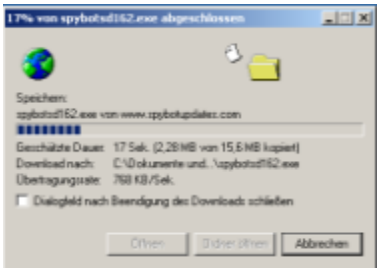
Installation and Instructions for Spybot Search & Destroy

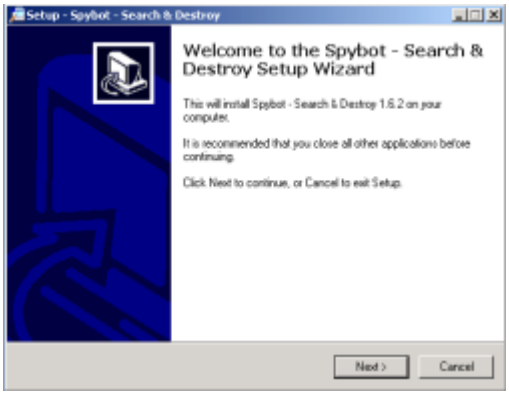
JoshBenson.com | Instructions (safer-networking.org)

1. Download



Obviously, the first thing you need to do is download Spybot-S&D from our download page. The download page first gives you a bit of donation information; if you like the program, I encourage you to come back later and donate something. But right now, you want to download. The downloads are on the same page, just scroll down a few lines and click *Spybot – Search & Destroy 1.6.2*. On the next page you will see a table with four download locations. Clicking on one of them will lead you to a page offering the download. Each of these pages is a bit different, but you should be able to find the download link there without problems.

2. Installation



The file you have downloaded will be named *spybotsd162.exe* or similar. To install Spybot-S&D, all you have to do is run the file, and the installation program will start (if you have downloaded with Internet Explorer, the download dialog will give you the option to open the file directly).

The installer will show you the license and ask you for the installation location. You can go with the default settings here and just click your way through the installer by using the *Next* button. After the installation has finished, you will see a *Spybot – Search & Destroy* button on your desktop and in your start menu. Click on it to start Spybot-S&D the first time.

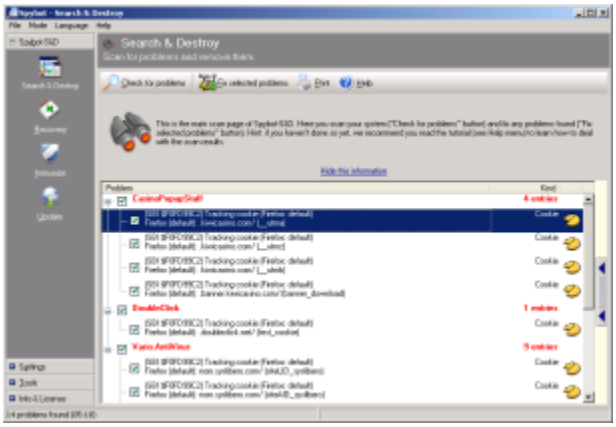
3. First run

The first time you start Spybot-S&D, it will display a *Wizard*, a small window helping you through the first steps. It gives you the possibility to add or remove the icons you have or haven't created during install, for example. Let's just say you want them and proceed to the next page.

If you are using a proxy in Internet Explorer, Spybot-S&D will show you this proxy and a button will give you the opportunity to use it for Spybot-S&D, too. If the text field is blank, you don't need to configure anything.

The next page deals with updates. It is very important to keep up-to-date. Using the two buttons this page offers to do the updates for you, you can also do the update at a later point. The last page of the wizard will ask you to read the help file. The help file is always a good resource if you are unsure what to do, so please do at least read the first pages of it.

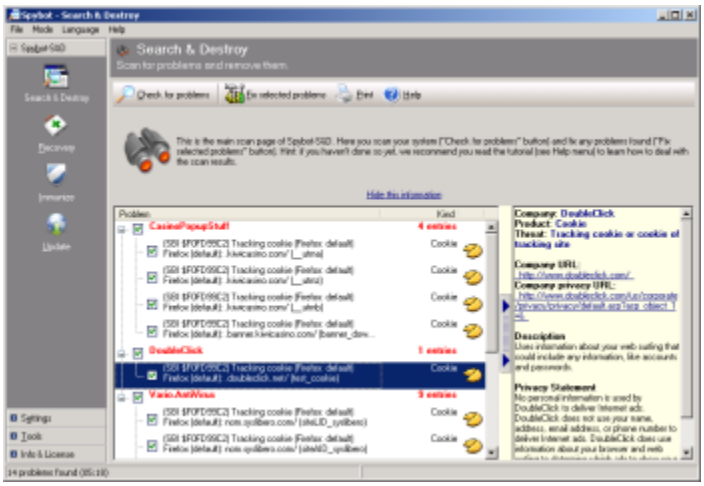
4. Doing a scan



After the Wizard has finished, you may find yourself on the *Settings* or *Update* page. As the default settings are ok right now, and you've already updated, let's ignore them for now and do the first scan. The left side of the program has a navigation bar that can lead you to all functions of the program.

