

Description

Spybot is an application designed for the removal of spyware, malware and other intrusive software.

Licence

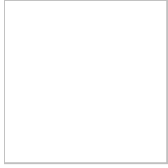
Spybot is only free to download for personal use. Business or other commercial users please refer to the End User [Licence Agreement](#).

Requirements

- Windows XP SP2 or later
- 512 MB RAM when used with Windows XP
- 1 GB RAM when used with Windows Vista or later
- 300 MB free hard disk space

FAQs

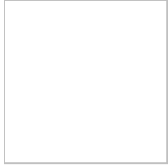
Visit the [website of Spybot](#) to get an answer for frequently asked questions.



Module Overview

One important change in Spybot is that the functionality is much more modularized. This has a lot of advantages, including:

- **Resources:** you do not need everything Spybot offers all at the same time. By loading only those parts you need when you need them, Spybot can run faster while it uses less system memory.
- **Speed:** the application will simply show much faster.
- **Interaction:** a challenge is to present it to the user in a way that is not affecting his ease of use; on the contrary, it should help him getting things done by presenting only what he currently needs, at the same time allowing him to easily go to another part.
- **Updates & Maintenance:** by having functionality separated, new functions or bug fixes mean that testing can concentrate on one module, and possibly those depending on it, but not on the full package, leading to faster and more stable updates.
- **Scripting/Scheduling:** if you want to automate things, you can restrict that to the modules that offer the functionality you want to script, without the need to load the full, slow loading old application all the time.



Boot CD

A boot CD can be used to start your computer from a read only medium that will allow malware detection and cleaning that is not influenced by any malware that your running system might be infected with. This is extremely useful when targetting rootkits that are able to hide on the active system; while Spybot is able to detect and remove many rootkits, this is the failsafe variant.

Availability

This module is available in the following editions:

- Professional
- Technician



Bootable CD

In some cases it can be helpful to repair a machine from a different system installation. A bootable CD is a useful device therefore.

© 2000-2013 Safer-Networking Ltd. All rights reserved.



Cleaner

The *Cleaner* module can remove malware where other approaches sometimes fail. On reboot it can clean using previous scan results eliminating the need to scan again. It can also use other cleaning mechanisms like the new WinLogon and Native Mode cleaners.

Available parameters

Basic

/help shows this page
/verbose displays more output

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar
/autoclean cleans problems from last scan
/autoclose close after cleaning

Supplemental Options

/youtube adds menu option to resize windows to YouTube video resolutions
/SDFiles starts the file scanner when user chooses to rescan
/forcereclean attempts to clean even items that have been previously cleaned

System Service related

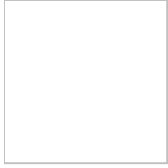
/serviceinstalltest fakes that services are not installed

Availability

This module is available in the following editions:

- Free
- Home

- Professional
- Corporate
- Technician



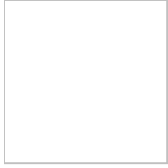
Disconnecting from the Internet while cleaning malware

In order to prevent re-infection during cleaning Spybot may offer to disconnect you from the Internet. The connection will be restored within a minute after cleaning or after a reboot.

If you accept the offer to disconnect from the Internet while downloading data, the data will be lost.

Helpful Hint

It is recommended that you accept this offer as otherwise re-infection can occur.



Offer to elevate privileges during cleaning

Malware can infect any part of a system, even if the user does not have administrator privileges. When scanning a system as a regular user, or on Vista or later as an administrator without elevated privileges, the user might not have sufficient rights to remove some malware. In these cases, Spybot offers to elevate the [Cleaner](#) to full administrator privileges.

Helpful Hint

Please choose the options below that describe your situation.

- I am using Windows Vista or later.
- This computer has other users.
- You are the first user to set up this computer.
- Your account is an administrator account.
- You have the password of an administrator account.

Please describe your situations by clicking the checkboxes above.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\).](#)

[Microsoft Windows 7: User Account Control \(UAC\).](#)

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)



File Remover

The *File Remover* can delete files that might not be removed by conventional methods.

Available parameters

Basic

/help shows this page
/verbose displays more output

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar

System Service related

/serviceinstalltest fakes that services are not installed

Supplemental Options

/youtube adds menu option to resize windows to YouTube video
resolutions

Options

/ask requests the users confirmation on file removal
/deep use malware removal methods to delete file
/silent output reduction for automated use

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician

© 2000-2013 Safer-Networking Ltd. All rights reserved.



File Scan

The *File Scan* allows you to scan selected files without having to do a complete system scan. It can be accessed in different ways:

- If Explorer integration is installed, by right-clicking any file or folder in Windows Explorer.
- If AutoPlay integration is installed, by selecting the *Spybot* option when connecting devices like USB sticks.
- By dragging files onto the File Scan icon.
- By dragging files into the File Scan open window.

It also [offers to clean files](#) if something is identified.

Available parameters

Basic

/help	shows this page
/verbose	displays more output
/opendialog	starts with an open dialog to choose files to scan from
/showanomalies	shows anomalies for scanned files
/hideanomalies	hides anomalies for scanned files

Automation

/silent	avoid unnecessary output
/taskbarhide	avoid UI appearing even in the taskbar

System Service related

/serviceinstalltest	fakes that services are not installed
/nosystemservice	loads services in memory instead of as a system service if possible

Supplemental Options

/youtube	adds menu option to resize windows to YouTube video resolutions
----------	---

Setup

/register	registers into context menu
/unregister	unregisters from context menu
/registerautoplay	registers into autoplay options
/unregisterautoplay	unregisters from autoplay options

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician

Additional resources

[You can find more information about this module in our forum by clicking here.](#)



Explorer integration: installation

Spybot integrates itself into the context menu of Windows Explorer for files and folders by default. You can change this on the *System Integration* tab of [Settings](#).

Helpful Hint

This dialog will only show you those options that apply to your current privilege level. For example on Vista or later, it might offer you [elevation](#).

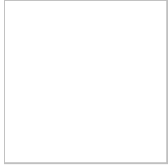
If you are the only user of this system, choose the 'global' otherwise choose 'current user'. If you are not the only user of the system please consult the other users before making changes.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\)](#).

[Microsoft Windows 7: User Account Control \(UAC\)](#).

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)



Explorer integration: removal

Spybot integrates itself into the context menu of Windows Explorer for files and folders by default. You can change this on the *System Integration* tab of [Settings](#).

Helpful Hint

This dialog will only show you those options that apply to your current privilege level. For example on Vista or later, it might offer you [elevation](#).

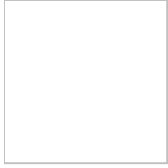
If you are the only user of this system, choose the 'global' option otherwise choose 'current user'. If you are not the only user of the system please consult the other users before making changes.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\)](#).

[Microsoft Windows 7: User Account Control \(UAC\)](#).

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)



AutoPlay integration: installation

Spybot can integrate into Explorers 'AutoPlay' dialogs. It will offer to scan removable drives, USB sticks etc. when they are attached to the system. This integration can be selected during installation, on the *System Integration* tab of [Settings](#). Depending on privileges, this can be installed for 'all users', or for the 'user only' account.

Helpful Hint

This dialog will only show you those options that apply to your current privilege level. For example on Vista or later, it might offer you [elevation](#).

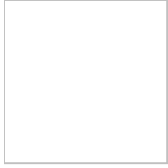
If you are the only user of this system, choose the 'global' option otherwise choose 'current user'. If you are not the only user of the system please consult the other users before making changes.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\).](#)

[Microsoft Windows 7: User Account Control \(UAC\).](#)

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)



AutoPlay integration: removal

Spybot can integrate into Explorers 'AutoPlay' dialogs. It will offer to scan removable drives, USB sticks etc. when they are attached to the system. This integration is selected by default during installation, you can disable it later on the *System Integration* tab of the [Settings](#).

