Description

Spybot - Search & Destroy can detect and remove spyware of different kinds from your computer. Spyware is a relatively new kind of threat that common anti-virus applications do not cover yet. If you see new toolbars in your Internet Explorer that you didn't intentionally install, if your browser crashes, or if you browser start page has changed without your knowing, you most probably have spyware. But even if you don't see anything, you may be infected, because more and more spyware is emerging that is silently tracking your surfing behaviour to create a marketing profile of you that will be sold to advertisement companies. Spybot-S&D; is free, so there's no harm in trying to see if something snooped into your computer, too :)

Spybot-S&D; can also clean usage tracks, an interesting function if you share your computer with other users and don't want them to see what you worked on. And for professional users, it allows to fix some registry inconsistencies and offers some extended reporting features.

License

Spybot-S&D; comes under the <u>Dedication Public License</u>.

Requirements

- Microsoft Windows 95, 98, ME, NT, 2000 or XP (32 and 64 bit), 2003, Vista.
- Compatible with bootable PE disks (e.g. BartPE) and Wine.
- Minimum of 10 MB free hard disk space, more recommended for updates and backups.

Usage

We recommend that you continue by reading the <u>tutorial</u> next.

I. Freeware

First of all, the reasons why Spybot-S&D; is free:

I.a. Dedication Spybot-S&D; is dedicated to the most wonderful girl on earth :)

I.b. Binary

What do you get if you buy software? Lots of ones and zeros, nothing more. If they were distributed as art, I could understand paying for it. But if the main goal of their order is to earn money - by fees or ads - I do not like it!

I.c. Conclusion

This means that I grant you the license to use Spybot-S&D; as much as you like. But if you like it, I ask two things of you: say a prayer for me (and the most wonderful girl while you are at it ;)) to your god - or whatever you believe - and wish us some luck.

II. Limitations

II.a. Reverse Engineering

Reverse Engineering is not allowed as with nearly any software. If anyone has doubts in the honesty of the code, I will give insight to a trusted organization like a university under certain limitations (for example only one copy, for a limited time, and that has to be removed after the evaluation time has ended).

II.b. Warranty

I tried my very best to make the code of Spybot-S&D; as stable as possible, and I give you the warranty that I placed no code to cause intentional harm to your system.

However, removing the threats targeted by Spybot-S&D; sometimes involves cutting deep into the system sometimes, and I cannot guarantee that your system will be running the same as before. For example, spyware hosts may stop working. Neither can I give you any warranty that Spybot-S&D; will remove every spy on your system, or that it will give you no false positives. For your own verification the location of the problem is shown with every

entry, and if you have any questions remaining you can visit the support forum for more information.

II.c. Liability

Under no circumstances can you make me liable for any damage, however caused, including, but not limited to damage you might do to your system using Spybot-S&D.;

II.d. Use of application in whole

Free use is limited to the application in whole. Usage of parts only, for example the database or the plug-ins, is not permitted.

II.e. Corporate use

As companies are not individual persons and would have problems fullfilling the above terms, there is a license for corporate users that can be found at <u>safer-networking.ie</u> (online link).

III. Distribution

Here are some basic rules about distributing Spybot-S&D.;

III.a. Private distribution

You may give away single copies of the software as long as you do not modify this license or other files of the archive.

III.b. Mirroring

If you want to mirror Spybot-S&D;, feel free to do so as long as you do not modify the original archive. If you want to be kept up to date about major updates, you can subscribe to the mailing list.

Official mirrors need to fulfill the Mirror Policy (online link).

III.c. Publishing

You may publish Spybot-S&D; in a book or magazine (or other media) by simply sending a written request for permission, including a description of your specific needs. I request a copy of the media in which Spybot-S&D; is published as compensation.

IV. Privacy

IV.a. Application offline privacy

Even though Spybot-S&D; scans your system, it will not search specifically for any personally identifiable information. Everything that is not detected as a possible threat will be ignored. Possible threats will be shown and, if log options are switched on, written to a local log file.

IV.b. Application online privacy

Spybot-S&D; has online functionality in 5 cases:

1. Update: The Update function now uses an ftp-protocol to download an info file containing update descriptions (this is called spybotsd.ini, and it will not be deleted, so you can look at it) and to download the update files you select. No information other than those your browser would also show will be transmitted. 2. News: On the web site (online link) of Spybot-S&D; you will find the News section. Here you can read about the most important news all around Spybot-S&D.;

3. Bug Report: The bug report function sends the problem description you enter and an automatically created report to our support staff. You can modify the extent of the report on the settings page, and you can preview this contents while you are writing the bug report.

Files listed in the attach box will be sent as attachments. The header will contain the information (sender name & address) you have entered in settings. *4. Product info & opt-out links:* those may often link to dubious pages. You may open them at your own risk, but you should take care to meet some security measures (like firewall, latest IE updates, updated antivirus software) first.

5. Other links: Due to the nature of the Internet I cannot give you any guarantee regarding other links found on my web pages (neither my own, the support forum, or the donation site). But I have put my trust in them and do not believe any harm can come from them.

First run	Tutorial
	Image of program wizard
The first time you start Spybot-	0 1 0
S&D, it will display a <i>Wizard</i> ,	
a small window helping you	
through the first steps. It gives	
you the possibility to add or	
remove the icons you have or	
have not created during install.	
for example. Let us just say	
you want them and procede to	
the next page	
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 do not need to do it, but in most cases this will show an internet address, and you should import this proxy setting.

The next page deals with updates. It is very important to keep up-to-date. Using the two buttons this page offers will do the updates for you, if you want to do it at a later point, use the update feature in the *Spybot-S&D*; section.

The last page of the wizard will ask you to read the help file. It looks like you are already doing this :)

Doing a scan

Tutorial

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 have already updated, let us ignore them for now and do the first scan.

On the left side of the program you can find 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 top. The first button in this toolbar is named *Check for problems* - that is the button you have got to press to start

the scanning. Lean back and watch the scan progress.

Interpreting the results

At this point, you could just jump to the last point, 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.

	Tutorial
Interpreting the results	

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, of course, you can trust us that we are choosing the targets using strict criteria, you can check for yourself. If you click on each product and then on the grey button on the right you can read the product information in the box popping up. Decision on exceptions

Tutorial

All problems displayed in **red** are regarded as **real threats** and should be dealt with. But while you read the product description (you can find it by selecting an item in the list and then clicking on the grey button on the right side), you may still decide to keep a threat, or just a <u>usage track</u>. Maybe you do not want your list of most recently used Word documents removed? At this point you have three options.

- You could decide on ignoring all . In that case you could open the *File sets* page in 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 rightclick a product in the results list.
- Finally, if you want to keep just one file, that is possible the same way.

Removing the threats found

Tutorial

So now you should know about everything you have found. It is 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 on the *settings* page (only when started in advanced mode).

Setting the basic options

Settings

All important settings are listed in a tree in this section. Please note that these settings are only visible if you start Spybot-S&D in advanced mode - the default mode will not show them.

The description that follows is sorted by the trees main categories.

Installation

This section lets you change the desktop icon as well as the start menu and quicklaunch item.

Main settings

These are some miscellaneous settings about essential warning and confirmation dialogs. Here you can for example change your backup preferences.

Automation

Spybot-S&D has two kinds of automation settings – on system start and on program start. Here you can set whether to start the program when you start up your Windows, or to check for updates automatically, or to delay the scan on system start for a specified delay or until other programs (scanners) have terminated.

Log file settings

Spybot-S&D can write details about each scan into text files. Here you can select whether to do this, whether the date and time should be included in the filename, and whether to append or to overwrite the log file.

Look & Feel

You can switch a few details about the look of Spybot-S&D. Just try the options and see what look you like most. After a while, you may want to

disable the introducing information panels, for example.

Bug Report

If you are unsure about problems, you may send a bug report to Safer Networking Limited. This section is about how the emailing should be handled. You should at least select to include system information and scan results in the bug report (you can preview it before sending). Also, if you want to receive the same email as Safer Networking Limited, you may select to send a copy to yourself (you need to change SMTP settings to do this – see the <u>Bug Report help</u>).

Expert settings

These are some settings the normal user may not need, but that could be useful to the power user. For example, you can set up external applications to view result data here.

You can find the main settings by choosing *Settings* from the *Settings* section in the toolbar to the left.

Settings

The Scheduler page allows you to add an entry to automatically run Spybot-S&D to the Windows scheduler. To do this, you first have to click the *Add* button, then set the necessary properties (scheduled time etc.) through the *Edit* button. You can remove a task later on by using the *Remove* button. Custom options that you will see are checkboxes to decide if you want to automatically fix problems after the scheduled scan, and to close the program after scanning/fixing has finished.

The *Edit* button opens the default Windows task properties dialog, so that you can change the task like any other Windows Scheduler task.

Choosing the interface language

Settings

If you downloaded Spybot-S&D; from the Internet, it will come with a lot of languages already included, but not the help files (to reduce the download size). You should use the update function to download additional files for your language after you have selected it.

If your language is not yet shown, you can go to the *Settings* page and enable the option to download foreign language updates. In that case, your next update will show you the updates for all available languages, even those not yet installed on your machine.

You can find the language settings by choosing *Languages* from the *Settings* section in the toolbar to the left.

Choosing what to scan (file sets)

Settings

Spybot-S&D; uses the concept of Include Files to make it more flexible. Each Include File is a file containing the description of some problems that Spybot-S&D; can detect and fix.

These files are divided into categories, so you can select what you would like to target in your next scan.

The basic categories are "Spybots" (which contains the includes for <u>spyware</u> <u>and adware</u>) and <u>Usage tracks</u>. For each category you may see Include Files with a short description on what they do and the number of files, registry entries and directories that will be checked.

You can select the Include Files you wish to use for your next scan by toggling the checkbox next to them.

If you see an Include File in italic letters, then it is one not originating from Safer-Networking Limited. As the Include File format is public, anyone may write Include Files. However, as Include Files can do a lot of harm to your system and Safer-Networking Limited is not liable for a foreign Include File, you will be asked whether you are really sure you want to use any file that is not from Safer-Networking Limited.

You will find the file sets settings by choosing *File sets* from the *Settings* section in the toolbar to the left.

Choosing what not to scan

Settings

Right now, there are five different Ignore sections:

Ignore products

This section lists all products defined internally and in the external include files. If you want to exclude a complete product, or include it again, select the file from this section and toggle the checkbox in front of the product name.

Ignore Cookies

Cookies are usage tracks, but you may want to keep some useful cookies. This section lists all cookies currently on your system, allowing you to exclude them from further searches.