The first section there (the top-most button) is labeled *Spybot-S&D* and leads you to the main page. Right now, you will see only an empty list and a toolbar at the bottom. The first button in this toolbar is named *Check for problems* – that is the button you've got to press to start the scanning. Lean back and watch the scan progress.

5. Interpreting the results



At this point, you could just jump to point 7, and remove the results. Instead we recommend that you first have a look at what all the stuff is that Spybot-S&D detected.

The first thing you should know is to distinguish between the red entries, which represent spyware and similar threats, and the green entries, which are usage tracks.

For the usage tracks (I hope you have followed that link to read what they are), removal is non-critical, but depends on your personal preferences. Ignoring the usage tracks for now, you should have a look at the red entries which represent the real threats. While you of course can trust us that we have chosen the targets using strict criteria, you can check for yourself if you click on each product and read the product information that will be shown in a pop-up window.

6. Decision on exceptions

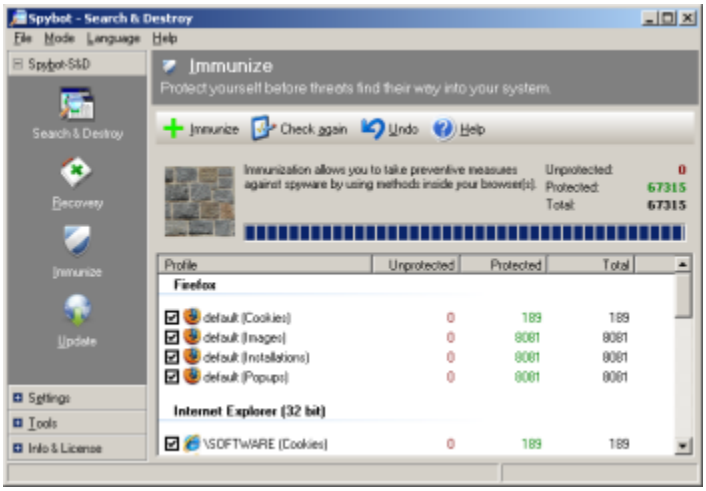
All problems displayed in red are regarded as real threats and should be dealt with. But while you read the product description, you may still decide to keep a threat, or just a usage track. Maybe you don't want your list of most recently used Word documents removed? At this point you have three options.

- You could decide on ignoring all usage tracks. In that case you could open the *File sets* page on the *Settings* section of the program, and disable the *Usage tracks* entries.
- Or if you want to just keep all tracks from a specific product, just right-click a product in the results list and choose the corresponding option.
- Finally, if you want to keep just one file, that is possible the same way.

7. Removing the threats found

So now you should know about everything you've found. It's time to use the *Fix selected problems button*. Once you start thinking about removing the usage tracks, too, you may think that ticking all the green entries is hard work. This is for a simple reason – to force you, the newbie – to look at the results. Once you know what you are dealing with, there is a hidden Select all button available for you.

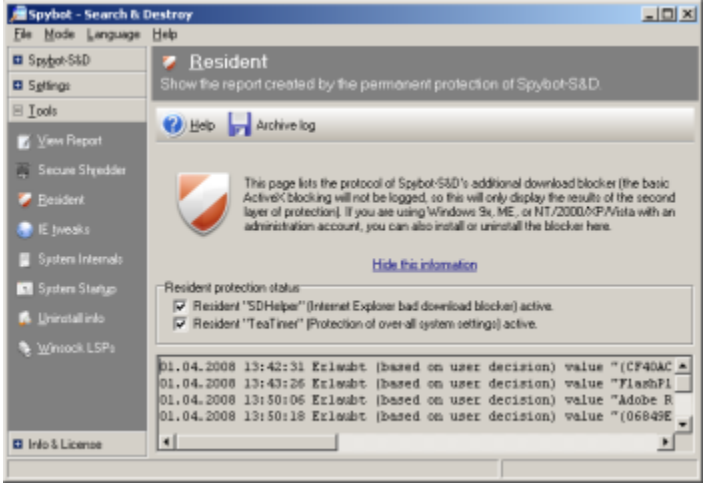
8. Resident



If you use Spybot-S&D's realtime protection against spyware, nasty spies will not enter your system. Currently there are three different kinds of protection.