Helpful Hint

This dialog will only show you those options that apply to your current privilege level. For example on Vista or later, it might offer you [elevation](#).

If you are the only user of this system, choose the 'global' option otherwise choose 'current user'. If you are not the only user of the system please consult the other users before making changes.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\).](#)

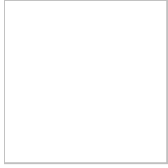
[Microsoft Windows 7: User Account Control \(UAC\).](#)

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)



Queue size warning

If the number of files chosen to be scanned is too large [File Scan](#) will issue a warning. If this happens you are advised to use the *Scan the system* option.



File Scan offers to start cleaning

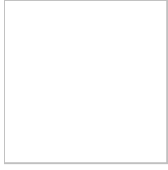
If the [File Scan](#) suspects a file, this dialog offers to start the [Cleaner](#) to remove these files.

Helpful Hint

The [File Scan](#) does heuristic scans as well as malware and virus scans. This can cause false positives. If you are in doubt about a file, you can request help on our [support forum](#).

Additional resources

[Safer Networking Forums](#)



Malware found

This dialog tells you that an application has been identified as harmful by Spybot. It offers to block this application and is able to show detailed information about the file.



Scan progress

This dialog shows which file is currently being scanned.





Immunization

Immunization pro-actively prevents malware from attacking your system. It does this by blocking access to sites known to contain malicious or unwanted software using a blacklist, if your browser supports this feature.

Available parameters

Basic

/help	shows this page
/verbose	displays more output
/savelog	stores a log to help tracking errors
/debuginfo	saves details about immunization for support cases

Available Operations

you need to specify one of these

/scan	test the current grade of immunization
/immunize	applies immunization
/undo	removes the immunization

Automation

/silent	avoid unnecessary output
/taskbarhide	avoid UI appearing even in the taskbar

System Service related

/serviceinstalltest	fakes that services are not installed
---------------------	---------------------------------------

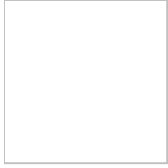
Supplemental Options

/youtube	adds menu option to resize windows to YouTube video resolutions
/noscan	does not check anything at program start
/autoclose	close user interface after chosen operation has finished

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician

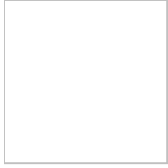


Immunization warning on open browsers

If a browser is opened, it already has the current immunization lists in memory, and might commit an old state back to disk when it is closed. It is therefore recommended to close the browser or browsers displayed in this dialog before taking any immunization action.

Helpful Hint

Immunization is intended as a pro-active action, which means it is not time critical. Better to complete anything you're currently working on in your open browser windows before continuing to immunize, than having an incomplete immunization result.



Typical Immunization issues

Users of Vista or later

With Vista or later, [Immunization](#) has to be run with elevated privileges, otherwise all global immunizations will fail. To elevate your privileges, right-click the [Immunization](#) shortcut and choose *Run as Administrator*.

Normally Spybot will offer to run the [Immunization](#) with elevated privileges. If a user has chosen not to display this dialog, it can be re-enabled using the *Dialogs* tab of the *Settings* window.

Computer Associates software users

Computer Associates Anti-Spyware for Yahoo! blocks some immunization entries in the category *Internet Explorer (32/64 bit)*. One such domain is *koolynoody.net*.

CA AntiVirus 8.4.0 has been known to block a larger amount of entries.

More information about this can be found on our support forums in threads tagged [immunization vs. ca](#).

AVG Antivirus users

AVG Antivirus blocks immunization of about 30 to 120 entries in the *Internet Explorer* category.

More information about this can be found on our support forums in threads tagged [immunization vs. avg](#).

ZoneAlarm users

ZoneAlarm blocks all immunization in the area *Windows: Global (Hosts)* by protecting this file against changes. To overcome this protection, you must

unlock using the ZoneAlarms *Firewall > Advanced* tab. Don't forget to relock it after immunization.

More information about this can be found on our support forums in threads tagged [immunization vs. za](#).

STOPzilla users

STOPzilla blocks all immunization in the area *Windows: Global (Hosts)* by protecting this file against changes. To overcome this protection, you must allow changes to be made. To do so:

1. Open Stopzilla
2. Click "Real-time Protection"
3. Click "Active Enforcers"
4. Click "Network"
5. Click "Hosts File" to uncheck it
6. Click "Apply"
7. Click "OK"

Do not forget to reverse this procedure after you've completed immunization. We would like to thank forum user michaelbmcgee for these instructions

More information about this can be found on our support forums in threads [immunization vs. stopz](#).

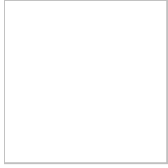
Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\)](#).

[Microsoft Windows 7: User Account Control \(UAC\)](#).

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)

[More discussions about this dialog in our forums can be found here](#).



Immunization elevation

A standard user can only immunize browser profiles that belong to his own user account. If you elevate your privileges to *Administrator* all accounts can be immunized.

Helpful Hint

Tick the boxes that best describe your situation. A suggested solution will then appear below.

- Are you using Windows Vista or later?
- Are there other users of this computer?
- Are you the first user set up on this computer?
- Do you know that your account is an administrator account?
- Do you have the password of an administrator account?

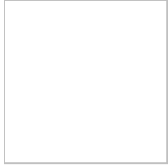
Please describe your situations by clicking the checkboxes above.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\).](#)

[Microsoft Windows 7: User Account Control \(UAC\).](#)

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)



Immunization preselection

Starting the [Immunization](#) tool shows this dialog which asks you to select what to immunize.

Helpful Hint

If you are unsure select *Full Immunization*. If you want to preselect what to immunize select *Customize selection*.



Immunization performance

The bigger the lists of items to block are, the more computing power is needed. To ensure optimum performance we constantly monitor the Internet and remove inactive domains from our lists.

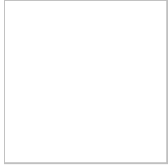


Immunization offer

Starting the [Immunization](#) tool shows this dialog to ask for a preselection of what to immunize.

Helpful Hint

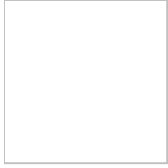
If you are unsure select *Full Immunization*. For a preselection of what to immunize select *Customize selection*.



Immunization progress

This dialog is displayed while the system is being immunized. This may take some minutes to complete. When completed access to domains known to contain malicious or undesirable software will be blocked.

During the process the dialog shows information about what is being immunized and an estimate of the time until it finishes. Select *Stop* to stop the process and your system will not be completely immunized. For complete immunization start the process again later. Select *Ignore* to hide this dialog while the immunization process proceeds.



Live Protection

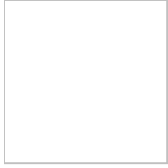
Live Protection scans every application before it even gets started, allowing to block malicious processes before they start.

If you want to disable *Live Protection*, you can right-click the Spybot icon in the Tray area next to the system clock, and uncheck the *Live Protection* entry. As an alternative, you can open *Settings*, make sure all tabs are shown (see *Advanced* checkbox), and check the options on the *Live Protection* tab. In this place you'll also find further options.

Availability

This module is available in the following editions:

- Home
- Professional
- Corporate
- Technician



OpenSBI Editor

This is an editor for the detection database.

Available parameters

Basic

/help shows this page
/verbose displays more output

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar

System Service related

/serviceinstalltest fakes that services are not installed

Supplemental Options

/youtube adds menu option to resize windows to YouTube video
resolutions

Availability

This module is available in the following editions:

- Professional
- Corporate
- Technician



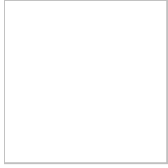
Phone Scan

This application will scan connected iTunes application storage for iPhone, iPod Touch or iPad applications that might include tracking software or spyware.