Ignore file extensions

This concerns the common Windows file opening dialog. It saves lists of opened (and saved) files broken down by their extensions. If you do not want to remove the WinWord files, for example, you could select *.doc* to be excluded in this section.

Ignore single entries

If you do not want to exclude a complete product, but only a single file orregistry setting of it, you can select that one from the results list. Theseare listed here, where you may remove them from the exclude list again.

Ignore system internals

If you have got <u>system internals</u> results on the list, you can remove them from the Ignore list here.

All the lists in these sections have a context menu with extended selection options.

You will find these options by choosing one of the four Ignore features from the *Settings* section in the toolbar to the left.

Setting the download directories

Settings

Some scans do also target the installer files of problems detected by Spybot-S&D. Installers that the user must explicitly download himself will only be scanned for in the directories entered into this list.

You can either use Drag and Drop to drop some directories from an Explorer window or use the context menu to add or remove directories to or from the list.

You will find the download directories settings by choosing *Directories* from the *Settings* section in the toolbar to the left.

Choosing a skin

Settings

Spybot - Search & Destroy supports the concept of basic skins, to adjust program colors to personal needs.

To get new skins (at first there are only two available, the original Spybot-S&D; and the Peace) you can visit the following homepages: <u>http://www.safer-networking.org/en/download/index.html</u> <u>http://www.allsecpros.com/sbsd.html</u>

Then choose your favorite skins and simply download them and extract them to the Spybot-S&D; skins folder.

The Skin section will show you a list of available skins. Select one to preview it. The (very simple) preview will be displayed in the left part of the window, with some information below the list and the skin logo at the bottom of the page.

If you like the skin, press the *Apply selected* button.

You can find the skin settings by choosing *Skins* from the *Settings* section in the toolbar to the left.

Ignore Cookies

Settings

Cookies are usage tracks, but you may want to keep some useful cookies. This section lists all cookies currently on your system, allowing you to exclude them from further searches.

(At the moment, only Internet Explorer and Netscape Navigator and Mozilla cookies are supported - Opera cookies can only be completely deleted)

Ignore file extensions

Settings

This is about the common Windows file open dialog. It saves lists of opened (and saved) files divided into extensions. If you do not want to remove common text files, for example, you could select *.txt* to be excluded in this section.

Ignore products

Settings

This section lists all products defined internally and in the external include files. If you want to exclude a complete product, or include it again, select the file from this section and toggle the checkbox before the product.

Ignore single detections

Settings

If you do not want to exclude a complete product, but only a single file or registry setting of it, you can select that one from the results list. These are listed here, where you may remove them from the exclude list again.

Ignore System Internals

Settings

If you have put <u>System Internals</u> results on the ignore list, you can remove them (from the ignore list) here.

```
Updating
```

Spybot-S&D;

In order to avoid large downloads and for more flexibility, the main part of scanning information is located inside the include files.

Include files, as well as newer help files, new languages, updated descriptions etc. can be downloaded using the integrated update function.

Of course, in order to update the program, you need an open internet connection.

After that, you can click the *Search for updates* button. That opens a new window, enabling you to execute the update programm "SDUpdate". After doing that, a list of available updates will be downloaded from a Safer Networking Ltd. server and compared to the files already installed on your system.

New files will be shown in the list, where you can select them and press the *Download updates* button afterwards. During download, every finished file will get a green check mark.

If you want to read about updates first, visit our website or the support forum.

You can find the update function by choosing *Update* from the *Spybot-S&D*; section in the toolbar to the left.

Reporting a bug

Tools

You should use the bug report only as a last resort. First, please check for newer versions, read the FAQ and visit the support forum.

If all that hasn't helped solve your problems, you may write a bug report. Before doing this please check if you have got a current version of Spybot-S&D.; To prove if you are up to date you can use the integrated update function (Spybot-S&D; section). After this check please go to the *Tools* section, then choose *bug report* and press *Next*. If this is the first time you are writing a bug report, you may need to adjust your email settings. Click the button *Mail settings* and change them to your settings. The dialog popping up will allow you to set all necessary data. If you are using Outlook or Outlook Express, you may even import your settings and will only have to enter your password.

Once the email settings are correct, you can write your bug description into the text field for *Your detailed description of the bug*. Then, please press *system generated report*. At this point, a specified report from the machine will be listed that will also be sent to us. If you want to attach a file to the report please drag it to the box at the bottom. Once you have done that and verified that everything is correct, you can press the *Send* button to send the email.

You will find more bug report options in the <u>main settings</u>.

Opting out

Tools

If you have subscribed to some advertisers service by accident in the past, and do not know where to opt out again, you may be lucky to find advertiser listed here. Double-click the address to either visit the website or send an opt out email (you can distinguish between the two by the icon in front).

Please do not use this function as a preventive measure, because that would give you no advantages, but instead give the advertiser your address.

You can find the Opt Out list by choosing *Opt Out* from the *Tools* section in the toolbar to the left.

Scanning your system

Spybot-S&D;

Once you have started Spybot - Search & Destroy, you can immediately start scanning.

Having started the program, you will already see the scan screen. If not, please select *Search & Destroy* in the *Spybot-S&D*; section in the toolbar to the left.

The search screen contains a toolbar with the most important options. Let us start a scan: please press the *Check for problems* button.

You will see the scan progress in the status bar at the bottom of the window, and can stop the progress at any point by pressing the *Stop check* button that has just appeared (it will vanish again once the check has finished).

If the scan has found something, the list will show it. There are two basic kinds of results:

- **Red entries** indicate <u>spyware</u> problems that should be fixed to avoid security and/or privacy problems. This is the only kind of problem that is preselected to be fixed.
- Green entries indicate <u>usage tracks</u>. It can do no harm to remove these.

For most of the problems there is more information available. On the right side of the window you will find a grey button. By clicking it a window will open and show you some information about the item selected (if there is none selected, you can simply click on it and the information will be displayed).

You can now select the problems you want to fix, by clicking the checkbox in front of it, or by selecting all using the button *Select all problems* (this button will only be available after enabling the expert button setting in advanced mode). More selection options are available if you look into the context menu (by right-clicking a problem). The context menu will also allow you to exclude single problems or whole products from further scans (you may later change the exclude settings in the <u>settings</u> section/Ignore...). Another option the

context menu offers is to copy or export the result list or a full report.

Once you are sure you have selected what you want to be removed from your computer, press the *Fix selected problems* button. You will see the fixing progress at the bottom status bar.

If some problems cannot be fixed right now (because they are still loaded and can't be terminated, for example), Spybot-S&D; offers an option to run on next system start, so you can check and fix again.

Should you notice at any later point that you have removed more spyware than you wanted, you can always restore it from the <u>Recovery</u> in the Spybot-S&D-section.;

You can also fine-tune your scan options by selecting special <u>File sets</u> and changing some <u>Settings</u>.

```
Immunize
```

Search & Destroy

Beginning from version 1.2, Spybot-S&D allows you to immunize your computer against some spyware. It currently offers three different immunities:

Permanent Internet Explorer immunity

The permanent immunity works on some Internet Explorer control options that are partly visible in the Internet Explorer interface, partly hidden in the registry only. It adds domains known to contain bad contents into the Restricted Zone, thus blocking installation of executable code from those pages; it also adds block options for bad executable code by its ID, and it sets known tracking cookies not to be accepted by Internet Explorer.

To cut it short: it modifies Internet Explorer, through official ways, to block a lot of the bad stuff known to Spybot-S&D.;

Permanently running bad download blocker for Internet Explorer

This is a second layer of protection for IE. While the Permanent Immunity blocks installers by their ActiveX ID, this one blocks anything that should come through by different aspects.

You can view a log of blocked installers in the <u>Tools / Resident</u> section.

Permanent Opera immunity

This list shows all Opera profiles, and how many of the plugins that Spybot-S&D knows as bad are already blocked in each profile. To set the complete protection, just tick the checkbox in front of the profile you want to protect. To remove the protection, untick the checkbox.

Not many browser plugins are currently working for Opera, but the attempt to install some may crash Opera, and ActiveX support for Opera is available in third-party beta software, so use this function as a precaution against future misuse of Opera through spyware.

This feature will (certainly) only be displayed if you have Opera installed on your system!

Recovery

Spybot-S&D

The recovery section is available by selecting *Recovery* from the *Spybot-S&D* section in the toolbar to the left.

If you have fixed some spyware problems in the past, this list will show it. Here you can select one or more problems (see also the context menu for extended selection options) and either recover or finally purge them from your system.

In addition to the Recovery feature, Windows ME, XP and Vista users have the possibility to enable the creation of System Restore Points for each fix. This option can be set in the *Main Settings* part of the *Settings* section. When going back to a System Restore Point, the Resident TeaTimer needs to be shut down: With TeaTimer running, it will take note of the changes and ask to either *Allow* or *Deny* them. However, in the process of restoring Windows will restart too fast to allow the changes.

Product information

In order to find the product information in the results list please click on an item and then on the grey button on the right side. There you will find more information about the problems Spybot-S&D; is targeting.

The information shown contains URLs only, but as some of these URLs may directly start an (ActiveX) download, you cannot open them by using the standard double-click. Instead, right-click somewhere in the info field and select the URL you want to visit if you are sure your browser is set to safe settings.

You can also choose to exclude a product from further searches by rightclicking it and selecting *Exclude this product from further searches* (this does the same as ignoring a product in the <u>settings</u> section).

In that context menu you will also find the option to copy the results or a full report to either to a text file or to the clipboard.

Blind users

Spybot-S&D has been adjusted to fit the need of blind (disabled) users. Already during the installation the user has the choice to create an icon to start Spybot-S&D in a special mode. It will also switch to that mode if it detects that accessibility support is installed. As a third option, the *Settings* page contains an option to switch to this special mode.

In this special *blind user* mode, the context menus (the ones that would appear if a user right-clicks on a list), the toolbar (usually at the top or bottom of each page) and the global navigation bar at the left are mirrored into two main menu submenus that the user can use for easier navigation. The two graphical lists (the results list and the recovery list) will also be switched to text format. As the checkboxes are not available in this text format, these lists will contain the text *CHECKED* or *UNCHECKED* at the end of each entry. This check option can be toggled using the space key.

Spyware and Adware

Dictionary

What is spyware? To put it simply, spyware is software that transmits personally identifiable information from your computer to some place in the internet without your explicit approval knowledge.

Spyware is typically not the product you install yourself, but small add-ons, that you may or may not disable during install. In most cases, the EULA somewhere has a few lines telling you about privacy matters, but typically most users do not read the complete EULA and never know they got spyware on their system.

