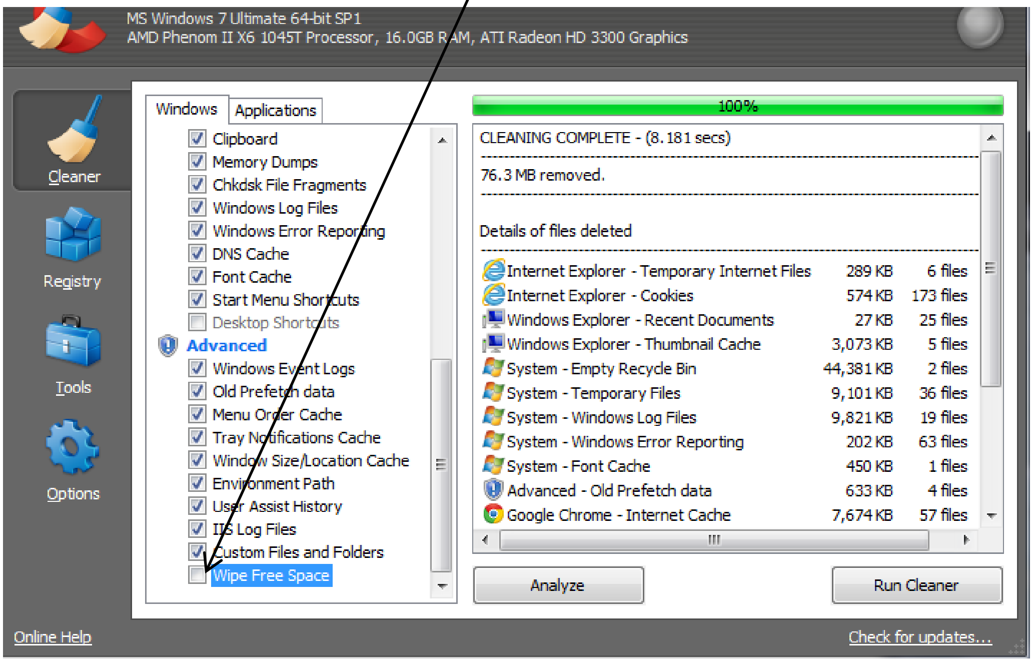
Select any additional options

☑ Add Desktop Shortcut
☑ Add Start Menu Shortcuts

☑ Add 'Run CCleaner' option to Recycle Bin context menu
☑ Add 'Open CCleaner...' option to Recycle Bin context menu

☑ Automatically check for updates to CCleaner
☑ Enable Intelligent Cookie Scan

Upon installation, before you run it, ***deselect*** the Windows Wipe option (it can take hours)



MS Windows 7 Ultimate 64-bit SP1
AMD Phenom II X6 1045T Processor, 16.0GB RAM, ATI Radeon HD 3300 Graphics

☑ Clipboard
☑ Memory Dumps
☑ Chkdsk File Fragments
☑ Windows Log Files
☑ Windows Error Reporting
☑ DNS Cache
☑ Font Cache
☑ Start Menu Shortcuts
□ Desktop Shortcuts

Advanced

☑ Windows Event Logs
☑ Old Prefetch data
☑ Menu Order Cache
☑ Tray Notifications Cache
☑ Window Size/Location Cache
☑ Environment Path
☑ User Assist History
☑ IIS Log Files
☑ Custom Files and Folders
□ Wipe Free Space