Availability

This module is available in the following editions:

- Home
- Professional
- Corporate
- Technician



Prepare Whitelist

A system Whitelist can speed up scans by ignoring known safe files. A Whitelist should only be created on a known uninfected system. We recommend that you only use a new system, after all software has been set up, but before connecting it to the Internet when creating the Whitelist if you intend using this feature.

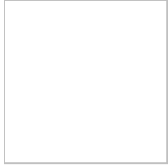
Whitelist Preparation is not available in Start Center

The Start Center shows this module only on systems that are not older than 30 days. It is recommended to create a whitelist in the scenario described above.

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician



Offer to create Whitelist

All system files can be whitelisted. This will mark them as good so that there is no need to scan them, this speeds up the scan.

Helpful Hint

Only create a Whitelist on a known clean system! If you are in doubt it is safer to not choose this option.



Whitelist created

This dialog tells you that all current files have been successfully flagged as 'good'.

© 2000-2013 Safer-Networking Ltd. All rights reserved.



Proxy Service

Spybot has its own web proxy that protects you against malicious websites and cookies systemwide. If enabled it acts as the default system proxy and every program using the system proxy uses Spybot proxy as well. Spybot proxy acts as an intermediary between your browser and the server that hosts the website you requested.

If you request a website that seems to be suspicious the proxy will block it. In this case you will see an internal website where you can choose between the following options:

- Show the website anyway
- Add URL to whitelist
- Add domain to whitelist

Using any of these options will redirect you to the website you requested. The last two options will add either URL or domain to the internal whitelist so the website you requested won't be blocked again. If you accidentally added a domain or URL to the whitelist you can edit the lists in the Spybot settings on Ignore Lists tab.

If you want to use a different proxy in addition to Spybot proxy you have to add it in Spybot settings on Internet Protection. Here you can enable and disable Spybot proxy as well.

Limitations

The proxy won't work if you change the proxy server in Windows LAN settings after Spybot installation or if you configured your browser to use a different proxy than the default system proxy.

Availability

The proxy is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician

Due to Microsoft security restrictions for Modern UI applications **the proxy is not available in Windows 8.**



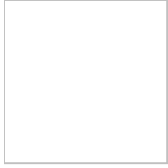
Quarantine

The *Quarantine* contains everything that has been removed by Spybot from an active system. Here, the user can either get rid of old quarantined items (an option that will be offered when old items are located) or restore removed items if there were false positives. False positives can happen in any security application.

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician



Selection of quarantine files by date

This dialog allows you remove files from [Quarantine](#) for a specified date range.

Helpful Hint

The default range is 90 days, which should suffice even for people rarely using their computer. Very active users may want to purge anything older than 30 days.

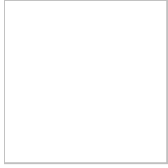


Offer to purge old quarantined items

Items are stored in [Quarantine](#) in case you might need to restore them at a later stage. If the removal of a file to [Quarantine](#) has not effected the functioning of the system there is no need to keep it. When opening the [Quarantine](#), it therefore offers to permanently delete any files older than 90 days.

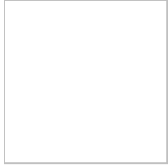
Helpful Hint

How often have you used your computer in the past three months? If it has been more than once a week and you have not had any issues since Spybot fixed the problems you should accept this offer.



Quarantine reading progress

This dialog is displayed while the system is updating its cached information on quarantined items. If you have updated from a previous version of Spybot it may take time but once it is finished the cached information will be available.



Quarantine purge error

This error dialog tells you that there was a problem while purging malware. This could be because of insufficient privileges, in which case the user is offered the opportunity to re-open the [Quarantine](#) with full administrator privileges.

Helpful Hint

Tick the boxes that best describe your situation. A suggested solution will then appear below.

- Are you using Windows Vista or later?
- Are there other users of this computer?
- Are you the first user set up on this computer?
- Do you know if your account is an administrator account?
- Do you have the password of an administrator account?

Please describe your situations by clicking the checkboxes above.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\).](#)

[Microsoft Windows 7: User Account Control \(UAC\).](#)

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)



Quarantine recovery error

This error dialog informs about problems while recovering false positives. A common reason might be lacking privileges to do so, in which case the user is offered to re-open the [Quarantine](#) with full administrator privileges.

Helpful Hint

Tick the boxes that best describe your situation. A suggested solution will then appear below.

- Are you using Windows Vista or later?
- Are there other users of this computer?
- Are you the first user set up on this computer?
- Do you know if your account is an administrator account?
- Do you have the password of an administrator account?

Please describe your situations by clicking the checkboxes above.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\).](#)

[Microsoft Windows 7: User Account Control \(UAC\).](#)

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)

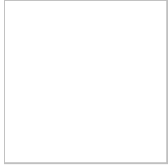


Quarantine purging confirmation

This is a confirmation dialog to ensure the user really wants to purge the selected items (the dialog will name them one by one). Purging means that items will be permanently removed.

Helpful Hint

If you are purging old files and you are sure that there are no problems with your system, continue. If you are trying to purge recently added files, remember that these files can do no harm while in quarantine, so it is better to keep them in Quarantine until you are certain that they are not required.

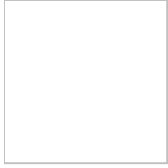


Quarantine recover confirmation

This is a confirmation dialog to ensure the user really wants to recover the selected items (the dialog will name them one by one).

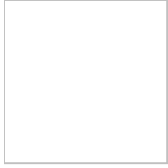
Helpful Hint

Recovering items means that you might introduce possible malware back into your system. Make sure you do this only for items that have been removed as a result of false positives, or for test purposes!



Old quarantined items

This dialog asks do you want to permanently delete files that have been in Quarantine for more than 90 days. Files that have been put into Quarantine are not deleted so that they can be restored if necessary. After 90 days it is very likely that they are dispensable so they can be purged to save disk space.



Quick Access

The *Quick Access* module allows you to directly start Spybot's tools via the notification area. Here you will find links to all modules without launching the *Start Center*.

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician



Selection of scanner

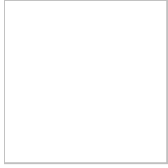
This dialog allows you to choose what to scan. [Malware Scan](#) is optimized to find malware that is active on a system. If you want to scan files from other sources the [File Scan](#) is faster.

Helpful Hint

Choose which of these options best describe your situation. A suggestion will appear in the box below.

- Do you want to scan your complete system for active malware?
- Do you want to scan a device (USB stick, memory card, etc) you attached to your system?
- Do you want to scan a large amount of malware samples for test purposes?

Please describe your situations by clicking the checkboxes above.



Repair Environment

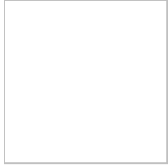
When the user executes the *Repair Environment* a new Windows Desktop is opened and the *Start Center* runs in there to allow the use of Spybot in a way where other software cannot interact and manipulate it as easily. The Windows Login screen and the User Account Control dialogs use the same technology to prevent keyloggers and other malware to have access and control.

A practical use of the *Repair Environment* would be where Spybot itself cannot be started any more, where it repeatedly closes out of the blue, seems to take actions on its own, or where malware that is known to exist on the system and that is known to be detectable does not appear in Spybots results.

Availability

This module is available in the following editions:

- Professional
- Corporate
- Technician



Report Creator

When you contact our Support Team for assistance, you may be asked to provide more details. The 'Report Creator' tool logs data that will help our team to analyze your issue. The created log files are saved in an archive file on your desktop. When done, you will be offered the options to view our privacy policy or the archive contents.

Available parameters

Basic

/help shows this page
/verbose displays more output

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar
/autocreate create archive using defaults at program start

System Service related

/serviceinstalltest fakes that services are not installed

Supplemental Options

/youtube adds menu option to resize windows to YouTube video
resolutions

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician

© 2000-2013 Safer-Networking Ltd. All rights reserved.