A less threatening kind of malware (i.e. malicious software) is adware. Adware is similar to spyware, but does not transmit personally identifiable information, or at least the collector promises not to sell it. Instead, aggregated usage information is collected.

Also, adware is often a side-effect of spyware, as both monitor you for a sole purpose – delivering advertisements to you that are especially tailored to your habits.

Another kind that is detected under the spyware category are tracking cookies. Cookies are used all over the internet in useful and less useful places. Advertisement companies often set cookies whenever your browser loads a banner from them. In that case and if that cookie contains a GUID, the company gets notice about every site you visit that contains their ads.

System internals

Dictionary

The windows registry contains a lot of information. Its consistency can be checked with good commercial programs like Symantec[™] System Works. But there are some small things I miss with those programs. Here is what SpyBot-S&D; searches for:

- **Missing help files** the registry contains information about the location of some help files. If this information points to incorrect directories, Spybot-S&D; will inform you about and allow to fix.
- **Missing shared DLLs** the registry contains a list of dynamic link libraries, where they are located and how many programs are using them. SpyBot-S&D; checks if all locations are correct and allows to change them if not.
- **Application paths** some applications (mostly those registered to a file extension) are registered in the registry. If they are pointing to a program file no longer existing, Spybot-S&D; can change their path or delete their entry.
- Wrong Uninstall information every program that has its own uninstall routine stores some information about it in the registry. If this information is incorrect, Spybot-S&D; will tell you about. For example, the uninstall program may have been located inside a temp directory (there are lots of programs that stupid!).
- **Broken Desktop Links** if one of the links on your desktop links to a file that no longer exists, Spybot-S&D; will tell you and allow you to either point the link to another file or delete it.

Warning: Please be aware that changes to these items can corrupt your system! If you are not sure whether a setting is really a problem you'd better leave it alone!

This warning especially applies if you are using Microsoft Office[™]. This

software suite has some registry entries pointing to wrong directories and some even pointing to non-existent help files. I have changed the first, but I would not delete the other one, because they may well point to files that will be installed on that "Install on first use" basis.



Usage tracks

Dictionary

Usage tracks are your fingerprints in your system. Whenever you visit a page with your browser, or just open any file, that information is stored deep inside Windows. In most cases that is very useful – if you want to open that file again, you can select it from a list instead of typing the whole filename or browsing the whole directory structure again.

But in some cases you may want to hide your activity, because spyware and internet attackers may use that information. Spybot - Search & Destroy can remove some of the most important and common tracks on your system.

Tools

Spybot - Search & Destroy offers multiple tools to help you looking deeper into your system.
View report

Tools

This tool allows you to create a new report including all or just a selection of the reports that Spybot-S&D can create. You can then save the report to a file for future reference.

The tool also allows you to view old reports again.

Resident

Tools

Resident is a permanently running application to protect your system. Currently, it consists of a browser helper for Internet Explorer that will block download of files known as malicious (spyware installers for example). This page inside Spybot-S&D; allows you to install/uninstall this helper as well as view the report of which pages it has blocked (that should only appear if the first layer of protection, the main IE immunity, did not stop the culprit).

The second resident tool is the <u>TeaTimer</u>

You can find the resident tools in the *tools* section.

What is the Resident TeaTimer?

TeaTimer

The Resident TeaTimer is a tool of Spybot-S&D; which perpetually monitors the processes called/initiated. It immediately detects known malicious processes wanting to start and terminates them giving you some options how to deal with this process in the future: You can set TeaTimer to:

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

There is also an option to delete the file associated with this process.

In addition, TeaTimer detects, when something wants to change some critical registry keys. TeaTimer can protect you against such changes again giving you an option: You can either *Allow* or *Deny* the change. As TeaTimer is always running in the background, it takes some resources of about 5 MB.

Why does Resident TeaTimer terminate the application before asking? TeaTimer

Because threats like toll <u>dialers</u> are time critical - they cost from the first second they have connected. In order to protect you, these have to be terminated at the moment they appear before they can connect at all.

Why is the TeaTimer called *TeaTimer*? TeaTimer

As we used to forget our tea, when we let it brew, we built a small tool with a system tray icon to remind us. We called this tool *TeaTimer*. When we started to develop the Resident tool for Spybot-S&D;, we also needed a system tray icon for this. As we do not like having too many icons in the system tray, we decided to put both tools together and kept the name *TeaTimer*. The next version of the Resident tool might also have the functions of the original *TeaTimer*.

You can find the Resident TeaTimer in the *tools* section.

ActiveX

Dictionary

ActiveX is a Microsoft technology that allows Internet applications that are more powerful than simple scripts. ActiveX applications do only work in Internet Explorer, so the use of ActiveX on web sites is not recommended. Due to the huge amount of influence ActiveX applications can have on the system (ActiveX applications have access to the same files you have access to, meaning all files in the case of most private computers), it is recommended to be very careful if dealing with ActiveX.

There are two types of ActiveX applications - signed and unsigned. The code of unsigned ActiveX applications has not been certified and should never be trusted. Signed ActiveX applications are certified, but can still contain malicious code! Signed ActiveX applications should only be trusted if they come from trusted web sites and only on a prompt base (meaning that Internet Explorer settings will ask every time a web site wants to load an ActiveX application).

Many <u>dialers</u> and <u>hijackers</u> install themselves using ActiveX applications.

ActiveX

Tools

Spybot-S&D; is able to display a list of installed ActiveX applications. It also has a small database integrated that will display a green checkmark in front of ActiveX applications known as legitimate, and a red sign in front if applications known as illegitimate.

This list can be exported into a text file as a reference and for further analysis.

Feature added in version 1.3: entries that have changed since the last snapshot (the first snapshot was created when you started Spybot-S&D; for the first time, later on you can create snapshots by right-clicking the list and selecting the corresponding menu item) are displayed in bold letters. This allows you to see changes to the list at once.

BHO, Browser Helper Object

Dictionary

A BHO is a small program that extends Microsoft's Internet Explorer. Examples of BHO usage include visible add-on toolbars in Internet Explorer, but can also be hidden functions. Ad- and spyware as well as <u>browser hijackers</u> often use BHOs to display ads or follow your track across the internet, because a BHO has access to each URL you visit and can redirect you or display other pages than you requested (ads, for example).

BHOs often use <u>ActiveX</u> installation programs.

BHO

Tools

Spybot-S&D is able to display a list of installed browser helper applications. It also has a small database integrated that will display a green checkmark in front of browser helpers known as legitimate, and a red sign in front if applications known as illegitimate. It also allows the user to enable or disable single BHOs.

This list can be exported into a text file as a reference and for further analysis.

Feature added in version 1.3: entries that have changed since the last snapshot (the first snapshot is created when you started Spybot-S&D; for the first time, later on you can create snapshots by right-clicking the list and selecting the corresponding menu item) are displayed in bold letters. This allows you to see changes to the list at once.

Browser pages

Tools

Spybot-S&D; is able to list all known locations where Internet Explorer start and search pages are anchored. If your browser got hijacked and you cannot use the normal Interent Explorer control panel to reset your start or search page, you can use this Spybot-S&D; tool to locate the URL (please send it to detections@spybot.info so that it can be added to the next update), and change it.

Hosts file

Dictionary

The hosts file could be described as an address book. While the normal user is accustomed to access other computers on the internet using names (for example security.kolla.de), every computer is accessed by a numeric address at a lower level. You may already have seen this numeric addresses; they look like 127.0.0.1 for example.

Every time you try to access another computer by using his name, your computer looks up his address in an address book. First it looks into a local address book (the hosts file), and only if it cannot find the address there it looks in a very big address book in the internet.

So, if you want to block an internet web site, you could simply redirect this sites name to a place where nothing will be delivered from. Such a place would be your computer for example. The address I already mentioned, 127.0.0.1 is an address that will always point to the local - your - computer. By adding an entry to the hosts file (your local address book) that redirects an ad site to your machine, you would trick your internet browser to think that ad site would be on your machine, and as your machine does not deliver ads, it would not get the ad and it will not be displayed.

Another way of using the hosts file is if you want to access computers that are not listed in any address book yet. For example if you have a local network, you would not list your local computers in any internet address book, if only because that would be very expensive. So you could just enter them into the local address book (your hosts file).

Spybot-S&D; using the hosts file

Tools

Spybot-S&D; can add a prepared list of web sites known for bad behaviour (installing spyware or tracking users, for example) to your hosts file. If you want to do this, we recommend you also read the FAQ about cures for possible slow-downs on Windows NT based systems (Windows NT, 2000, XP and Vista). And if you should notice you cannot visit a site that worked before, you should check the Hosts file section to see if that site is on the block list.

IE Tweaks

Tools

These are very small changes recommended to make your system a bit safer and more secure. Locking the hosts file will prevent most hosts hijackers (even unknown) from doing harm; locking the IE settings will prevent other users of your computer to change your preferences.

You can also change the Internet Explorer title to a user-defined text, or remove a pre-defined text.

Process list

Tools

This tool displays a list of all currently running processes, including some information about them. It also allows you to kill some processes, but please do not use this function until you know what you are doing!

System startup

Tools

This tool lists all programs that are started at Windows startup. If those items are in the database coming with Spybot-S&D, it will display some more information about them. It also allows you to disable (and enable) items, as well as delete them, change them or insert new items.

The entries will be displayed in different colours:

- **Green**: legitimate program
- **Yellow**: unknown, unneeded or unambiguous program (e.g. malware programs might use the same file name as legitimate programs)
- **Red**: malicious program

On Windows 9x and ME, the user has full access to this list. On Windows NT/2000/XP/Vista, the list will display the global and the current user entries. For some functions like seeing all entries or even changing some, the user may need admin or power user rights.

Since version 1.3 entries that have changed since the last snapshot (the first snapshot is created when you started Spybot-S&D; for the first time, later on you can create snapshots by right-clicking the list and selecting the corresponding menu item) are displayed in bold letters. This allows you to see changes to the list at once.

Uninstall info

Tools

This tool lists all programs that have registered some kind of Uninstall information with Windows. You can use it to remove the uninstall information of no longer existing programs as well as to simply get an overview.

Entries that have changed since the last snapshot (the first snapshot is created when you started Spybot-S&D; for the first time, later on you can create snapshots by right-clicking the list and selecting the corresponding menu item) are displayed in bold letters. This allows you to see changes to the list at once.

