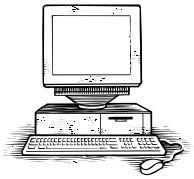
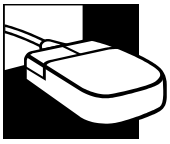


Ohio University
Computer Services Center
October, 2004
Spyware, Adware, and Virus Guide



Definitions

Malware – is term meaning malicious software. Malware is software designed to disrupt a computer system. A trojan horse , virus , or worm would be classified as Malware. Some advertising software is malicious in the way it installs without permission and can try to re-install itself after you remove it.

Spyware – is a term for software that collects personal data like names and e-mail addresses without a user's consent. It is usually installed on a computer as the result of downloading a new program. It can often cause system slowness, crashes, and problems in general.

Adware - gathers user information for the purposes of advertising, installing programs, and sending cookies to other spyware programs. Some adware will push popup windows based on keyword searches and visited websites.

Virus – A parasitic program written intentionally to enter a computer without the user's permission or knowledge. The word parasite is used because a virus attaches to files or boot sectors and replicates itself, thus continuing to spread. Some viruses do little but replicate others can cause serious damage or effect program and system performance.

Trojans –destructive programs containing hidden code which can view, modify, and delete data; monitor your actions online; and use one computer to attack other computers. They often can have backdoors that allow hackers access to your computer.

Computer Worm –A self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself.

Web bugs - are tiny graphics placed on a website or e-mail designed to monitor who is reading the web page or e-mail message.

Key logging - software can record each keystroke made on a computer. The data it gathers, which often includes passwords and screen names, can be stored for later retrieval.

Phishing - programs use fake web sites and emails (spam) to trick users into giving away private information like credit card numbers, account usernames and passwords, and social security numbers. Phishers lure users to harm by mimicking the names and appearance of trusted web sites and organizations. Once the user feels safe, they often unwittingly give up personal information to the "phishers."

Symptoms

The following are possible symptoms to watch for to determine if your machine has Malware problems. They are not 100% certain indicators of an infection or software problem since some hardware problems could also produce similar problems. Also normally installed software can conflict as well.

Slow Computer – Slower then normal when opening and exiting programs and going to the Internet. Perhaps starting up and shutting down is slower or not working properly.

CPU and **Hard Drive** – If the CPU is in constant use or hard drive constantly spinning and in use your computer may be infected.

Popup Ads – If the popup ads seem out of control perhaps spyware is to blame.

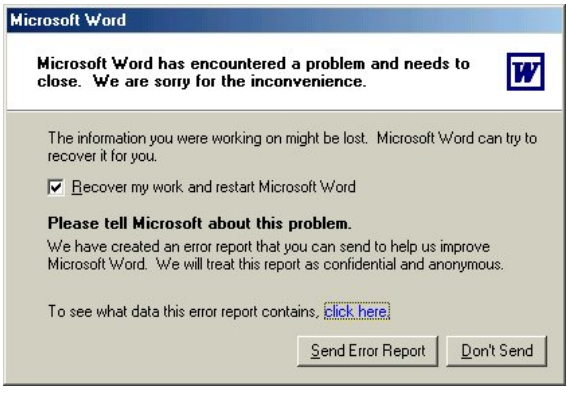
Hijacked – Some adware takes control of your web browser and takes you to pages not of your choosing.

E-mail – Some viruses will use your email account to propagate. If you see out look opening unexpectedly or get bounced messages you may be infected.

Computer Crashes – Some Malware can even cause the computer to be unstable and crash. In the past referred to as the Blue Screen of Death.

Windows 95, 98, ME, and 2000

Windows XP



Downloading and Installing Spyware and Adware Tools

The two software programs suggested by the Ohio University help desk for spyware and adware removal are Ad-Aware by lavasoft and Spy Bot - Search and destroy by PepiMK Software. The help desk suggests you install both programs and run them once a week to keep your system clean. You should also check for updates weekly as well. These two programs used in tandem seem to do a good job of catching and removing these forms of malware. The best part is they are free.