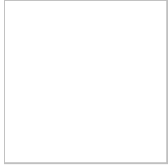


Log creation information

The log files that our software can create helps us to find and eradicate new malware. After the [Report Creator](#) tool has been run, it asks if you want to view our 'Privacy Policy' or check the data in the archive. It does this because maintaining the individuals privacy is why we created and maintain Spybot. Nothing will be sent unless the user agrees that they want to send it.

Helpful Hint

Read our 'Privacy Policy' to reassure yourself that you are happy sending us your log files. Examine the archived log files that will be sent so as you are aware on what information is about to be sent.



Rootkit Scan

Malware sometimes uses rootkit technology to hide itself at system level. This makes it undetectable by standard tools. Our plugins help Spybot to detect this form of malware. Our *Rootkit Scan* tool shows anything that uses certain rootkit technologies, even if it's not in Spybot's detection database.

The *Rootkit Scan* is a tool that checks the file system, the registry and process related lists. When *Rootkit Scan* is started, it performs a quick scan of a few critical locations. This check takes about a second on modern machines. To check the full system, it is possible to choose a Deep Scan.

Available parameters

Basic

/help shows this page
/verbose displays more output

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar
/autodeepscan immediately starts a deep scan
/autoclose closes after automated actions have finished

System Service related

/serviceinstalltest fakes that services are not installed

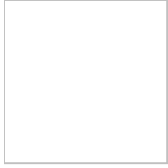
Supplemental Options

/anomalies also scans for file anomalies
/noanomalies force Anomalies to not be scanned for
/youtube adds menu option to resize windows to YouTube video
 resolutions
/scanuserhives includes HKEY_USERS in autodeepscan action

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician



Rootkit Deep Scan offer

A quick scan with our [Rootkit Scan](#) searches the most common system locations for malware. If it detects anything, it immediately offers to run a *Deep Scan* which will detect a threat at any location on the system.

Helpful Hint

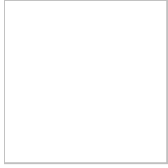
If the time is available, it is worthwhile doing a *Deep Scan*.



Rootkit Scan progress

This dialog is shown during a deep rootkit scan. Please have patience and let it finish.

© 2000-2013 Safer-Networking Ltd. All rights reserved.

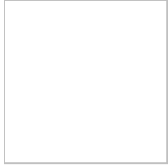


Confirm exit while scanning

The scanning process can be stopped by clicking the *Stop* button at the left of the [Rootkit Scan](#) window. If a user tries to close the window while a scan is in progress, the user will be asked whether he really wants to close it.

Helpful Hint

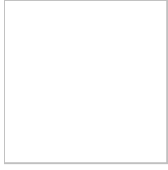
If you don't have time for a full rootkit scan now, but have reason to believe there is a rootkit on your system (if for example the Quick Scan reveals something), please run it later.



Deep Scan progress

This dialog is displayed while a deep scan is being performed by the [Rootkit Scan](#).

© 2000-2013 Safer-Networking Ltd. All rights reserved.



Scan Service

This provides malware scanning services that some Spybot modules need in order to function. The [File Scan](#) and Internet Protection depend on this service. If this service is stopped or paused protection will be disabled.

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician



Script Editor

The script editor allows you to create complex malware detection patterns using our OpenSBI syntax and the Pascal language. A most simple script that you also implement using a simple .sbi file as well would be this:

```
begin
    sbiFile('<$FILE_DATA>', '\Malware.txt', 'filesize=182,md5=83C36
end.
```

Now imagine you want some user input or custom calculation, because malware is individual to your system.

```
var sName, sFilename: String;
begin
    InputQuery('Username', 'Please enter', sName);
    sFilename := 'C:\Users\' + sName + '\test.txt';
    sbiFile('test', sFilename, 'filesize=10');
    ShowMessage('Did look for ' + sFilename);
end.
```

This demonstrates interaction with the user. In reality, you could of course just use the proper path template for scanning all users directories (see the OpenSBI wiki). Also, the use of scripting will be more in complex calculations and conditions than user interaction.

Availability

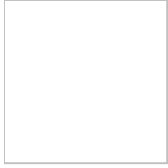
This module is available in the following editions:

- Professional
- Corporate
- Technician

Additional resources

- [Basics of the Pascal language](#)
- [Details of this scripting engine](#)

- [OpenSBI documentation, example](#)



Secure Shredder

The *Shredder* was developed to completely eradicate files and malware. It is included because some of our users requested it. The open source tool [Eraser](#) is a good and more modern alternative.

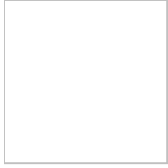
Additional resources

[Eraser project page at SourceForge](#)

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician



Secure Shredder confirmation

Since shredding files will get rid of files permanently, the [Secure Shredder](#) asks for confirmation before it proceeds with shredding.

Helpful Hint

Take a look at the list of files. Are you sure you want to completely eradicate these files with no way of ever getting them back ever?



Shredder elevation

If a user is not an administrator (or not elevated on Vista or later), he might not be able to shred just any file. In this case, the [Secure Shredder](#) offers to elevate to administrator privileges to retry on those files.

Helpful Hint

Tick the boxes that best describe your situation. A suggested solution will then appear below.

- Are you using Windows Vista or later?
- Are there other users of this computer?
- Are you the first user set up on this computer?
- Do you know if your account is an administrator account?
- Do you have the password of an administrator account?

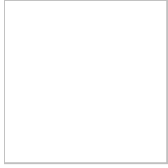
Please describe your situations by clicking the checkboxes above.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\).](#)

[Microsoft Windows 7: User Account Control \(UAC\).](#)

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)



Shredder template elevation

The [Secure Shredder](#) may recognize that the user does not have sufficient privileges to shred files that belong to the selected template. In this case, it offers to elevate to administrator privileges to continue.

Helpful Hint

Tick the boxes that best describe your situation. A suggested solution will then appear below.

- Are you using Windows Vista or later?
- Are there other users of this computer?
- Are you the first user set up on this computer?
- Do you know if your account is an administrator account?
- Do you have the password of an administrator account?

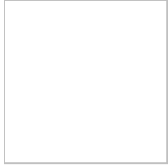
Please describe your situations by clicking the checkboxes above.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\).](#)

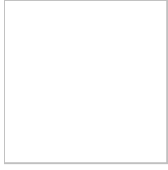
[Microsoft Windows 7: User Account Control \(UAC\).](#)

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)



Shredder files warning

If an attempt is being made to delete files, using the [Secure Shredder](#), and a file does not exist anymore this dialog will appear. This can occur when a file, after it has been added to [Secure Shredder](#) and before it is deleted by [Secure Shredder](#), has been moved somewhere else or has been deleted.



Security Center Service

The *Security Center Service* integrates Spybot into the Windows Security Center (Windows Vista) or the Action Center (Windows 7/Windows 8). After integration Spybot will report its update and operation status to Windows allowing the user to find all security related items in the Security Center/ Action Center.

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician



Settings

Settings allows users to customize Spybot to their personal preferences or make changes to the choices made during installation.

Language

Spybot offers to be used in different languages. This tab allows the user to select the preferred language.

Scope

This tab allows a user to make decisions on the scope Spybot is expected to scan.

Categories

The various categories Spybot can scan for. It is recommended not to disable any categories here unless there is a good reason to do so.

Live Protection

A user is able to install the Live Protection here and to select the type of monitoring. Additionally there are options for allowed, blocked or quarantined files.

System Integration

This allows the user to enable or disable Spybot in the context menu of Windows Explorer for files and folders or in AutoPlay dialogs. It also allows to decide whether the Spybot Tray icon is to be shown.

System Services

Spybot includes several services. These can be managed on this tab.

Browsers

In case a user wants to exclude a browser from being scanned for bad entries he can do this here.