LSP, Layered Service Provider

A Layered Service Provider is a system driver linked deep into the networking services of Windows. It has access to every data entering and leaving the computer, as well as the ability to modify this data. A few such LSPs are necessary to allow Windows to connect you to other computers, including the Internet. But Spyware may also install itself as an LSP, thus having access to all the data you transmit. LSP are currently used by CommonName, New.Net, NewtonKnows and webHancer.

Winsock LSPs

Tools

Spybot-S&D is able to display a list of installed network drivers as a reference for professionals, and allows this list to be exported for future reference.

Since version 1.3 entries that have changed since the last snapshot (the first snapshot is created when you started Spybot-S&D for the first time, later on you can create snapshots by right-clicking the list and selecting the corresponding menu item) are displayed in bold letters. This allows you to see changes to the list at once.

© 2000-2008 Safer Networking Ltd. All rights reserved.

Dictionary

About TeaTimer

Spybot - Search & Destroy is an on-demand spyware and malware scanner. That means it scans for threats whenever you choose to do so. It also offers some preventive measures like its Immunize function.

Resident, of which *TeaTimer* is a part, is Spybot-S&D's permanently running partner that does on-access scanning. This means that it will instantly detect and counteract to threats and unsolicited system settings changes.

TeaTimer

Spybot - Search & Destroy has detected a change to a Browser Helper Object.

Definition

TeaTimer

Spybot-S&D; Resident watches for new or deleted Browser Helper Objects (which are plugins for Internet Explorer, sometimes expanding its functionality, but often used for malicious purposes as well).

User interactions

TeaTimer

Did you just try to install some Internet Explorer plugin? If it is not shown as a bad one, you should proceed. If this happens out of the blue sky while surfing the web, you should get cautious.

TeaTimer

Spybot - Search & Destroy has detected a change to an Internet Explorer toolbar.

Definition

TeaTimer

Spybot-S&D; Resident watches for new or deleted Internet Explorer toolbars.

User interactions

Did you just try to install some Internet Explorer plugin? If it is not shown as a bad one, you should proceed. If this happens out of the blue sky while surfing the web, you should get cautious.

© 2000-2008 Safer Networking Ltd. All rights reserved.

TeaTimer

TeaTimer

Spybot - Search & Destroy has detected a change to some ActiveX installation.

Definition

TeaTimer

Spybot-S&D; Resident watches for new or deleted Internet Explorer Internet installations.

User interactions

TeaTimer

Did you just try to install some Internet Explorer plugin? If it is not shown as a bad one, you should proceed. If this happens out of the blue sky while surfing the web, you should get cautious.

TeaTimer

Spybot - Search & Destroy has detected a change to some custom Internet *Exlorer menu entry*.

Definition

TeaTimer

Spybot-S&D; Resident watches for custom Internet Explorer menu entries.

User interactions

Did you just try to install some Internet Explorer plugin? If it is not shown as a bad one, you should proceed. If this happens out of the blue sky while surfing the web, you should get cautious.

© 2000-2008 Safer Networking Ltd. All rights reserved.

TeaTimer

Spybot - Search & Destroy has encountered and terminated a process that is listed as part of a malicious software.

Definition

Spybot-S&D; *Resident* watches all applications that are being started on your computer. It knows the same bad files as the on-demand scanner of *Spybot*-*S*&*D*;, and if it encounters an application that is known as a threat, it will automatically terminate this application.

User interactions

After the process has been terminated, you are presented with a few choices. You can assign the action Resident should take the next time it encounters this threat (like automatically killing it, and/or deleting the offending file).

Frequently Asked Questions

Q: Why does *Resident* terminate the application before asking? A: Because threats like toll dialers are time critical - they cost from the first second they have connected. In order to protect you, these have to be terminated before they can connect at all, at the moment they appear.

© 2000-2008 Safer Networking Ltd. All rights reserved.

TeaTimer

TeaTimer

Event

TeaTimer

TeaTimer

TeaTimer

Spybot - Search & Destroy has detected a change to Internet Explorer start or search page setting.

Definition

TeaTimer

Spybot-S&D; Resident watches all known Internet Explorer start and search page settings, and warns you about changes to them.

User interactions

TeaTimer

If you get a warning about an Internet Explorer page that has changed when you did not change it yourself, you should usually deny it (if it is not a microsoft.com page that is set - IE tends to change pages itself on a fresh computer).

TeaTimer

Spybot - Search & Destroy has detected a change to a System Startup entry.

Definition

TeaTimer

Spybot-S&D Resident watches for changes to this setting, and allows you to react to them.

User interactions

TeaTimer

Not all startup entries are bad - you have to decide if you trust the program that asks the change. During a user-initiated software installation for example, you would usually allow this change. If this happens while surfing the web or without any intended system changes, you should be careful.

Dictionary

The dictionary contains some explanations of common terms when dealing with malware.

Dialer

Dictionary

A dialer is a very small program, often installed using the ActiveX technology. Dialers often promise access to free porn, free games or free cracks for commercial software. Once installed, a dialer offers to use your dial-up device to call in to the service, usually calling a quite expensive phone number. Some dialers explain the costs of the connection they will be making, since it is required by local law in some countries, but many dialers just display a button offering to connect, without informing the user of what is happening behind it. In the worst case, the dialer sets up the expensive number as the default Internet connection, meaning the user will have to pay high rates for being online, without even knowing it until receiving the next high phone bill.

Firewall

Dictionary

A firewall is basically some kind of software or hardware that controls data transfers. The typical use of a firewall would be to secure the access a computer or a network of computers to another network (which may even be the internet). A hardware firewall is simply a box that is put between the local and the far network and that allows or denies transfers based on predefined rules; a software firewall is a software installed on a computer and basically does the same. It has the advantage that it can also set rules based on the software that is doing the transfer, but the disadvantage that it depends on how wise the user uses it.

Browser hijacker

Dictionary

A browser hijacker is a small program or registry setting that is responsible for changed IE start and search pages. If your browser starts with a different start page (one you have not changed yourself), you most probably got hijacked. Intelligent hijackers do not only change these pages, but also add a small file that will restore the hijacked settings upon each system start. Hijackers often use <u>ActiveX</u> installation programs and/or security holes.

Java applet

Dictionary

A Java applet is capable of doing more than just a JavaScript, but hasn't got the full access to your machine like a full Java application. An applet still needs the browser to be run in, while a full Java application could run stand-alone (using just the runtime engine).

Java Script

Dictionary

A Java script is a very small program that is running on your computer when visiting websites that have defined such a script. Java scripts have little access to your computer, but can modify your browser.

Keylogger

Dictionary

The name keylogger was defined back in old DOS times, where computers were handled just by using a keyboard. The most basic keyloggers back from that time just log the keys you press. The spy, a person with physical access to your machine, could get that log at a later point and see everything you typed.

Modern keyloggers are much improved. They do not only log the keys you press, but do also make screenshots to show the spy what Windows you are working with, they capture information about your internet use, and much more. The spy does not even need physical access to your machine because many current keyloggers send their logs by email.

Passwords

Dictionary

You surely know what a password is. When accessing private data on a protected system, you need a password (sometimes also called passphrase) and most often a username to tell the system your identity.

Most things about passwords have already been said, but some things cannot be repeated too often.

- 1. Do not tell your passwords to anyone. If you are asked by anyone to tell them your password, say no. There simply is no reason. If someone tells you he is an admin and needs to know your password, he is lying.
- 2. When choosing your password, do not choose something that others could simply guess. Do not use the name of your spouse or cat, or the company name printed on your computer or monitor. While the best thing would be a random string of characters and numbers and even special characters, if you really need something that is easy to remember, take parts of words and combine them into something that you can still speak, but that gives no sense. Attach a few numbers to it to be on the safer side.
- 3. Do not write your password down on a sticky attached to your screen, or anywhere on your workspace. If you need to write it down, put the paper with it into your wallet, but never anywhere near the computer.
- 4. Do not save a file with all your passwords on your computer. If you cannot remember them all, write them down. If you really want to save them in a file, encrypt that file.

Trojan horses

Dictionary

Even though a trojan horse is sometimes also called Trojan, it is more a Greek. The Greeks built the so-called "trojan horse" in the fight about Troja to get into the town, so they are the real snoops ;)

A trojan is a program that has gotten onto your machine without your knowledge and contains malicious code, that would for example allow persons using another computer to connect to yours over a network. Typical trojans are open to anyone trying to connect (any person on your local network or even the internet). Special trojans are designed to make your machine accessible just to the person who infected your computer with the trojan.

The access an outsider can gain using a trojan on your machine can be nearly anything. From watching all your behaviour (like a <u>keylogger</u>), manipulating your computer to basically doing anything you can also do using your keyboard and mouse.

Your computer can get infected with a trojan by multiple ways. A person with physical access to your machine can place it there, but you can also accidentally install it yourself by opening an unknown email attachment that by chance contains a trojan.

According to some definitions, trojans are also programs that sneak into other programs, for example to gain access. As these programs are consciously used by the other, they are not trojans, but are *backdoors*.

General questions

- <u>Why is Spybot-S&D; that fast?</u>
- How can I contribute to the cause?
- Where are features like the *Tools* or *Settings* section?
- What is *blindman.exe* for?
- <u>Are there any command line parameters?</u>
- <u>I have two installations on my hard disk. Can I scan both at the same time?</u>
- How can I get Administrator rights under Windows Vista?
- <u>Is Spybot-S&D; compatible with WinPE/BartPE bootable CDs?</u>
- Which browsers does Spybot-S&D; support?
- <u>Is Spybot-S&D; compatible with other resident protection tools?</u>
- What is the immunization feature and what are the other permanent protection options?
- What is new at Spybot-S&D; 1.5?

Updates

- What files do I need to update?
- Why is the integrated update not working?
- Why do I receive the message "update is forbidden" / "bad checksum!!!"?
- Why does Spybot-S&D; freeze up on update?
- Why do I receive a "Socket Error"?

Detections

- Why does Spybot-S&D; also remove IE toolbars that seem useful to me?
- Why do other spyware programs find spies in Sypbot-S&D;'s directory?
- <u>Why can I not remove the *Sti_Trace.log* (or *SchedLgU.txt*) file?</u>
- <u>Why do I receive ads titled "Messenger Service", although Spybot-S&D;</u> <u>cannot find anything?</u>
- Why does Spybot-S&D; find so many Spyware installers / how is that Download directories setting used?