The Sites:

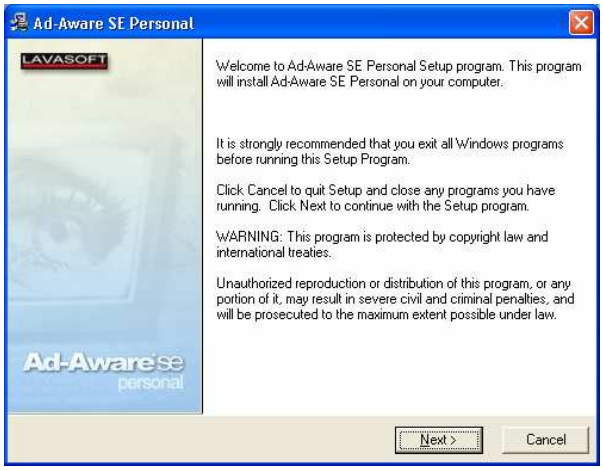
http://www.download.com/

http://www.lavasoft.de/ - **Ad-Aware**

http://spybot.safer-networking.de/en/index.html - **Spybot - Search & Destroy**

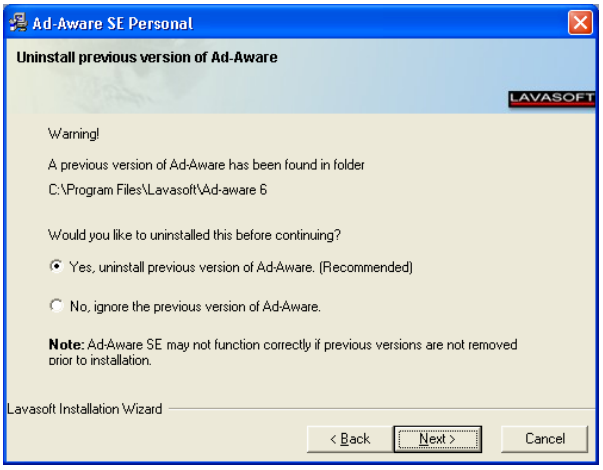
Installing and Running Ad-Aware

The file you download will be named something like aawsepersonal.exe, find where you downloaded this to and double click it.

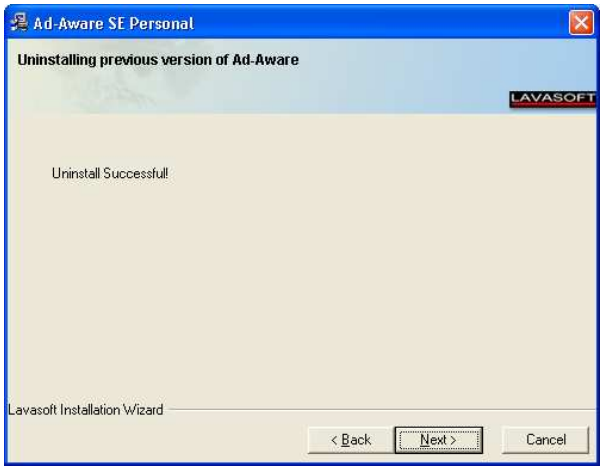


You will see the intial install screen appear. Click Next

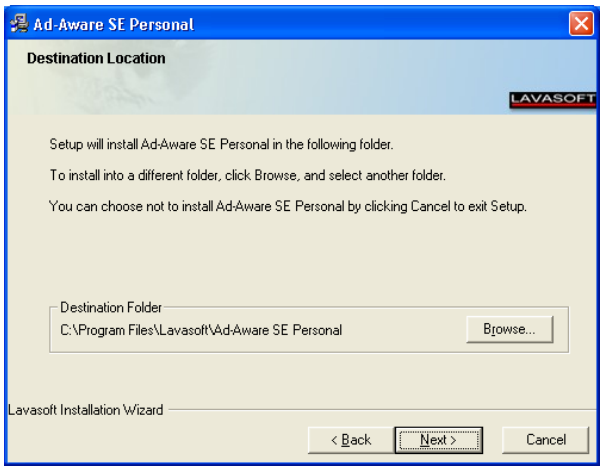
You must accept the license agreement to install the software so click in the box. It is not a bad idea to read license agreements on software some even reveal that spyware is going to be installed. The problem is most people just click yes and next and move on. After you have agreed to this one and check the appropriate box click next.