Ignore Lists

A list of products and items that should not appear in the scan results, e.g. if there is some PUPS (Possibly UnPopular Software) that a user has intentionally installed. It is recommended to read the available documentation in our [malware removal guides](#) for any product before adding it to the Ignore List. There are also lists of domains and URLs that shouldn't be blocked by the Spybot proxy.

Schedule

Allows to control when automated tasks should take place.

Dialogs

Spybot has various dialogs that offer assistance where it may be needed. All these dialogs offer the option to not show themselves again, storing the preferred choice. This settings tab allows to change those preferences, for example if a specific dialog should be shown again the next time.

Portable Browsers

Spybot detects dozens of browsers. To save time for the regular user, it does not detect portable versions, which by design should leave no traces on a system. If it is required to immunize or scan a portable browser installation on a USB stick for example, it can be added here.

Internet Protection

Spybot comes with its own web proxy. The user is able to decide whether to use this one or the users own proxy. Using both or none is also possible.

Download Directories

Here a user is able to add download directories for special scrutiny during scans.

Available parameters

Basic

/help shows this page
/verbose displays more output

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar

System Service related

/serviceinstalltest fakes that services are not installed

Supplemental Options

/youtube adds menu option to resize windows to YouTube video resolutions

Tab to open

/showDialogs shows the Dialogs tabSettings after opening
/showPortable shows the Portable Browsers tabSettings after opening
/showBrowsers shows the Browsers tabSettings after opening
/showOnAccess shows the Live Protection tabSettings after opening
/showSchedules shows the Schedules tabSettings after opening
/showCategories shows the Categories tabSettings after opening
/showScope shows the Scope tabSettings after opening
/showProxy shows the Internet Protection tabSettings after opening
/showIgnores shows the Ignore Products tabSettings after opening
/showDownloadDirs shows the Download Directories tabSettings after opening
/showServices shows the System Services tabSettings after opening
/showIntegration shows the Integration tabSettings after opening

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician



Settings elevation

Some settings can only be successfully applied with the privileges of a system administrator. Spybot offers to re-open its [Settings](#) with those privileges (should the user be able to access them).

Helpful Hint

If you try to describe your situation as correctly as possible by selecting the options below that apply, we can make a suggestion.

- Are you using Windows Vista or later?
- Are there other users of this computer?
- Are you the first user set up on this computer?
- Do you know that your account is an administrator account?
- Do you have the password of an administrator account?

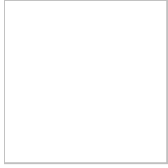
Please describe your situations by clicking the checkboxes above.

Additional resources

[Microsoft Windows Vista: How to use User Account Control \(UAC\).](#)

[Microsoft Windows 7: User Account Control \(UAC\).](#)

[Microsoft Windows 8 \(or later\): What are User Account Control settings?](#)



Selection of products to ignore

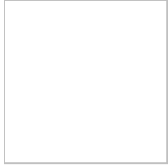
This dialog allows you to add to the list of products that Spybot should ignore during scans. In previous versions this has lead to misunderstandings. **Please Note:** this is *not* a list of anything detected on the system!

Helpful Hint

Please make sure you know exactly why a product you want to ignore is listed within Spybot before adding it to the ignore list. Our [removal guide forum](#) lists details about products, often including descriptions as to why they were added.

Additional resources

[Safer Networking Forums: Malware Removal Guides](#)



Loaded Registry Hive information

This dialog shows information about the registry hive. The information includes user accounts on the running system and dormant locally connected systems.



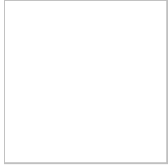
No categories selected

It is possible to select categories of malware the [System Scan](#) looks for. This can allow you reduce the time a scan needs, to add your own categories, to add new detection patterns (see OpenSBI) or for testing purposes. If no category is selected, [System Scan](#) will only do a generic scan of browser profiles and system services. For regular use, selecting some categories (usually all) is highly recommended.



All products get ignored

Highly unlikely, but still possible: if all products that Spybot detects are set to be ignored, scans never lead to any results. Therefore, the [Settings](#) window warns if that is the case.



The Start Center

In all versions of Spybot prior to 2.0, all tools were combined in a single interface. Beginning with version 2 Spybot is more flexible through [modularity](#). And while all modules now list associated tasks for easy navigation, the *Start Center* was created to give an overview over all parts of Spybot, plus quick information on its current state.

The main menu includes access to this help, as well as links to our website and forum.

The top area of the *Start Center* shows the version and status information. Clicking some items (e.g. a warning 'No Update attempt registered.') will allow the user to change that state.

The main area includes links to the modules included in Spybot. Depending on the way the user intends to use it, he may want the window to close once he has clicked a link, in which case he should select the checkbox at the bottom named *Close this window after opening link*. In case this checkbox is hidden, this can be changed in Settings on the Dialogs tab. Deselecting the option 'Hide above option within Start Center' shows the previously mentioned checkbox.

The bottom area shows the *Tip of the Day*, a random tip that might hint at features a user has not yet seen, issues where care should be taken, and other things. This can be closed for the session by clicking the large *X* at the left, or more tips can be viewed by clicking *Next tip*.

Available parameters

Basic

/help shows this page
/verbose displays more output

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar

System Service related

/serviceinstalltest fakes that services are not installed

Supplemental Options

/youtube adds menu option to resize windows to YouTube video resolutions

Start Center

/mode=
(standard|experienced) toggles which mode to start with

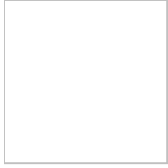
/forcewhitelist enforces whitelist creation offer and icon

/suppresswhitelist suppresses whitelist creation offer and icon

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician



Information on supposed incompatibilities with installed software

When installing some anti virus software you might be forced to uninstall Spybot. We are aware that this has happened, on occasion, with products from Kaspersky, McAfee, Symantec, or Trend Micro. The 'Anti-Spyware Coalition' considers forcing a user to uninstall security software as an indicator of the presence of malware. Unfortunately some vendors software still persist on forcing an unnecessary uninstall.

Our own research has never shown any issues that would warrant a full or partial uninstallation. Remember: even in the worst case, Spybot could be used as a pure on-demand scanner. We have never received a satisfactory explanation from any company as to why a user should need to uninstall Spybot. We can only assume that it is because some companies regard us as serious competition.

Helpful Hint

Trying to force you to uninstall legitimate software (you rely on) is anti competitive. Should you ever suspect that our software is causing a conflict please immediately inform our support team who will give it their immediate attention.



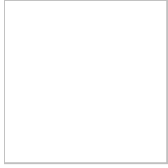
Information on supposed incompatibilities with running setup

When installing some anti virus software you might be forced to uninstall Spybot. We are aware that this has happened, on occasion, with products from Kaspersky, McAfee, Symantec, or Trend Micro. The 'Anti-Spyware Coalition' considers forcing a user to uninstall security software as an indicator of the presence of malware. Unfortunately some vendors software still persist on forcing an unnecessary uninstall.

Our own research has never shown any issues that would warrant a full or partial uninstallation. Remember: even in the worst case, Spybot could be used as a pure on-demand scanner. We have never received a satisfactory explanation from any company as to why a user should need to uninstall Spybot. We can only assume that it is because some companies regard us as serious competition.

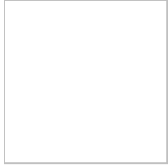
Helpful Hint

Trying to force you to uninstall legitimate software (you rely on) is anti competitive. Should you ever suspect that our software is causing a conflict please immediately inform our support team who will give it their immediate attention.



Detected Clients Information

Spybot is able to detect the number of clients in a network. If too many clients are detected Spybot asks if the Private or Corporate Edition is installed.



Selection of installation type

Spybot is available in different versions. The user has to select for which purpose Spybot will be used.