- Why do other anti-spyware applications detect so many more tracking cookies?
- <u>Why does Spybot-S&D; not detect running processes?</u>
- Why does MS AntiSpyware complain that Spybot-S&D; adds bad sites to the trusted zone?
- <u>Why does Spybot-S&D; flag changes in the Windows Security Center?</u>

Bugs and problems

- <u>What should I do if my internet programs stopped working?</u>
- Why does my network react very slowly after inserting the Hosts File?
- Why are there some items left to immunize?
- Why has the number of scanned items been reduced (and now searches for only a few items)?
- What can I do if Spybot-S&D; flashes and disappears immediately?
- Why can I no longer access my IE settings?
- <u>Why does Spybot-S&D; not scan network drives (shares)?</u>
- <u>How can I disable the notifications popping up when a download was</u> <u>blocked (e.g. Avenue A, Inc., DoubleClick)?</u>
- Why are some products set to be ignored by default?
- <u>What can I do if Spybot-S&D; freezes during scan?</u>

TeaTimer

- How do I edit the Black & White list in resident TeaTimer?
- How do I disable the TeaTimer notifications?
- What is the Resident TeaTimer?
- Why does Resident TeaTimer terminate the application before asking?
- Why is TeaTimer called *TeaTimer*?

Error Messages

- Why do I receive the error message that there is a problem in *Hijackers.sbi* and I should look into the *Include errors.log* file?
- Why do I receive the error message "*ws2_32.dll* missing, EReadError"? / Does Spybot not run under Windows 95?
- <u>Why do I receive the error message "No Zip File specified" when I update</u> or fix?

- <u>Why do I receive the error message "framedyn.dll is missing"?</u>
- Why do I receive the error message "Problems in the include file (*Trojans.sbi*)"?

Why is Spybot-S&D that fast?

FAQ #001

There are different ways to search for spies. One would be to search the complete registry and hard disk for suspicious entries and files. That can take a lot of time.

Spybot-S&D takes advantage of the fact that all spies have to anchor themselves at a few places over the system to get active. It starts to search at this places, following the information gathered there to catch the whole spy.
Why does Spybot-S&D; also remove IE toolbars that seem useful to FAQ #002

Nearly all IE toolbars have something in common: they want to make the web easier for you. Sadly, to tailor their information to your needs, they need to collect data about you; and most privacy statements are unclear about how they do use this data beside sending you what they think is what you want.

What should I do if my internet programs stopped working? FAQ #003

If you remove a spy, the application that has installed it may notice this and refuse to work any longer. Spybot-S&D; is able to replace a few spies with harmless dummies; but where that is not possible, I recommend either to search for a good alternative that comes without spy- or adware, or using the recovery option in Spybot-S&D; to restore the spy. In the later case, you can do it step by step, until you found the files that are absolutely necessary for the spy, and at least keep some files from your system, like the data saved about you.



```
Why do other spyware programs find spies in Sypbot-S&D;'sFAQdirectory?#004
```

Please look at the path where such a program found the spyware. As Spybot-S&D has no spyware integrated, this must be a false alarm.

The reason for such a false alarm is simple: Spybot-S&D saves backups of the problems you have fixed; to make it possible to recover them in case something stops working after the fix.

If the file found is in the *Recovery* directory inside the Spybot-S&D directory, it is such a backup. It is no longer of any harm there, as the file will not be found and loaded from there. But once you are sure you do not need the backup, go to the Recovery section inside Spybot-S&D and purge that files.

Current versions compress the recovery files into password-protected zip archives, thus avoiding other spyware applications will give false alarms. Some programs might notify you that they cannot access these zip archives - this can easily be ignored. As the recovery files are named after the threat some programs might also naively detect the backups as threats just because of the file name. This can also be ignored.

In recent weeks there was a noticeably high number of cases where other antivirus and anti-spyware programs wrongly detected parts of Spybot-S&D, which probably has to be traced back to insufficient testing at these companies.

How do I edit the Black & White list in resident TeaTimer? FAQ #005

Please right-click the *Resident* icon in the system tray *Spybot S&D resident* and select *Settings*. There you will find four lists for remembered decisions (allowed/denied processes and registry changes). In order to remove an entry, just click on the cross next to it. TeaTimer will then "forget" this decision and you will be asked again the next time.

Why can I not remove the *Sti_Trace.log* (or *SchedLgU.txt*) file? FAQ #006

The *Sti_Trace.log* file is opened on many machines; most often on Windows ME/2000/XP/Vista. The reason is that the *Still Image Monitor* runs all the time, using this file. You can use *msconfig* to disable the Still Image Monitor, but as it is of no harm I would suggest to add this log file to the single ignore list.

The same is valid for the *SchedLgU.txt*; it is the log file of the scheduler. If the scheduler is running, this file is kept open. If you are not using the scheduler, I suggest disabling it, this will not only allow you to back up this file, but also save some RAM.

(To add a problem to the single ignore list, simply right-click on it in the results list, and choose the appropriate menu item.)

Why do I receive the error message that there is a problem inFAQ*Hijackers.sbi* and I should look into the *Include errors.log* file?#007

This error usually is the result of updates you have missed or installed only partially. To solve the problem, please install all updates checked by default at least, if not all. If you do not want to use the update function of Spybot - S&D;, take a look at the <u>download page</u> (online link) here and download all manual updaters.

The background of this problem are extensions to the detection engine which provide new ways of detecting malware. These updates are usually labeled *Plugin*, contrary to the weekly *Detection update*, and might therefore be overlooked. Since version 1.4 Spybot-S&D; and later allow you to hide these messages, but this is generally not recommended since missing plugins might mean missing or reduced chances to find the newest malware.

How do I disable the TeaTimer notifications?

FAQ #008

The reason why TeaTimer asked you is because it would ask you about any similar changes in the registry without regarding if it is good or bad. There are so many registry keys that it is impossible to classify them by default. So the user has to decide if he wants to allow it or not. The TeaTimer is making snapshot files when you start it the first time and the tool is comparing the current registry with the snapshot files.

If you want to make new snapshot files please shutdown the TeaTimer with the *Resident* icon and then start it manually from the Spybot S&D program folder. There is no possibility yet to hide the popups which remind you which keys are blocked. As a workaround, you can only make new snapshot files.

What files do I need to update?

FAQ #009

Updates can be divided into the following categories usually:

- 1. Detection updates and plugins: these updates are usually preselected when you use the updater, it is highly recommended to download them whenever there are updates available, since these are responsible for the detection rate. These are usually named *Detection rules, Advanced detection library, Detection support library* or *Some plugin*.
- 2. Localized updates: language files and localized product information. These files are not necessary if you use Spybot-S&D; exclusively in English. If you use only one other language, you just need your local ones.
- 3. Beta updates: if you are willing to help us improve Spybot-S&D;, you might download these as well. Do not forget the usual beta disclaimer though: there might be a bunch of new features, but there is also the risk of new bugs.
- 4. Malware documentation and help updates: as the name already indicates, these are for those who like to read up some information, on malware and on Spybot-S&D.;
- 5. Full updates: rare, but when a new release comes out, it will usually be available through the updater.

The second and third option are not displayed by default; in version 1.4 you can enable these categories on the settings page, version 1.5 has two checkboxes for them on the start page of the new updater application.

Why is the integrated update not working?

The main reason for this problem is that you need to use a proxy server to access the internet. In that case, the proxy server is already set up in your browser, where you can look up its settings and enter them into Spybot-S&D.;

- In Mozilla, you can find the Proxy settings if you open the *Edit* menu, choose *Settings*... at the bottom, and navigate to the section *Advanced Proxies*.
- In Internet Explorer, see the Menu *Extras Internet options*, go to the tab *Connections* and click the *Settings* button at the bottom.
- In Opera, see the Menu *Tools Preferences*, go to the tab *Advanced*, section *Network* and click the *Proxy servers* button. Look for the *HTTP* proxy there.

Back inside Spybot-S&D; go to the *Advanced Mode* (via menu *Mode*), then choose *Settings* \rightarrow *Settings*, and scroll down to the entry *Automation* - *Web update* - *Use proxy*. Now check the box below it, and a dialog will appear where you can enter your proxy settings.

The format is *host:port* (the host is the name, the port the number you found in your browser). If you need to access your proxy using a login, you can use the format *username:password@host:port*.

```
Why do receive the error message "ws2_32.dll missing" (and others)? FAQ# 011
```

Spybot - Search & Destroy 1.4 was incompatible with Windows 95, while version 1.3 or earlier and version 1.5 and later are compatible. However, the lack of following updates usually causes problems (all following links are online links):

• <u>HTML Help 1.3</u>

If you receive the message "*Error message: HHCTRL.OCX is missing*", you are probably using an old version of Internet Explorer, thus the needed HTML help components are not installed.

• <u>Winsock2</u>

If you receive the message *"Error message: WS2_32.DLL is missing"*, you need a Winsock update for Windows 95. More information is available in Microsoft's <u>knowledgebase</u>.

• <u>Active Accessibility 1.3</u> Spybot-S&D; tries to support solutions for disabled people, so you need to install the Active Accessibility runtime package if you receive complaints about problems in *oleacc.dll*.

<u>Common Controls</u>

Spybot-S&D; might also need this update if things are not probably displayed or you receive messages about other missing functions.

• Shell Folders

If you are running one of the older Windows 95 releases and do not even have Internet Explorer 4, you need this update for a newer *SHFolder.dll*, which is responsible for the *Application Data* folder used by many applications to store data.

We recommend these updates to any Windows 95 anyway, and we have included an option to download and install missing updates in the installer of Spybot-S&D; 1.5.

Why does my network react very slowly after inserting the Hosts FAQ #012

Please read <u>this article</u> (online link).

Why do I receive ads titled "Messenger Service", although Spybot-FAQS&D; cannot find anything?#013

These are sent using the Messenger service integrated into Windows 2000 and XP (try the *net send* command to see for yourself).

To disable the Messenger service, go to *Start* \rightarrow *All Programs* \rightarrow *Administrative Tools* \rightarrow *Services*. In *Services*, click on *Services* (*Local*), then on the right side, find *Messenger* and disable it.

Note: not everyone will have *Administrative Tools* in the *Start* menu. You need to make it visible under *Taskbar and Start Menu Properties* (right-click on taskbar \rightarrow *Properties*). The safest way to get to *Component Services* is to enter %systemroot%\system32\com\comexp.msc into the command line.

Why does Spybot-S&D; find so many Spyware installers / how is thatFAQDownload directories setting used?#015

Detection of files that might be found in variable locations,typically the installer archives of malware, is sometimes optimized by combining their lookup, in which case they receive this generic name.

The *Download directories* setting can be used to put special attention for such files on folders you use for incoming files. Spybot-S&D 1.5 also adds a few guessed locations to this internally to reduce the risk of forgetting standard download folders.