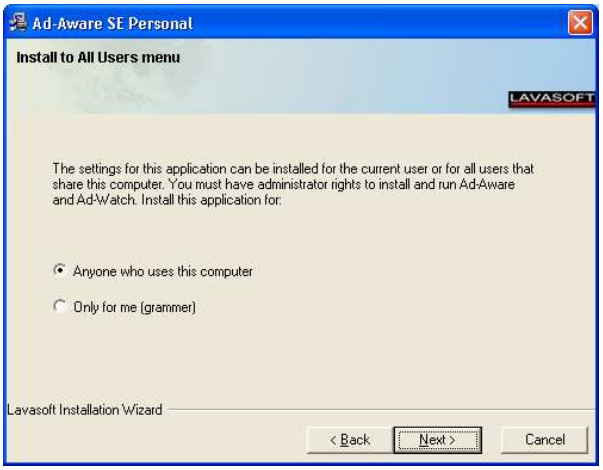
If you have a previous version of Ad-aware installed allow it to be removed. Click next.



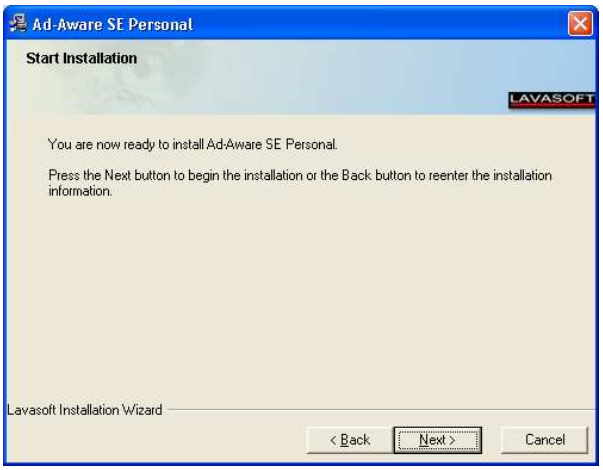
Click next.



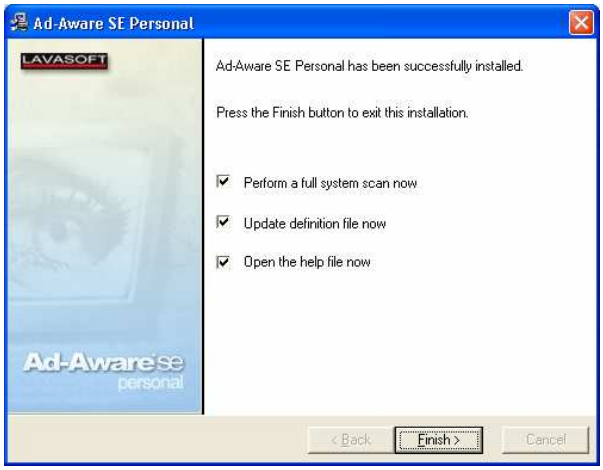
If you are satisfied with the default install location click next.



This software I would normally leave open to anyone. Click next.



Click next



Decide if you want to read the help file now and I would leave the update on and perform a full scan now by clicking finish. Ad-Aware will now do an auto update and then begin search your computer for spyware processes and files.

As it progresses it will inform you of the number of objects found. It will identify if these are processes, Modules, Registry keys or values, files, or folders. If browse much on the internet you will invariably pick up some cookies that will be found and seen as files of an Ad-ware nature.

When it is done scanning you will see a window similar to the one below.