100%

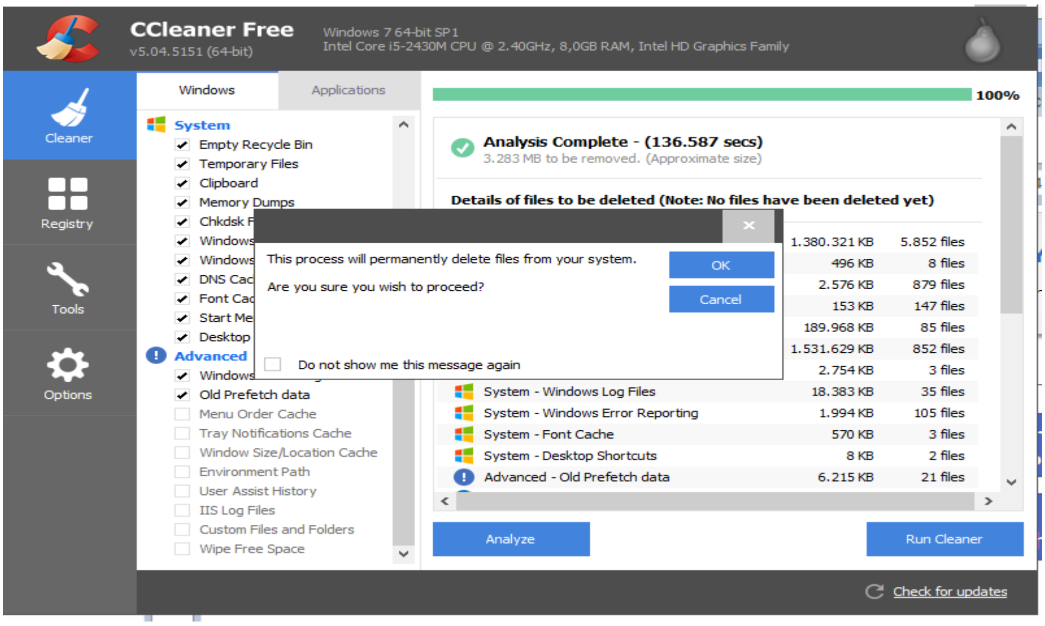
CLEANING COMPLETE - (8.181 secs)

76.3 MB removed.

Details of files deleted

Internet Explorer - Temporary Internet Files	289 KB	6 files
Internet Explorer - Cookies	574 KB	173 files
Windows Explorer - Recent Documents	27 KB	25 files
Windows Explorer - Thumbnail Cache	3,073 KB	5 files
System - Empty Recycle Bin	44,381 KB	2 files
System - Temporary Files	9,101 KB	36 files
System - Windows Log Files	9,821 KB	19 files
System - Windows Error Reporting	202 KB	63 files
System - Font Cache	450 KB	1 files
Advanced - Old Prefetch data	633 KB	4 files
Google Chrome - Internet Cache	7,674 KB	57 files

All the advanced options are now by default unchecked. If you check mark an option, you will get warning messages as stated below: Make a choice whether or not you want to remove. It is OK to do so but leave the last “wipe free space” option unchecked.



System
- ☑ Empty Recycle Bin
- ☑ Temporary Files
- ☑ Clipboard
- ☑ Memory Dumps
- ☑ Chkdsk F
- ☑ Windows
- ☑ Windows
- ☑ DNS Cac
- ☑ Font Cac
- ☑ Start Me
- ☑ Desktop

Advanced
- ☑ Windows
- ☑ Old Prefetch data
- □ Menu Order Cache
- □ Tray Notifications Cache
- □ Window Size/Location Cache
- □ Environment Path
- □ User Assist History
- □ IIS Log Files
- □ Custom Files and Folders
- □ Wipe Free Space

Analysis Complete - (136.587 secs)
3.283 MB to be removed. (Approximate size)

Details of files to be deleted (Note: No files have been deleted yet)

	1.380.321 KB	5.852 files
	496 KB	8 files
	2.576 KB	879 files
	153 KB	147 files
	189.968 KB	85 files
	1.531.629 KB	852 files
	2.754 KB	3 files
System - Windows Log Files	18.383 KB	35 files
System - Windows Error Reporting	1.994 KB	105 files
System - Font Cache	570 KB	3 files
System - Desktop Shortcuts	8 KB	2 files
Advanced - Old Prefetch data	6.215 KB	21 files