It is unnecessary, even counterproductive, to add whole drives to this setting!

Why are there some items left to immunize?

FAQ #017

If you are not immunizing with full administrator rights, Spybot-S&D might not have permission to immunize all user accounts.

If you are using Windows Vista, you should also read <u>this FAQ entry</u> about getting Administrator rights under Vista.

Why do I receive the error message "No Zip File specified" when I FAQ update or fix? #018

This happens if you have ZipMagic from Aladdin Systems (to my knowledge it came from Ontrack before) installed. ZipMagic displays all zip files as folders, and even denies other applications access to the real zip file.

To allow another application direct access to zip files, ZipMagic has a setting somewhere on its Options page. You need to add *SpybotSD.exe* there. Instructions from kind user follow:

- 1. Open the ZipMagic properties,
- 2. Click on the icon *Applications* at the left.
- 3. Check the option *These applications see Zip files as files*,
- 4. Press the *Add*... button, and
- 5. Select the SpybotSD executable in the dialog appearing (usually *C:\Program files\Spybot Search & Destroy\SpybotSD.exe*).

This will tell ZipMagic to allow Spybot-S&D; access to zip files again.

How can I contribute to the cause?

FAQ #019

As you may have read, we are working full-time on this free project, but we have got to pay hosting bills and development software. So we would be glad if you could <u>donate a small amount</u> (online link) to our cause. Thank you :-)

Where are features like the *Tools* or *Settings* section? FAQ #021

If you have a fresh installation of Spybot-S&D, you may miss some functions like the *Tools* or *Settings* section. They have not vanished but Spybot-S&D has two different modes. From the menu bar item *Mode* you can choose between *Default Mode* with the basic functions and *Advanced Mode* where you will find the *Tools* and the *Settings* section.

Why has the number of scanned items been reduced (and now searches FAQ for only a few items)? #022

Please run Spybot - Search&Destroy; and switch to *Advanced mode* via the menu bar item *Mode*, then select *Settings* \rightarrow *File Sets* in the left bar.

There, please right-click somewhere into the list and choose *Select all available checks*.

What can I do if Spybot-S&D; flashes and disappears immediately? FAQ #023

This might happen if you enable all of the *Program automation* settings. While version 1.5 should not allow you to lock yourself out this way, here are instructions on how to revert this, e.g. for older versions:

- 1. You can delete the configuration file (which is named *Configuration.ini*). Where it is located depends on your Windows version.
 - For Windows 95/98, the file is located in *C:\Windows\Application Data\Spybot Search & Destroy\.*
 - For Windows ME, the file is located in *C*:\Windows\All Users\Application Data\Spybot Search & Destroy\.
 - For Windows NT/2000/XP, the file is located in *C*:\Documents and Settings\All Users\Application Data\Spybot Search & Destroy\.
 - For Windows Vista, the file is located in *C:\ProgramData\Spybot Search & Destroy*.

Either delete that file, or edit it (for example in *notepad*), and set all the Automation values in it to zero.

2. You can download a small tool that will do those changes for you: <u>click</u> <u>here</u> (online link).

If this does not fix the problem, your system is possibly infected by the CoolWWWSearch.SmartKiller (v1 and v2). This is a new, really ugly variant of CoolWWWSearch. When running, it will close every browser window visiting an anti-spyware-site. It will even close Spybot-S&D; and some other anti-spyware applications as well.

So if your copy of Spybot-S&D; (or the anti-spyware application of your choice) closes a few seconds after starting, or your browser closes whenever you try to visit an anti-spyware site, check our <u>CWS.SmartKiller</u> removal utility (online link).

Why can I no longer access my IE settings?

FAQ #024

Internet Explorer tells you to contact your administrator when you try to access the IE settings?

This can happen if you use Spybot-S&D in advanced mode and you have used the Immunize feature without reading all the text.

- 1. Please start Spybot-S&D again in advanced mode (usually from the Start menu group *Spybot Search & Destroy*, until you have already changed the desktop icon to advanced mode).
- 2. Select *Tools* in the left bar, then *IE tweaks*.
- 3. There you will see a group *Recommended miscellaneous locks*. Untick the checkboxes in front of both *Lock IE*... options.
- 4. You may need to close all Explorer windows, and maybe even restart Windows before these changes take place.

Hint: this lock function has been added mostly for multi-user environments where you would not want other users of your computer to change your IE settings. If you are the only user of your computer, there is no real need to enable them.

What is *blindman.exe* for?

FAQ #025

Some of you may have noticed a new file *blindman.exe* inside the Spybot-S&D; folder, and have asked yourself what it is for. In short words: it does nothing.

I guess an explanation is needed why a file that does exactly nothing comes with Spybot-S&D.; Spybot-S&D; offers a tool to control the *System startup* in its *Tools* section. This includes the ability to disable or enable startup entries from the *Autostart* group (found in your Start menu under *Programs*). This group contains links to the actual files. Windows stores those links as files with the extension *.lnk*. When Windows encounters a **.lnk* file in that folder upon startup, it will start the linked application. Now the easiest way to disable those entries is to change the extension *.lnk* to *.disabled*. This easily prevents the linked application from being started. But as Windows does not know this extension, this could slow the startup down. So Spybot-S&D; does link that extension to *blindman.exe*. Windows now tries to run the *.disabled* file with *blindman.exe* - and as *blindman.exe* does exactly nothing, there is no slow-down in booting.

Some people have suspected it could even be spyware itself. For those I will print the Delphi source code (*blindman.dpr*) here (the included resource file is *blindman.res* and contains just the icon):

program blindman; {\$R *.res} begin end.

Anyone knowing a very small bit of programming should see that this program is totally harmless (actually, the version shipped with Spybot-S&D; 1.5 is a bit larger than the above, because one of Microsofts certification requirements is that every executable file need to call *GetVersionEx* at least once, and needs to

crash on inserted injections, even if just a 1 millisecond empty dummy).

Why does Spybot-S&D; not scan network drives (shares)? FAQ #026

Scanning network shares sounds like a good idea at first - the scanner needs to be installed only on a single machine and one person can do the scan. To simply remove installers, this is not a bad idea at all, so Spybot-S&D allows to add network shares as well in its *Download directories* setting.

But scanning for and removing files on other computers can be dangerous as well. Most threats are not only files, but also linked by registry entries - removing just the files would cause the 'cleaned' Windows to produce a lot of errors. But while those messages may be harmless (and remote registry cleaning could at least be added for NT/2000/XP/Vista), there is an even worse case - some threats need to be removed by using API calls. Removing LSP hijackers by just deleting their file will disable the network access of the cleaned machine, and repairing LSPs by fixing the registry is not fail-safe either.

That is why an anti-spyware tool needs to be run on each machine. We are developing a client/server scanning system that will work in network environments.

Why do I receive an error message "*framedyn.dll* is missing"? FAQ #027

Please visit this <u>Microsort support page</u> (online link); you can download the file <u>here</u> (online link) for example. More information is available in our <u>forum</u> (online link).

Are there any command line parameters?

Here is a list of command line parameters that the Spybot-S&D main executable (*SpybotSD.exe*) supports:

• /taskbarhideRuns Spybot-S&D completely hidden (no window, no taskbar icon), so make absolutely sure you use it only in combination with */autoclose* (otherwise it would remain in memory sitting idle). Useful only in combination with */autocheck, /autoupdate* or */autoimmunize*, as it cannot be controlled when completely invisible.

• /minimized

Starts the window minimized.

• /uninstall

Uninstalls Spybot-S&D. This command line parameter is very outdated - **unins000.exe** should be used instead!

• /blinduser

Starts with support for blind users (special menus).

• /autoupdate

Does an update after starting the program.

• /autocheck

Starts scanning immediately.

- /autofix Fixes problems after scan.
- /autoclose

Closes program after it has scanned or updated.

• /autoimmunize

Runs the immunization at program start.

• /onlyspyware

Fixes only spyware (red) entries with */autofix*, leaving all usage tracks as they are.

• /easymode

Starts with easier interface for beginners.

• /createenglish

Updates the *English.sbl* language file with the newest texts; useful only for translators.

And here is a list of command line parameters that the Spybot-S&D installer (*spybotsd15.exe*) supports:

• /sp-

Will skip the first page of the installation wizard (*Do you wish to continue?* ...)

• /silent

Will display the progress during installation, but not the wizard.

- /verysilent Even the progress will not be shown. Errors etc. would still be shown.
- /surpressmsgboxes
 Will use standard actions for message boxes (no overwriting of files, cancelling where the alternative would be retrying...)
- /log (or /log="filename")
 Creates a log file in the temp folder that contains detailed information about actions taking place during the installation.
- /nocancel

Disables the Cancel and Close button. Useful with /silent.

- /norestart Suppress reboots even if they were necessary at the end of the installation.
- /restartexitcode=N
 If a restart is needed, the setup would return the specified exit code.
- /loadinf="filename" (and /saveinf="filename")
 Can be used to use a saved setup configuration (or save one).
- /lang=language Overrides the language dialog with a predefined language. Use ISO 2 letter language describers here.
- /dir="x:\dirname"

Installs into that directory instead of the default one.

• /group="folder name"

Installs into a program group of that name instead of the default one.

• /noicons

Avoids creation of any icons for the installed software.

• /type=typename

Starts installation with a give type. Supported types are

- full,
- *blind* and
- compact.
- /components="comma separated list of component names"

Installs the given components instead of the default ones. Supported components are

- main,
- *blind* (icons for blind users),
- *language* (all language files),
- skins,
- *updatedl* (for downloading updates as part of the installation),
- *updatew95* (to download prerequisites on Windows 95),
- *SDWinSec* (to install the Security Center integration on Vista),
- SDShredder (to install the stand-alone shredder), and
- *SDDelFile* (to install the file removal helper).

• /tasks="comma separated list of tasks"

Specifies a list of tasks that should be executed. Tasks currently supported are:

- desktopicon
- quicklaunchicon
- launchsdhelper
- launchteatimer

• /mergetasks="comma separated list of tasks"

Same as /tasks, just with the exception that standard tasks are not disabled by default.

Note: Please be aware that the Spybot-S&D path has to be in quotation marks and multiple parameters have to be separated by a space.

Example: "C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe" /taskbarhide /autoclose /autocheck /autofix /onlyspyware

Why does Spybot-S&D; freeze up on update? FAQ #032

Spybot-S&D; can be freezed up if the servers are reacting very slowly. This often happens the day new updates are released, when too many people try to download them at the same time - it is just delayed though and very slow in reacting. There are a few possible solutions for this problem:

- 1. Wait a minute, it should be active again.
- 2. Select a different download location: After *Search for update*, you can select another mirror in the toolbar. To do that, click the small arrow next to the currently selected mirror name.
- 3. Please try again later.