System Repair

The *System Repair* module is a registry repair tool to repair or delete registry entries that are corrupt and thus not functioning. This tool is not intended to replace 'registry cleaners' that automatically try to repair bad entries. To use this tool some technical expertise is required.

Available parameters

Basic

/help shows this page
/verbose displays more output

Available Operations

you need to specify one of these

/scan scans for system inconsistencies when the program starts

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar
/autorepair starts the fixing process after a previous scan action
/autoclose closes after previous scan or repair action

System Service related

/serviceinstalltest fakes that services are not installed

Supplemental Options

/youtube adds menu option to resize windows to YouTube video resolutions

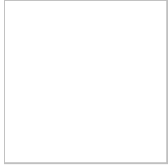
Availability

This module is available in the following editions:

- Free
- Home

- Professional
- Corporate
- Technician

© 2000-2013 Safer-Networking Ltd. All rights reserved.



System Scan

This is the main on-demand scanner. It is used to scan a complete system for active malware. For scanning just a few selected files, should the [File Scan](#) be used instead, which can be found in the list of associated tasks at the left of the main window, inside the [Start Center](#), or by right-clicking any file in Windows Explorer, in case that integration has been installed during installation.

Available parameters

Basic

/help shows this page
/verbose displays more output

Available Operations

you need to specify one of these
/scan starts a scan immediately
/scanforlastresults starts a (re-)scan for just the products detected during the last scan

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar
/cleanclose closes after /scan if results are clean

System Service related

/serviceinstalltest fakes that services are not installed

Supplemental Options

/youtube adds menu option to resize windows to YouTube video resolutions
/forcemarquee tries to force scan progress marquee dialog to display even on unsupported OS
/nomarquee skips the progress marquee dialog during scans

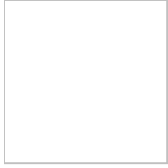
Scan limitations

/browsercache scans just the browser cache
/services scans just system services
/justincludes just the filesystem

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician



Scan Duration Information

A Spybot *System Scan* only scans for active malware on a running system. That is why this *System Scan* does not last hours like it might happen with traditional anti-virus scans.

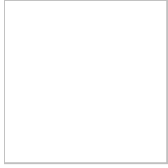
When starting a scan the user will be asked whether he wants to scan his system with a standard *System Scan* for active malware. This is recommended for regular users. In case the user wants to scan just a few files or inactive samples he is recommended to use the [File Scan](#).



Offer to disable 3rd party cookies

If you think that Spybot may not have displayed a result that some other security application has detected you can choose to disable third party cookies.

Should you suspect that Spybot may not have detected a threat please send the details to: detections@spybot.info.



Cookie handling alternatives

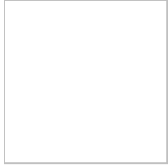
Cookies are small pieces of data that websites use to store information on your computer. "Bad" cookies can be used to track a users Internet usage. Rather than remove them after they have been stored on your computer you can choose to block them.

We recommend that you disable all third party cookies. This stops them arriving so you do not have to remove them later.

To undo these changes, the appropriate settings within the affected browsers can be used. These are, for example:

Mozilla Firefox and most clones: type *about:config* into the address bar. Confirm that you want to continue editing settings. Enter *network.cookie.cookieBehavior* into the filter box. Double-click and change the value to 0 to get the default behaviour back. All possible settings are explained at [mozillaZine](#).

Internet Explorer: see changes to 1A05 and 1A06 on [Microsoft](#), or look for *Allow 3rd party persistent cookies* and *Allow 3rd party session cookies* within the Internet zone settings.



Cleaning temporary files

While it is running, a system creates temporary files. These are usually removed when they are no longer being used. Applications that terminate unexpectedly can cause files that are no longer needed to be left in folders. The Windows 'Disk Cleaner' can 'Clean Up' these folders by deleting files but it is rarely used. Scanning the folders where temporary files are stored can take time, but it is necessary as they can contain malware. This is why Spybot offers to clean up temporary folders.

Helpful Hint

If you have for some reason stored files that you want to retain in a temporary folder do not use this feature. Otherwise it is safe to use, since it will not delete files currently in use.



Confirm exit while scanning

A scanning process can be exited by clicking the *Stop* button at the left of the [System Scan](#) window. If a user tries to close the window while a scan is in progress, the user will be asked whether he really wants to close it.

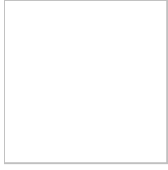
Helpful Hint

Did you know that the buttons at the left of the window allow you to stop or pause a scan? If you require more computing power and want to finish the scan later, don't close the window just pause the scan.



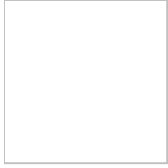
System Scan progress

This dialog is shown while a full system scan is running. It shows the progress and allows to pause or stop the scan.



Re-scan Information

After cleaning a system the user might want to re-scan the cleaned items. If no previous cleaning attempts are found the user is prompted to do a full system scan.



Startup Tools

This module contains the up-to-date versions of tools integrated into older versions of Spybot along with some of our stand-alone tools such as RunAlyzer.

Startup Tools allows you to select what programs run automatically at start-up. Managing autorun locations is a task that requires some technical expertise.

The [Report Creator](#) tool, found here, can create a comprehensive report that may be used when contacting Team Spybot for help.

Available parameters

Basic

/help shows this page
/verbose displays more output

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar
/autoclose saves log and closes application after all data has been read

/fasttest does not load lasshes or file properties to speed up debugging
/nolasshes does not load lasshes to speed up debugging
/noattr does not load file properties to speed up debugging

Registry Hives

/allhives tries to load all possible registry hives
/externalhives tries to load hives from other system installations
/userhives tries to load hives from all user accounts
/nouserhives skips hives from other user accounts

System Service related

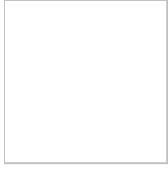
/serviceinstalltest fakes that services are not installed

Supplemental Options

/youtube	adds menu option to resize windows to YouTube video resolutions
/savelogonly	creates a log file
Availability	

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician

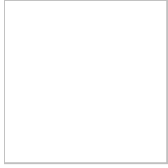


Disable/Delete confirmation in Startup Tools

This dialog shows details of the item that is about to be disabled or deleted. It includes information from the version resource of the associated file.

Helpful Hint

If you are not sure, always disable rather than delete. If your action has caused an error you can always re-enable later whereas deletion is final.



Process termination confirmation

The [Startup Tools](#) application shows running processes and allows you to terminate them.

Helpful Hint

Terminating a process 'kills' it, without allowing it to shut down in an orderly fashion and can cause a loss of data. Termination should only be used when you cannot otherwise shut down an application.



Update

With the Free Edition of Spybot you can use this module to keep your Spybot up to date. It will show information about the files and allow you to choose which ones to update.

Using a Home or higher Edition updates are automated. Spybot will create a Windows scheduler task to keep your Spybot up to date. Of course manually updates like in the Free Edition are possible, too.

Available parameters

Basic

/help shows this page
/verbose displays more output

Available Operations you need to specify one of these

/autoupdate immediately starts looking for updates

Automation

/silent avoid unnecessary output
/taskbarhide avoid UI appearing even in the taskbar

Supplemental Options

/youtube adds menu option to resize windows to YouTube video resolutions

System Service related

/serviceinstalltest fakes that services are not installed
/nosystemservice loads services in memory instead of as a system service if possible

Availability

This module is available in the following editions:

- Free
- Home
- Professional
- Corporate
- Technician

Additional resources

[More discussions about this module in our forums can be found here.](#)

© 2000-2013 Safer-Networking Ltd. All rights reserved.

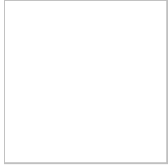


Update progress

To allow more automation in updating, it has been moved into a background system process that would update the system without any attention needed by a user. Since the update process is a typical security risk with many anti virus applications (browse past IT news for exploits in the updater of well known ones), we decided to pay special attention to this issue and kept the interface between the user interface and the more powerful background service as small as possible.