The **Immunize function** prevents e.g. Tracking Cookies from entering your system. Immunize works with Mozilla Firefox, Internet Explorer and Opera, allowing you to adjust specific settings of the browser to block known spyware installers, (and similar baddies) already included in Spybot-S&D's database.

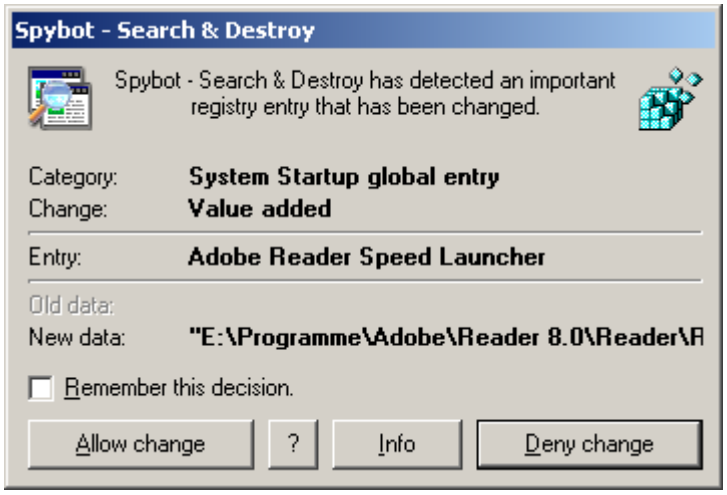
You start the Immunize function by clicking on *Spybot-S&D → Immunize* on the left navigation bar.



Resident SDHelper is a second layer of protection for IE. Immunize function blocks installers by their ActiveX ID, while SDHelper blocks badware that tries to enter using a different method. Thus Internet Explorer cannot download bad files. You start SDHelper by clicking on *Tools → Resident* on the left navigation bar (therefore Spybot-S&D has to run in *Advanced Mode*). There you can tick the checkboxes next to *Resident "SDHelper" (Internet Explorer bad download blocker) active* in order to activate SDHelper.

Resident TeaTimer prevents unwanted files from being installed – no matter how – on your system. It monitors the processes called/initiated perpetually. If known malicious processes want to start, TeaTimer immediately terminates them, giving you three options how to deal with this process in the future:

- be informed when the process tries to start again
- automatically kill the process
- generally allow the process to run



There is also an option to delete the file associated with this process.
If something tries to change critical registry keys, TeaTimer will detect it.

TeaTimer can protect you against such changes by giving you an option: You can either *Allow* or *Deny* the change. TeaTimer is always running in the background.

Since Spybot-S&D 1.6 the TeaTimer uses our database where known files are rated as good or dangerous. This database contains several hundreds of thousands entries and is enlarged continuously. Nonetheless now and then there are files which are not contained yet. In these cases and if you use older Spybot versions Resident TeaTimer will ask your permission for every change. If you are not sure if you should allow the change, there is a simple rule of thumb:

If you have been installing something and/or if you judge the file that is going to be installed as good because you know its name, you can proceed by allowing the registry change (same thing if you or Spybot-S&D were deleting an application). But if the message comes out of the blue sky while you were surfing the web, you should get cautious. In this case it is better to deny the registry change.

You start Resident TeaTimer by clicking on *Tools → Resident* on the left navigation bar (therefore Spybot-S&D has to run in *Advanced Mode*). There you can tick the checkboxes next to *Resident "TeaTimer" (Protection of over-all system settings) active* in order to activate TeaTimer.

Of course it is possible to revise each of your personal decisions. That could be necessary if you have denied some process which turns out as a good one later. You do so by right clicking on the TeaTimer symbol in the system tray – it is the blue one with the lock. (If you cannot see the symbol, it is probably hidden. Just click on the arrows in the system tray to show all hidden symbols.) A window appears where you have to click on *Settings* to modify your personal lists of registry changes and processes.

Find more step-by-step instructions in our how-tos

- How to update
- How to uninstall
- How to switch the language
- How to make a recovery
- How to make a backup
- How to export the Startup list
- How to exclude products from the search
- How to enable the Select all button
- How to download Spybot-S&D
- How to disable the proxy
- How to disable Spybot-S&D temporarily