Information about updating is also available in our section <u>How to</u> (online link; includes a screenshot); take a look at point 5 of this description that shows you how to select a different download location.

What is the Resident TeaTimer?

FAQ #033

The Resident TeaTimer is a tool of Spybot-S&D; which perpetually monitors the processes called/initiated. It immediately detects known malicious processes wanting to start and terminates them giving you some options, how to deal with this process in the future. You can set TeaTimer to:

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

There is also an option to delete the file associated with this process.

In addition, TeaTimer detects when something wants to change some critical registry keys. TeaTimer can protect you against such changes again giving you an option: You can either *Allow* or *Deny* the change.

As TeaTimer is always running in the background, it takes some resources of about 5 MB.

Why does Resident TeaTimer terminate the application beforeFAQasking?#034

Because threats like toll dialers are time critical - they cost from the first second they have connected. In order to protect you, these have to be terminated before they can connect at all, at the moment they appear.

Why is TeaTimer called *TeaTimer*?

FAQ #035

As we used to forget our tea when we let it brew, we built a small tool with a system tray icon to remind us. We called this tool *TeaTimer*.

When we started to develop the Resident tool for Spybot-S&D, we also needed a system tray icon for this. As we do not like having too many icons in the system tray, we decided to put both tools together and kept the name *TeaTimer*.

A future version of the Resident tool might have the functions of the original *TeaTimer* again.

Why do other anti-spyware applications detect so many more	FAQ
tracking cookies?	#037

Some anti-spyware applications have started to detect nearly every third-party cookie they find as a tracking cookie. In many cases, that is more or less correct, since many contain a GUID (Generic Unique Identifier).

But instead of bloating our detection database with thousands of cookies out there, we prefer recommending to change your browser settings a bit to block out all these third party cookies before they even come into your system (all following links are online links):

- **Internet Explorer:** Open "Internet Options..." from the "Tools" menu. Choose the "Privacy" tab, and raise the Settings to at least Medium; or use the "Advanced..." button to enabled "Override automatic cookie handling" and set "Third-party Cookies" to "Block". <u>Screenshot 1</u> <u>Screenshot 2</u>
- **Firefox 1.x:** Open "Options" from the "Tools" menu. Click the "Privacy" icon, and open the "Cookies" category. Under "Allow sites to set cookies", just set the "for the originating web site only" option. <u>Screenshot</u>
- **Firefox 2.0:** Type "about:config" into Firefox's address bar, then type "network.cookie.cookiebehavior" in the "Filter" box. That will leave one settings line visible; double-click it, type "1" in the "Enter integer value" box, then click OK.
- Mozilla/Netscape: Open "Preferences..." from the "Edit" menu. Open the category "Privacy & Security" and click on its first entry "Cookies". In the group "Cookie Acceptance Policy", select "Allow cookies for the originating web site only". Screenshot
- **Opera:** Open "Preferences" from the "Tools" menu. Click on "Privacy" in the list on the left, then open the pull-down list about "Third party cookies" on the right and set it to "Refuse all cookies". <u>Screenshot</u>
- **Opera 9:** Open "Preferences" from the "Tools" menu, go to "Advanced"

 \rightarrow "Cookies" and select "Accept cookies only from the site I visit.".

Do I need this FAQ?

FAQ #039

Before you read this FAQ or other support documents, we would recommend that you use the update function and see if you have the most current updates for Spybot-S&D; (we removed some FAQ entries for versions from last year or earlier to keep this FAQ easier to look through).

If you have, we hope to be able to help you either here, on the support forum or by email.
Why does Spybot-S&D; not detect running processes? FAQ #040

But it does! This is often misunderstood as we do not display an extra list of running processes after the scan. But we do not see that as necessary - every running process is identical to a file on the hard disk, because a process is more or less that file loaded into memory.

But when you use Spybot-S&D; to fix problems, it will automatically terminate the bad processes detected before doing anything else. And if you are using our TeaTimer, TeaTimer will detect malware processes as soon as they are started and terminate them.

Our logs of course do include a full list of processes, and since version 1.4 Spybot-S&D; even lists open network connections per process (except for on Vista), allowing you to easily see which processes are connecting to the outside and where to.

I have two installations on my hard disk. Can I scan both at the same FAQ time? #041

Yes, if you have Windows 2000, XP, 2003 or Vista, Spybot-S&D; does allow you to scan inactive Windows versions as well, including the registry of other installations!

To scan your system including installations on other partitions, right-click the link/icon you use to start Spybot-S&D;, and add */allhives* to the command line (separated by a space from the rest). If you now start Spybot-S&D; through this link, it will automatically detect other installations, and scan theirs registries and files as well.

How can I get Administrator rights under Windows Vista? FAQ #042

On Windows Vista, Spybot-S&D; might tell you that for some actions, you are not being allowed to operate them, since they would require administration elevation. You can solve this problem as follows:

- 1. Right-click the Spybot Search&Destroy; entry in your start menu, instead of just left-clicking to start it.
- 2. Choose Run as administrator from the context menu.

Is Spybot-S&D; compatible with WinPE/BartPE bootable CDs? FAQ #043

Yes, Spybot-S&D; has full support for PE in general and PEBuilder. You can download the necessary plugin for <u>version 1.4 here</u> (online link) or for <u>version 1.5 here</u> (online link), or run it from your harddisk after booting a PE disk.

Once run from your bootable PE CD, Spybot-S&D; will automatically scan all registry and drives it can find (if you want that feature without PE, see <u>this</u> <u>FAQ entry</u>.

How can I disable the notifications popping up when a download wasFAQblocked (e.g. Avenue A, Inc., DoubleClick)?#044

This message is created by the bad download blocker for IE, a tool of Spybot-S&D.; The feature of the silent bad download blocker in version 1.5 is in a different place than in older versions.

Please open the *Tools* menu in your Internet Explorer and choose *Spybot-S&D*; - *Configuration*. There you will find a drop down menu (see screenshot below) where you should select *Block all bad pages silently*. With that option set the notifications will no longer come up, but you will still have the protection.

New configuration for LF, plugin
rett comparation for 12 pragm

Why does MS AntiSpyware complain that Spybot-S&D; adds badFAQsites to the trusted zone?#045

That is a mistake by Microsoft. Microsoft has released <u>knowledge base article</u> <u>902956</u> (online link) that describes this problem of theirs.

Why does Spybot-S&D; flag changes in the Windows SecurityFAQCenter?#046

Spybot - Search & Destroy detects registry changes associated with Microsoft Security Center; they are listed as "Windows Security Center". This is neither a false positive nor a bug. It is just an information about a *potential* threat -Spybot-S&D only wants to bring to your attention that someone or something disabled one or more notifications in the Windows Security Center, e.g. the notifications that your virus protection is not active or not up-to-date.

If you changed the settings yourself you can safely tell Spybot-S&D to exclude those detections from further scans. In order to do so, please right-click each in turn, then click *Exclude this detection from further searches*. That way, should any other part of security center settings change, Spybot-S&D will still detect those. The same is true if you have another security solution installed (like McAfee Security Center or Norton Internet Security). These programs disable announcements of Window Security Center in order to signal things by themselves.

The reason why the changes are flagged by Spybot-S&D is that there are also malware programs that disable the notifications so the user does not take note of his security tools not being effective. Some more information is also available in our <u>forum</u> (online link).

Which browsers does Spybot-S&D; support?

Spybot-S&D; does support many common browsers. As for resident protection, Spybot-S&D; contains the Resident TeaTimer which is completely browser independent. It is a Spybot-S&D; tool perpetually monitoring the processes called/initiated. In addition, TeaTimer detects changes to some critical registry values.

Spybot-S&D; supports detection in cookies, history, start & search pages and bookmarks of these browsers plus cache for Internet Explorer and Opera (all following links are online links):

- <u>Beonex Communicator</u>
- Firefox pre-0.9, 0.9, 1.x, 2.0 and compatible, including old Firebird variants
- <u>K-Meleon</u>
- Microsoft Internet Explorer 5.0, 5.5, 6.0, 7.0
- <u>Mozilla Suite</u>
- Netscape Communicator 4.x, 6, 7
- <u>Opera</u> 4.x, 5.x, 6.x, 7.x, 8.x, 9.x and compatible
- <u>Thunderbird</u> 1.x and compatible (where applicable)

Is Spybot-S&D; compatible with other resident protection tools? FAQ #049

Using more than one anti-spyware program with a resident protection tool might cause conflicts. However, Spybot - Search & Destroy's Resident protection is designed such that there should not be any compatibility issues.

One thing that could appear is that another programm detects our TeaTimer as bad - because theoretically, it has the same function as a keylogger as it runs in the background. But only theoretically - it is a realtime protection tool for you and there is nothing bad about it.

Another issue could be that the Keylogger detection files *Keyloggers.sbi* and *Keyloggers.*.nfo* of Spybot-S&D; are detected as Activity Monitor keylogger. These detected keyloggers are just the Spybot-S&D; detection rules, which obviously need to contain the names of the threats. Please ignore these false positives.

For more information we created a <u>compatibility overview</u> (online link) listing some software for which there have been questions on compatibility.

One last thing could be that removed items which are now stored in the recovery area as zip files are being detected. The zip files are needed for the recovery. If something does not work after fixing a problem with Spybot-S&D; you can restore these files. So there is nothing bad with them, either.

What is the immunization feature and what are the other permanentFAQprotection options?#050

- Beginning with version 1.2, Spybot-S&D; has been allowing you to immunize your computer against some spyware. This has been extended in every further release, and tweaks browser settings to use their methods of blocking cookies, malware installations, bad websites and more.
- SDHelper is an Internet Explorer plugin that adds a second layer for blocking bad stuff.
- *Resident TeaTimer* is explained in <u>this FAQ entry</u>.

Why are some products set to be ignored by default?

FAQ #051

CDilla and SideStep are listed in the ignore products by default. Please see the topic <u>Why are CDilla & SideStep checked in Ignore Products?</u> (online link) in our forum.

What can I do if Spybot-S&D; freezes during scan?

This could be caused by several reasons like an old version of Spybot-S&D;, too much temporary files or problems with the system restore point.