We also wanted to avoid problems arising from a partially updated system which could leave a state of perfect integrity.

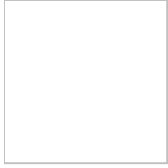
Both issues combined led to this dialog that shows the status of the background updating in a plain and simple way.



Missing log file

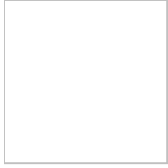
Information about the updates are stored in a log file. In case this file does not exist this dialog is shown.

That this file does not exist might mean that the Updating Service is not running. To check whether the Updating Service is installed and running open [Settings](#) and select the *System Services* tab.



System service execution

Some functionalities of Spybot need certain system services. This dialog asks whether this additional started service is to be stopped after closing this application or allowed to keep running.



Internet Explorer URL warnings

This dialog warns about an URL or cookie that is possibly malicious. The user will be informed about the location and what was identified.



System Restore Point offer

System Restore Points are fixed points in the history of system changes that can be reverted back to in case of problems. The [System Repair](#) and the [Malware Cleaner](#) offer to create system restore points before taking action.

Helpful Hint

In case of doubt, the additional time needed to create a restore point always puts you on the safe side.

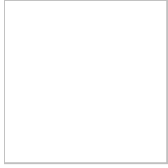
Additional resources

[Microsoft Windows XP: How to restore Windows XP?](#)

[Microsoft Windows Vista: What is System Restore?](#)

[Microsoft Windows 7: What is System Restore?](#)

[Microsoft Windows 8: How to restore, refresh, or reset your PC](#)



Missing files warning

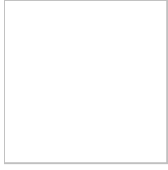
When started, the [Malware Scan](#) checks the installation for missing files. Sometimes malware can delete files if it is attacking Spybot. If there are missing files you are offered two options to recover these files. One is to use the [Update](#) to do a full integrity check and try to restore the files. The other is that the user is directed to our 'boot CD' creation page. The 'boot CD' allows you to do a 'clean boot' and scan the system. The second one is recommended if files are repeatedly going missing.

Helpful Hint

We recommend that you try to manually start the [Update](#) if you see this message. If it does not solve the problem and the message reappears, your system may be infected with software that is actively attacking your Spybot installation, in which case you should scan using the bootable CD.

Additional resources

[Safer Networking Forums: Creating a bootable CD to run Spybot from.](#)



Restore Point creation progress

Spybot waits while restore points are being created. Creating a restore point can take some time. Windows offers no indication on the progress of restore point creation, so we cannot estimate how long it will take. We ask to be patient and wait until it completes.

Additional resources

[Microsoft Windows XP: How to restore Windows XP?](#)

[Microsoft Windows Vista: What is System Restore?](#)

[Microsoft Windows 7: What is System Restore?](#)

[Microsoft Windows 8: How to restore, refresh, or reset your PC](#)



System Restore Point offer forcefully

System Restore Points allow you to revert back to the state before changes were made. This can be useful if a change causes a problem. The [System Repair](#) and the [Malware Cleaner](#) offer to create system restore points before taking an action.

Helpful Hint

In case of doubt, the additional time needed to create a restore point always puts you on the safe side.

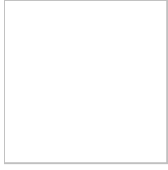
Additional resources

[Microsoft Windows XP: How to restore Windows XP?](#)

[Microsoft Windows Vista: What is System Restore?](#)

[Microsoft Windows 7: What is System Restore?](#)

[Microsoft Windows 8: How to restore, refresh, or reset your PC](#)



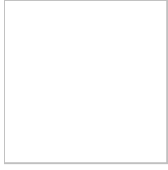
Command line parameter

Spybot offers the use of various command line parameters. Please notice that the availability of parameters depends on the Spybot edition you are using. To get information about parameters for each module use the parameter */help*.

Example:

```
SDScan /help
```

Alternatively see the module descriptions in this document for further information about the parameters of each module usable with parameters.



Supported Browsers

Spybot has dedicated support for most browsers. It can, for example immunize these browsers, or create restricted access shortcuts for your safety. Where we list product versions, these are the ones that have been tested; other versions are likely to be supported depending what changes have been made to them.

Unlisted browsers that are clones of listed browsers are also likely to be supported (e.g. most IE based browsers and many Google Chrome variants use the same cache location and formats).

Internet Explorer & clones

- [Acoo](#)
- [Avant](#)
- [Internet Explorer](#)
- [Lunascape](#) (5.x, 6.x)
- [Maxthon](#)

Mozilla based browsers

- [Beonex](#)
- [Firebird](#) (early versions of Firefox)
- [Firefox](#) (also mobile application)
- Flock (discontinued, not recommended)
- [K-Meleon](#)
- Lolifox (discontinued, not recommended)
- [Lunascape](#) (5.x, 6.x)
- [Postbox](#)
- Netscape (discontinued, not recommended)
- [SeaMonkey](#) (also mobile application)
- [Songbird 2](#)
- [Thunderbird](#)
- [Qtrax](#)
- [Wyzo](#)

Opera browsers

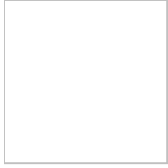
- [Opera](#) (4, 6.x, 7.x, 8.x, 9.x, 10.x)

Webkit based browsers

- [Apple Safari](#)
- [Chrome Plus](#) (Chromium based, also mobile application)
- [Google Chrome](#) (Chromium based, also mobile application)
- [Lunaspape](#) (5.x, 6.x)
- [SRWare Iron](#) (Chromium based, also mobile application)

Other browsers

- [Amaya](#)



1 Preface

If you miss our old license terms, we are sorry - they needed some legal adjustment. In order to offer a clean boot of Windows for our Service CD (comes with the Personal Edition), we had to license a limited Windows 7 from Microsoft and adjust our terms. Our Private Edition download will be free for your private use as you know Spybot Search & Destroy from the past.

2 Terms of Non-Commercial Use

This License Agreement (hereinafter Agreement) between Safer-Networking Ltd.of Mill Road, Greystones, Co. Wicklow, Ireland (hereinafter Safer-Networking Ltd.) and the Customer (hereinafter Licensee) deals with the terms and conditions of Licensee's use of Spybot - Search & Destroy software programs for non-commercial purposes, i.e. Spybot - Search & Destroy Private Edition and Spybot - Search & Destroy Personal Edition, including any additional components, e.g. the limited Operating System (Windows 7) as the case may be, updates, upgrades, modifications, revisions, copies, documentation and design data set out in the Schedule (the Software).

§1 GRANT OF LICENSE

1.1 The Software is copyrighted, trade secret and confidential information of Safer-Networking Ltd.or its Licensors who maintain exclusive title to all Software and retain all rights not expressly granted by this Agreement. Insofar as Software is supplied to Licensee (either in tangible or non tangible form) and subject to (i) the full payment of the License Fees, as the case may be, set out in the relevant Price List and (ii) depending on the Software obtained by Licensee, Safer-Networking Ltd.grants to Licensee a non-exclusive right to use the Software under the following conditions.

a) Spybot Search & Destroy Private Edition (Private Edition Software)

The Licensee shall be entitled to download, install, and run the Private Edition Software for Licensee's non-commercial purposes. The number of clients, i.e. devices, on which the Personal Edition Software is used, is not restricted, as long

as all are for private use only.

b) Spybot Search & Destroy Personal Edition (Personal Edition Software)

The Licensee shall be entitled to run the Personal Edition for the Licensee's non-commercial purposes. The number of clients, i.e. devices, on which the Personal Edition Software is used, is not restricted, as long as all are for private use only. The Personal Edition Software is distributed as a bootable Service CD that also contains a limited Operating System (Windows 7). For such limited Operating System (Windows 7) separate license terms apply (see Sec.1.1.c). The Personal Edition includes an installation file of the Private Edition.

c) Limited Operating System (Windows 7)

The Service CD may contain Windows software licensed from Microsoft Corporation and/or MS Affiliate(s) (limited Operating System). It is expressly stated, that the limited Operating System is not sold to Licensee and is provided as is. The Licensee may load and run the limited Operating System only as a boot, diagnostic, disaster recovery, setup, restoration, emergency service, test and/or configuration utility program. The use of the limited Operating System is restricted to one physical computer at a time. It is strictly prohibited to use the limited Operating System as a general purpose operating system or as a substitute for a fully functional version of any operating system product.