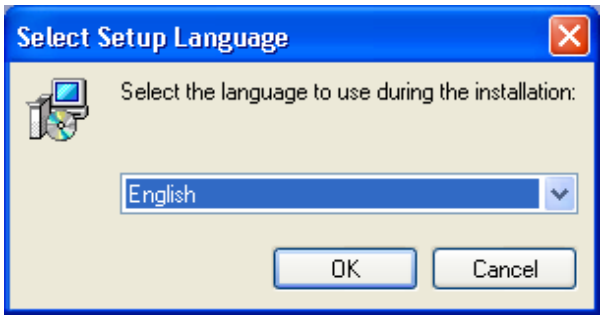
You can now learn more about the items detected and select which you want removed or quarantined. A fast way to select them all is click the scan summary tab and check each of the boxes. Then click next.

The status box above tells you what has been done. Clicking next would take you to the scan now screen. Since we have just scanned we do not need to do it again for a week or so.

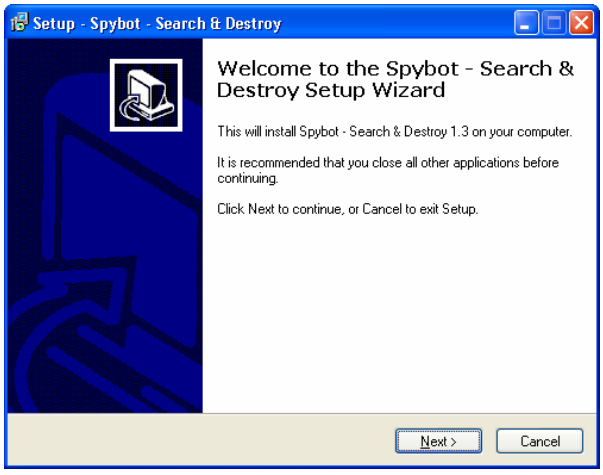
Ad-Watch and Add-ons are additional features of the program that require you to purchase a commercial version. We are now done and can close the program by clicking the "x" in the upper right hand corner.

Installing and Running SpyBot: Search and Destroy

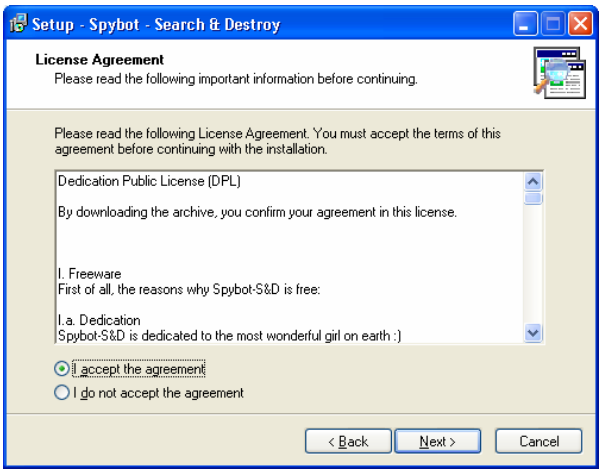
Find the file you downloaded, it should be something like spybotsd13.exe. Double click it to begin the installation.



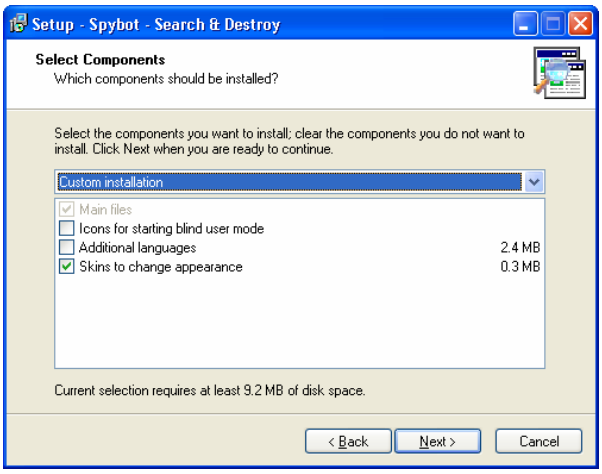
Choose your language and click OK.