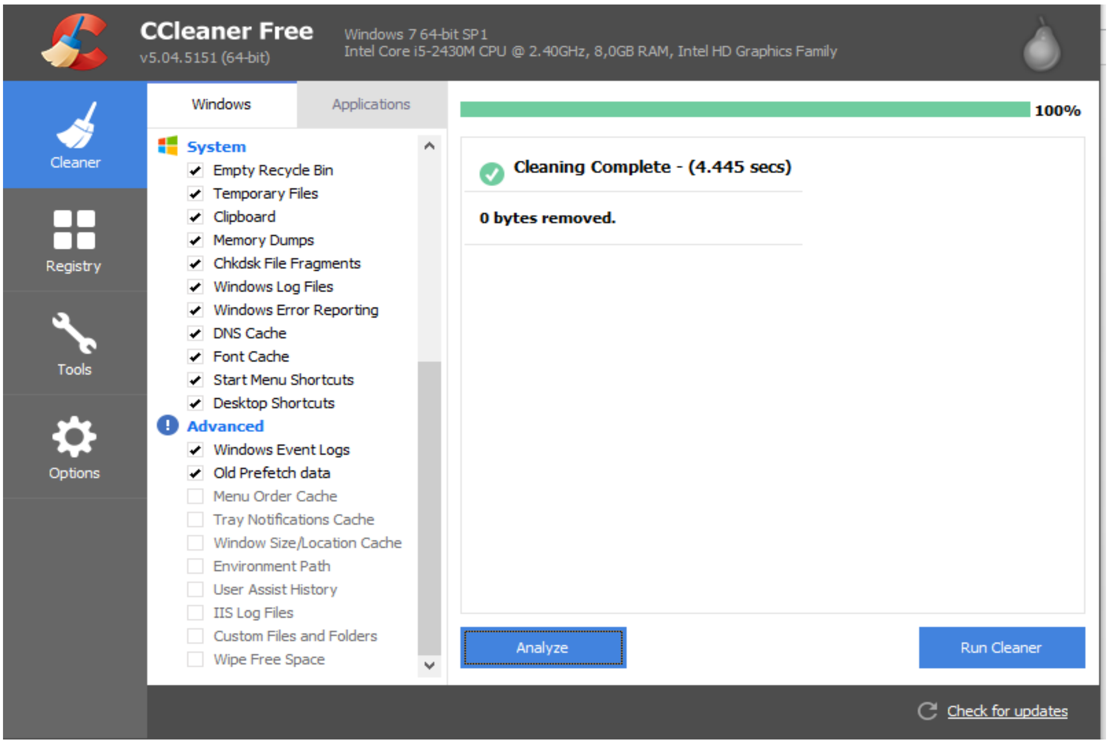
This process will permanently delete files from your system.

Are you sure you wish to proceed?

OK Cancel

□ Do not show me this message again

Click **Run Cleaner**. Upon completion, you do *not* have to click Analyze again. You may want to make multiple passes and run it several times until you get the message “Cleaning Complete.”



System
- ☑ Empty Recycle Bin
- ☑ Temporary Files
- ☑ Clipboard
- ☑ Memory Dumps
- ☑ Chkdsk File Fragments
- ☑ Windows Log Files
- ☑ Windows Error Reporting
- ☑ DNS Cache
- ☑ Font Cache
- ☑ Start Menu Shortcuts
- ☑ Desktop Shortcuts

Advanced
- ☑ Windows Event Logs
- ☑ Old Prefetch data
- □ Menu Order Cache
- □ Tray Notifications Cache
- □ Window Size/Location Cache
- □ Environment Path
- □ User Assist History
- □ IIS Log Files
- □ Custom Files and Folders
- □ Wipe Free Space

Cleaning Complete - (4.445 secs)

0 bytes removed.

<u>Note</u>:

*You should run **CCleaner**, **Adware Cleaner** and **SpyBot Search & Destroy** about twice a week to keep your computer free from being infected.*

Other maintenance Suggestions:

1. Regularly defrag your PC and laptop. Use **Smart Defrag V4.02**. This utility is more powerful than the Windows version. Go to to http://www.iobit.com/iobitsmartdefrag.html to download the free version.
2. If you are unable to remove an accidentally installed program in the Control Panel, use **Revo Uninstaller**).