In case you are using a dated version of Spybot-S&D;, as a first solution, please download the latest version of Spybot - Search & Destroy, which should fix the problem. You will find links to several download locations on our <u>homepage</u> (online link). Do not forget to use the integrated update after installing Spybot-S&D.;

If this does not help, please delete the contents of your Windows *temp* folder and try it again. Also, you might want to disable the *Create system restore point when fixing spyware/usage tracks* option on the settings page.

Why do I receive a "Socket Error"?

FAQ #053

Please take a look at the security settings of your firewall (if you are using one) and make sure that Spybot-S&D; is not blocked. That should help to get into the updates. If Spybot-S&D; is not blocked it is also possible that our server is temporarily not available. Please try again a few hours later.

If this does not help please download the <u>manual updaters here</u> (online link; here is also a <u>direct download link</u>). The manual updaters are self-installing, you just need to execute them.

Why do I receive the error message "Problems in the include fileFAQ(Trojans.sbi)"?#054

Please download the update called "TCP/IP Settings plugin" using the integrated update function, or, if you do not use the integrated update, you can download a manual installer from our <u>download page</u>.

If even after updating, the file is not there, you can try the following:

- 1. Close Spybot-S&D.;
- 2. Unzip (extract) the *plugtcpip.zip* file that is in your *Spybot-S&D*;*Updates* folder to the main Spybot-S&D; folder.
- 3. Restart Spybot-S&D.;

For more informations, please do also have a look at our <u>forum</u>.

What is new at Spybot-S&D; 1.5?

FAQ #055

An overview of the most important changes since version 1.5 of Spybot-S&D;:

System support

- Restored Win95 compatibility
- Improved Wine compatibility
- Fixed HyperThreading issues
- Improved 64 bit immunization
- Create *Portable.ini* in main folder to use app folder as data folder as well
- New warnings about missing admin rights on Windows Vista
- Support for multi-line bookmarks (IE 7 / Vista)
- New Immunization for Firefox & Mozilla
- Improved Immunization for Opera

Reports

- Added version info to bug report
- Include Errors.log now includes timestamps
- Improved Windows version display

Misc

- "Single excludes" now include filenames to be more unique
- Improved settings retrieval from registry (mixed installations)
- Fixed .reg import bugs
- Added support for automated removal of F/Ps from host lists
- Changed update UserAgent and Referrer
- Improved (Vista-compatible) support for fast user switching
- Updater now in separate executable file
- Vista manifests for assigning required rights to each application
- Deactivated list of active ports per process for Vista (incompatible)
- Fixed support for handle list on 64 bit systems

- Improved disabling/enabling BHOs
- New special error reporting for beta versions
- Support for Windows Error Reporting for public versions
- Fixed update-related crashes on Vista
- Fixed memory leaks (replaced Indy with Synapse)
- Vista-compatible MSI installer for those who like/need that
- Support for alpha tests on services and domains lists
- Added hundreds of new automated tests of internal functionality for prerelease QA
- Added TeaTimer hide icon (disabled) registry value in installer

Detection and removal of threats

- Improved PE detection all over the place
- New 64 bit detection all over the place
- Improved file removal methods
- Added optional custom RecoveryDir setting in Default.ini
- Automatic guessing of "Download Dir" folders
- Added support for renaming services before stopping/killing/deleting them
- Improved plugin support (example: current TCP/IP Plugin)
- Support for regular expressions nearly all over the SBI interface
- Much improved logic connections between files, registry and API detections (others would invent a new TLA for that *g*)
- Speed-ups through improved caches
- File version checking
- Authenticode checking
- Improved archives checking
- Faster fulltext checking
- Improved Sys Internals file location algo
- Improved hosts file location algo
- Added some more Opera 9 detection schemes

User interface changes

- Fixed "show more information" panels
- Implemented workarounds for misarranged buttons (including TeaTimer)
- Improved support for /allhives in tools section (inactive installation

support)

- Fixed flag shown on shortcut bar after changes
- Fixed IE proxy import in wizard
- Changed "use proxy" button to checkbox
- Improved localization on simple dialogs
- Added option to add a proxy inside app if running on Win PE
- Improved localization of list of updates
- Added Firefox icon on Cookie exclude page
- Fixed bad keyboard handling on some exclude lists
- Fixed cookie removal selection problems
- New confirmation dialog for system restore points
- Changed default font to Tahoma
- Red cross (trademarked) replaced with green cross
- Made "Check" option unavailable during fix
- Process list now is a bit less eager on tooltips
- Improved "delay start" dialogs
- Now displays checksum for each result for better trackback of results
- Fixed "Ignore Products" column width problems on Vista
- Improved localization of product descriptions
- Adjusted wizard for new situation (external updater etc.)
- Fixed Tools snapshot comparison highlighting
- Made display of registry changes in results list less confusing
- Improved SDHelper dialogs and block/allow choices
- Update date format on info page now localized
- Displayed app version is now four digits (e.g. 1.5.1.12)
- (De+)Select all in list of old reports
- Improved Warning/Confirmation dialog IE plugin
- Configuration & Information dialog in IE plugin

FAQ #056

Spybot-S&D; will uninstall from the Windows *Add/Remove Software* control panel without problems.

If you want to completely get rid of Spybot-S&D; 1.4 (also earlier versions) and the Add/Remove doesn't help, you can delete the installation folder (usually *C:\Program Files\Spybot - Search & Destroy*), then download <u>this</u> <u>very small fix</u> by right clicking and saving it, then execute it (important! - this will remove all remains from the registry).

If you just want to upgrade to a newer version, please follow the same instructions like above and then install the new version.

After following these instructions please restart your system so that the changes can take place.

Also, neither the automated uninstall nor the manual uninstall like described above will remove the following directories, which you will have to remove by hand:

- Windows 95 or 98: C:\Windows\Aplication Data\Spybot Search & Destroy\
- Windows ME: C:\Windows\All Users\Application Data\Spybot Search & Destroy\
- Windows NT, 2000 or XP: C:\Documents and Settings\All Users\Application Data\Spybot - Search & Destroy\
- Windows Vista: C:\ProgramData\Spybot Search & Destroy\.

(Please note that the *Application Data* Folder is hidden. So if you can't find this folder please check your folder properties.)

Explanation: this folder contains the backup (the quarantined files) that Spybot-S&D; creates. If the Uninstall would remove this folder as well, this would mean that those backups would be gone. We saw it a few times that new users uninstalled Spybot-S&D; in panic after they've experienced a small problem,

thus removing the backup that would have undone any changes.

Command line parameters

For large environments or people who want to control and automate everything themselves, here is a list of command line parameters of both the <u>installer</u> and <u>main executable</u> to make your work easier.

Main executable Command line parameters of *SpybotSD.exe*

Here is a list of command line parameters that the Spybot-S&D; main executable (*SpybotSD.exe*) supports:

/taskbarhideRuns Spybot-S&D; completely hidden (no window, no taskbar icon), so make absolutely sure you use it only in combination with /autoclose (otherwise it would remain in memory sitting idle). Useful only in combination with /autocheck, /autoupdate or /autoimmunize, as it cannot be controlled when completely invisible.

• /minimized

Starts the window minimized.

• /uninstall

Uninstalls Spybot-S&D.; This command line parameter is very outdated - **unins000.exe** should be used instead!

• /blinduser

Starts with support for blind users (special menus).

• /autoupdate

Does an update after starting the program.

• /autocheck

Starts scanning immediately.

- /autofix Fixes problems after scan.
- /autoclose

Closes program after it has scanned or updated.

• /autoimmunize

Runs the immunization at program start.

• /onlyspyware

Fixes only spyware (red) entries with */autofix*, leaving all usage tracks as they are.

• /easymode

Starts with easier interface for beginners.

• /createenglish

Updates the *English.sbl* language file with the newest texts; useful only for translators.

Note: Please be aware that the Spybot-S&D; path has to be in quotation marks and multiple parameters have to be separated by a space.

Example: "C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe" /taskbarhide /autoclose /autocheck /autofix /onlyspyware



Installer Command line parameters

Here is a list of command line parameters that the Spybot-S&D; installer supports:

- /**sp**-Will skip the first page of the installation wizard (*Do you wish to continue*? ...)
- /silent

Will display the progress during installation, but not the wizard.

- /verysilent Even the progress will not be shown. Errors etc. would still be shown.
- /surpressmsgboxes

Will use standard actions for message boxes (no overwriting of files, cancelling where the alternative would be retrying...)

- /log (or /log="filename") Creates a log file in the temp folder that contains detailed information about actions taking place during the installation.
- /nocancel

Disables the Cancel and Close button. Useful with /silent.

• /norestart

Suppress reboots even if they were necessary at the end of the installation.

- /restartexitcode=N
 If a restart is needed, the setup would return the specified exit code.
- /loadinf="filename" (and /saveinf="filename")

Can be used to use a saved setup configuration (or save one).

- /lang=language
 Overrides the language dialog with a predefined language. Use ISO 2 letter language describers here.
- /dir="x:\dirname" Installs into that directory instead of the default one.
- /group="folder name" Installs into a program group of that name instead of the default one.

/noicons
 Avoids creation of a

Avoids creation of any icons for the installed software.

• /type=typename

Starts installation with a give type. Supported types are

- full,
- *blind* and
- compact.

• /components="comma separated list of component names"

Installs the given components instead of the default ones. Supported components are

- ∘ main,
- *blind* (icons for blind users),
- *language* (all language files),
- skins,
- *updatedl* (for downloading updates as part of the installation),
- updatew95 (to download prerequisites on Windows 95),
- *SDWinSec* (to install the Security Center integration on Vista),
- *SDShredder* (to install the stand-alone shredder), and
- *SDDelFile* (to install the file removal helper).

• /tasks="comma separated list of tasks"

Specifies a list of tasks that should be executed. Tasks currently supported are:

- desktopicon
- quicklaunchicon
- launchsdhelper
- launchteatimer

• /mergetasks="comma separated list of tasks"

Same as /tasks, just with the exception that standard tasks are not disabled by default.

Why do I get an error message during updating that the update isFAQforbidden/bad checksum?#020

Some users have reported they are not able to download updates. The 'Search for updates' reveals updates, but they cannot be downloaded. Often a 'HTTP Error 403' or 'bad checksum' is displayed. This has a simple reason - thousands of people trying to download from the default server, which can't handle such a load. If you try again, have a second look at the menu bar. It has a pull-down item to select a mirror. Click the arrow beside it, and select a different location, where you'll most probably have better chances to download.

Current problems with the main installer download have the same reason - the servers not being able to handle such large amounts of downloads. Even the University isn't able to deal with many thousands of downloads at the same time. Please have some patience; more mirrors are being added again.