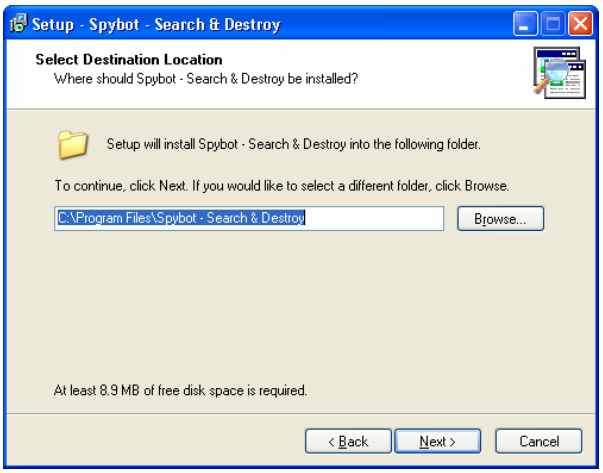
Click next to move on from the intro screen.



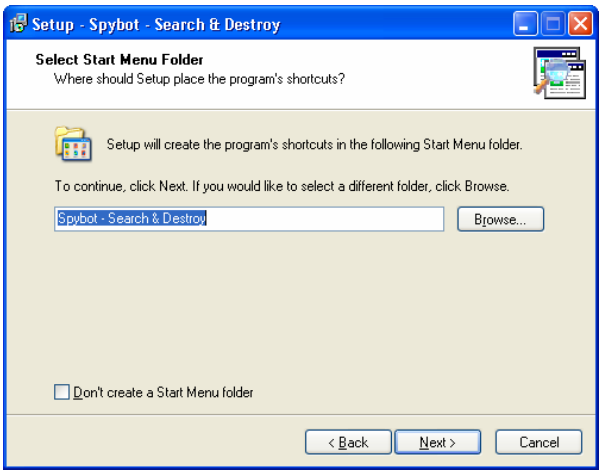
You must accept the license agreement in order to install the software. It is good practice to read these. Click next after accepting.



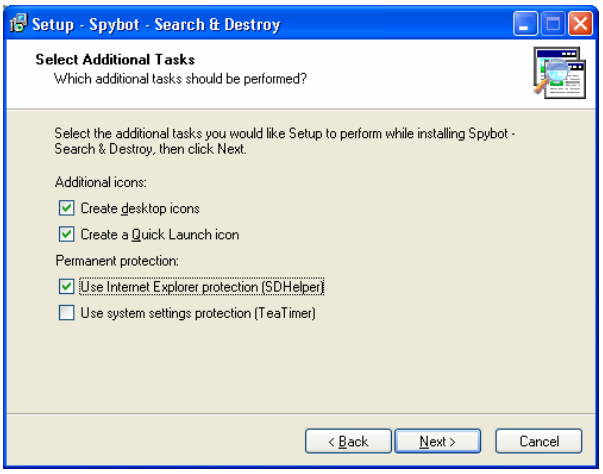
Click next to continue.



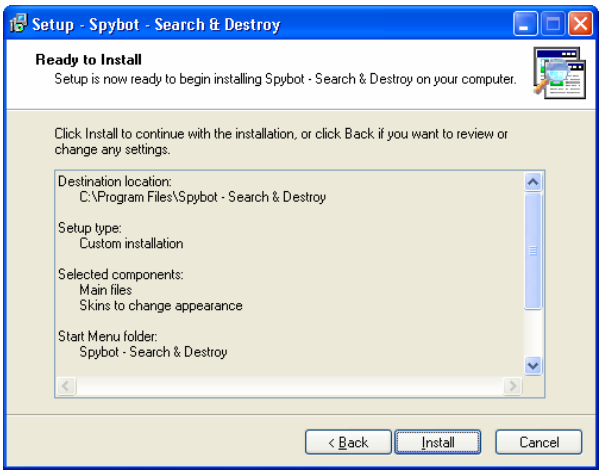
If the default install directory is okay click next to go on. Next will be an options menu for the default selections will be okay for most users.



The start menu selection should be okay click next.