§2 LIMITED WARRANTY

Safer-Networking Ltd. has endeavored to ensure that the Software does not contain any backdoors or content to intentionally harm the Licensee. Safer-Networking Ltd. does not warrant that:

(1) the Software corresponds with its description in any advertising, marketing or other documentation howsoever published by it, its servants or agents or by third parties about the Software;

(2) the Software is merchantable and fit for the purpose for which the Licensee has contracted this agreement and the use of the Software nor that it will meet the Licensees requirements;

the Software is free of defects and that its use or operation will be error-free

(3) and free of interruption or down time.

Safer-Networking Ltd. has no liability to the Licensee for any representations made about the Software and it disclaims any liability to the Licensee, its assignees, permitted or otherwise, and invitees for all loss and costs, if any, which may be claimed to have been suffered by anyone as a result of the use of the Software the subject of this Agreement.

§3 DOCUMENTATION AND UPDATES

Safer-Networking Ltd. provides the necessary user documentation for the Software. This may also be provided electronically, e.g. via provision in the Internet. Safer-Networking Ltd. has no contractual obligation to provide regular updates and the provision of updates does not constitute any such contractual obligation of Safer-Networking Ltd.

§4 RESTRICTIONS

4.1 Safer-Networking Ltd. does not authorize all or any portion of the Personal Edition or the limited Operating System to be issued to the Public, put into circulation, or subject to a first sale as the copyright laws may use those (or similar) terms. Licensee is not allowed to distribute, sell, sublicense, lease, rent, loan or otherwise transfer the Personal Edition Software or the limited Operating System to a third party. Licensee may distribute the Private Edition Software only for non-commercial purposes. It is expressly prohibited to sell the Private Edition Software or parts of it to a third party, for the avoidance of doubt this also applies to any forms of bundling the Private Edition Software with any third party software.

4.2 All Software will be supplied and may be used in object code form only. Except as otherwise permitted for purposes of interoperability as specified by applicable and mandatory law, Licensee shall not reverse-assemble, reverse-compile, reverse-engineer or in any way derive from Software any source code or decrypt the database.

4.3 The Licensee shall not remove alphanumeric identification characters, trademarks and copyright notices.

4.4 The Licensee may copy Software only as reasonably necessary to support the

authorized use and may make necessary backup copies. Each copy must include all notices and legends embedded in Software and affixed to its medium and container as received from Safer-Networking Ltd.

4.5 The provisions of this Section 4 shall survive the termination or expiration of this Agreement.

§5 CANCELLATION OF CONTRACT

This agreement may be cancelled by the Licensee for whatever reason without any penalty or charge within seven days of receipt by the Licensee of the Software the subject of this agreement by written notice of cancellation from the Licensee to Safer-Networking Ltd. at its above address and the return to Safer-Networking Ltd. at the said address of the Software received by the Licensee on the giving of such notice of cancellation.

§6 FEES

6.1 The Private Edition Software can be obtained by the Licensee free of charge. Licence fees for the Personal Edition Software, which contains the limited Operating System are laid down in the Price List and shall be payable in advance in Euros (USD if Licensee is located in USA or Canada). If Software is delivered to Licensee on a data storage medium (e.g. CD-ROM) additional shipping costs may apply.

6.2 If the use of the limited Operating System at any time exceeds the maximum number of licenses granted to the Licensee under this Agreement the Licensee shall pay to Safer-Networking Ltd. the applicable additional License Fee so arising at the rates in the Price List. The number of the limited Operating Systems licenses granted shall be deemed to be adjusted accordingly on payment by the Licensee of the applicable additional License Fee.

6.3 License Fees and other charges from Safer-Networking Ltd. are due when invoiced and payable within 14 calendar days of the receipt of invoice by the Licensee.

6.4 License Fee and all other charges are exclusive of VAT and all other Taxation, which shall, if applicable, be chargeable to the Licensee.

§7 INSTALLATION AND SUPPORT

7.1 The Licensee is responsible for installation and use of the Software. Support issues of the Licensee will be handled solely by Safer-Networking Ltd. and not by any of its Licensors. Available support consists of email support and user forum. Phone support information is given on safer-networking.org.

7.2 THE LIMITED OPERATING SYSTEM CONTAINS A TIME-OUT FEATURE THAT WILL AUTOMATICALLY REBOOT THE DEVICE AFTER SEVENTY-TWO HOURS OF CONTINUOUS USE. THIS TIME-OUT FEATURE WILL RESET EACH TIME THE COMPONENT IS RE-LAUNCHED.

§8 SPECIFICATION OF THE SOFTWARE

The Software is designed to scan for software that poses a threat to the privacy of the user of a computer (Malware). While the Software endeavours to detect known Malware, not all Malware will be detected. Spybot - Search & Destroy software runs on Windows computers running 2000, XP, 2003 Server, Vista, 2008 Server, Windows 7 or Windows 8 only.

§9 LIMITATION OF REMEDIES AND DAMAGES

Any and all liability of Microsoft Ireland Operations Ltd. and its affiliates related to the Software, especially to the Limited Operating System is excluded.

§10 EXPORT

From time to time the Software may be subject to regulation by local laws and European Union export regulations, which prohibit export or diversion of certain products, information about the products, and direct products of the products to certain countries and certain persons. The limited Operating System is subject to U.S. export restrictions. Licensee agrees that Licensee will not export any Software or direct product of Software in any manner without first obtaining all necessary approval from appropriate local and European Union government agencies.

§11 GOVERNING LAW AND JURISDICTION

This Agreement shall be governed by and construed under the laws of Ireland. All disputes arising out of or in relation to this Agreement shall be submitted to the exclusive jurisdiction of the courts of Ireland. This section shall not restrict

the right of Safer-Networking Ltd. bring an action against the Licensee in the jurisdiction where the Licensee's place of business is located.

§12 SEVERABILITY

If any provision of this Agreement is determined by a court to be or becomes invalid, unenforceable or illegal, such provision shall be (i) modified to be made valid, enforceable and legal in such a manner as to best effectuate the intent of the parties at the inception of this Agreement; or (ii) be deemed eliminated where such modification is not practicable; and (iii) the remainder of this Agreement shall remain in effect in accordance with its terms as modified by such modification or deletion.

§13 PRIVACY

Even though Spybot - Search & Destroy scans the Licensee's system, it will not search specifically for any personally identifiable information. Everything that is not detected as a possible threat or usage tracks will be ignored. Possible threats and usage tracks will be shown and, if log options are switched on, written to a log file that may reside on an intranet server depending on the installation. For further information please visit <http://www.safer-networking.org>.

§14 MISCELLANEOUS

This Agreement sets forth the entire understanding and agreement of the parties regarding the subject matter hereof, and supersedes all prior agreements or representations, oral or written regarding such subject matter. This Agreement may not be modified or amended except in writing signed by a duly authorized representative of the party against whom enforcement is sought.

Windows is a registered trademark of Microsoft Corporation.

Spybot and Spybot Search & Destroy are Trademarks of Patrick Kolla-ten Venne.

This agreement is accepted when installing the software.