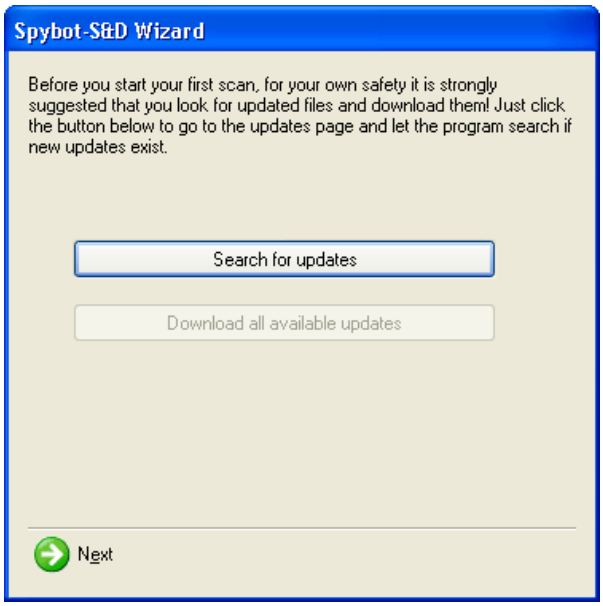
More options the default selections should be okay click next to continue.



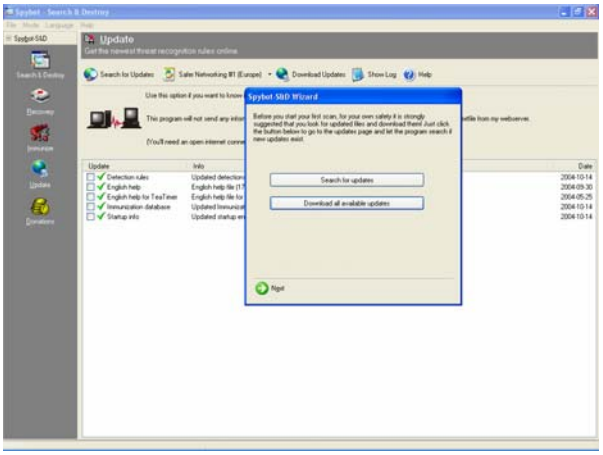
Click install.

Click finish to run Spybot: S&D.

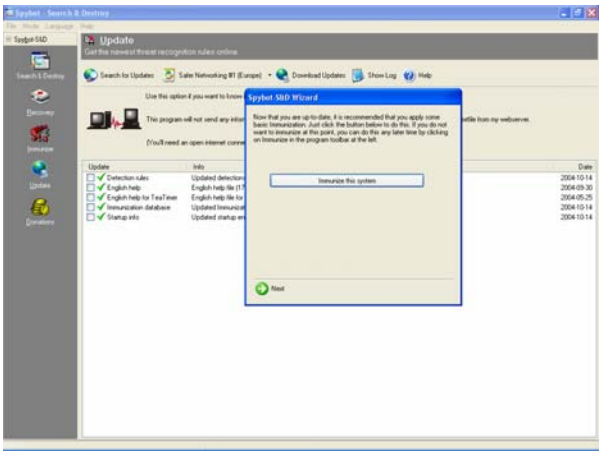
This is not a bad idea click the "Create registry backup" button. When finished click next.



Click the search for updates button. Then click download all available updates, if any were found.

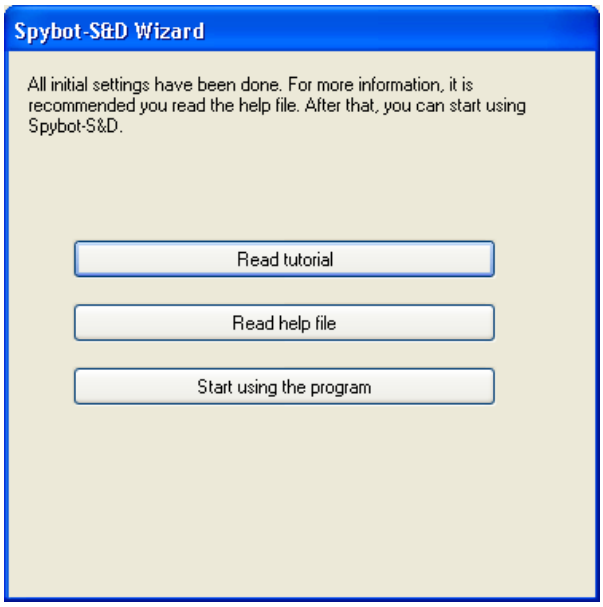


Click next.

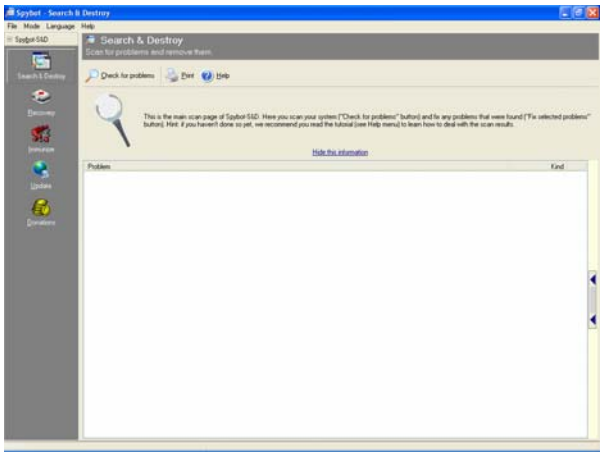


Click immunizes this system.

Click next.

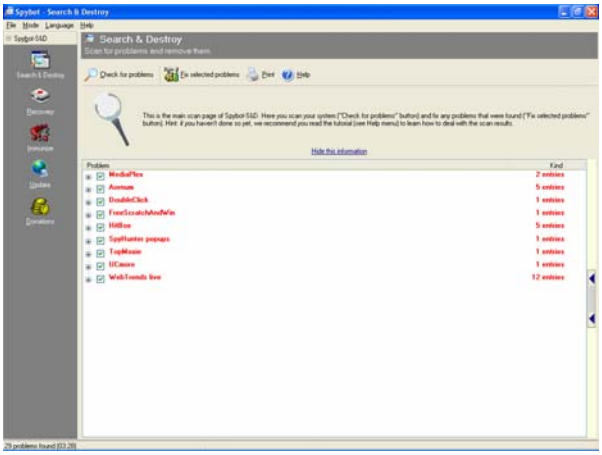


Choose if you wish to read a tutorial or the help file. Finally click start using the program.

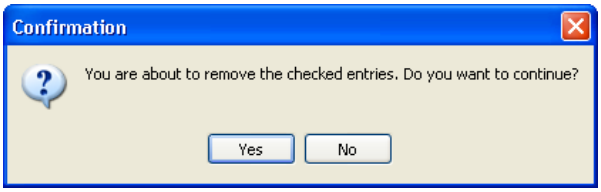


Click the search and destroy icon on the top left of the screen. Then click check for problems.

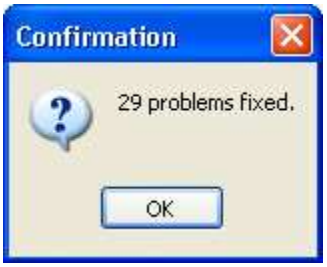
The program will begin looking for potential problem files and list them in the box. These two programs used in combination offer a good approach to catching many spyware and adware programs.



A few files were identifier as potential problems and marked to be fixed. If they seem to be programs you want fixed or removed click fix selected problems.



This warning is to make sure you are sure. Click yes.



These were all missed by the Ad-Aware program, glad I got a second opinion. Click ok. You are done now and can click the "x" in the upper right hand corner to close the program. Again you might want to run it again in about a week.

Computer Security and Info Website Links

http://www.microsoft.com/security/

http://www.spychecker.com

http://www.spywareinfo.com/

http://cexx.org/adware.htm

http://www.securityfocus.com/

http://www.ftc.gov/ **(Some Info)**