

SOPHOS

Sophos Anti-Rootkit

User manual

Sophos Anti-Rootkit 1.0
August 2006



Getting started

This guide tells you :

- what a rootkit is
- system requirements
- how to install Sophos Anti-Rootkit
- how to check for rootkits and remove any found
- how to access command line help
- how to remove Sophos Anti-Rootkit
- how to access technical help.

Contents

1	Introduction and system requirements.....	4
2	Installing Sophos Anti-Rootkit.....	5
3	Scanning for and removing rootkit.....	6
4	Running Sophos Anti-Rootkit from the command line	10
5	Removing Sophos Anti-Rootkit	11
	Technical support.....	12

1 Introduction and system requirements

1.1 What is a rootkit?

A rootkit is a program designed to conceal the presence of an application on a computer by hiding processes, files, configuration information, network traffic or other observable information from a user. For this reason you need to run Sophos Anti-Rootkit to remove the rootkits and then clean up any malicious files.

1.2 Before you start

Sophos Anti-Rootkit will support the following operating systems:

- Windows NT 4.0 (SP 6a with IE 4.0)
 - Windows 2000 (Professional or Server)
 - Windows XP (Home or Professional)
 - Windows Server 2003 standard edition
 - Windows Small Business Server 2003.
- ❗ On Windows NT 4.0 Sophos Anti-Rootkit will only detect hidden files and registry entries.

Sophos Anti-Rootkit requires:

- Minimum 128 Mb RAM.
- ❗ A rootkit scan may take several minutes on a desktop computer or significantly longer on a server. We suggest you run this process at a time when it will cause least inconvenience. You can stop a scan at any time, but the results given will be incomplete.
- ❗ It is strongly recommended that you close down all non-essential applications, and allow Windows Update to complete before running Sophos Anti-Rootkit.

2 Installing Sophos Anti-Rootkit

❗ Sophos Anti-Rootkit does not auto-update. Please ensure you have the latest version from the Sophos website. Sophos can not guarantee that versions downloaded from other sources will find the latest rootkits. You also run the risk of downloading a version that has been tampered with.

1. Download and run the program `sarsfx.exe` from the Sophos Anti-Rootkit web page.
2. Accept the licence agreement.
3. Follow the instructions to install the program.
4. When you run the installation, two programs are installed, `sargui.exe` and `sarcli.exe` in `C:\SOPHTEMP`, which is the default location.

`sargui.exe` is the graphical user interface (GUI) of the Sophos Anti-Rootkit. It is accessed through Windows and is described in section 3 of the this manual.

`sarcli.exe` is the command-line version of Sophos Anti-Rootkit. It is accessed through the command line, and is described in section 4 of this manual.

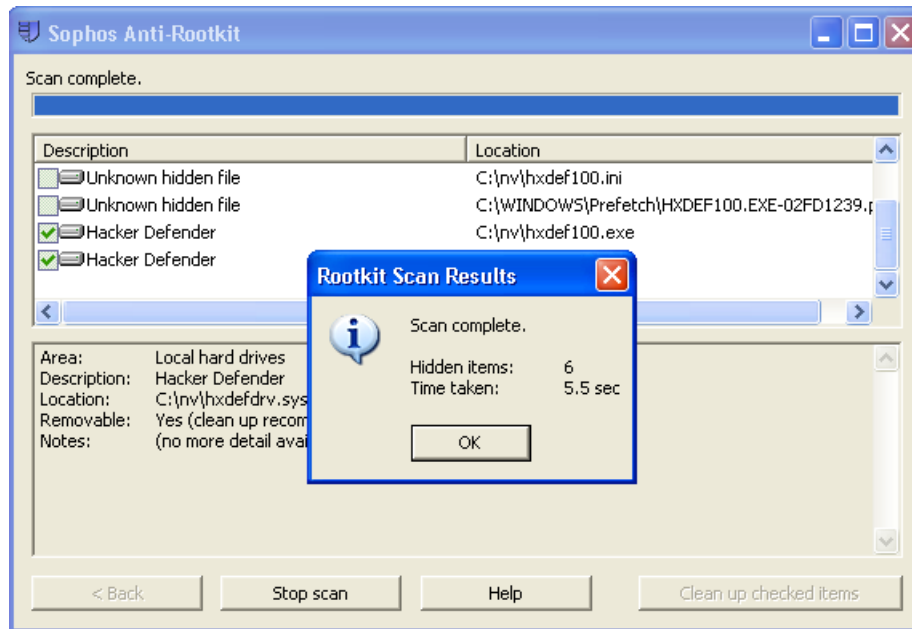
5. To start Sophos Anti-Rootkit, double-click `sargui.exe`.

3 Scanning for and removing rootkits

- ❗ When Sophos Anti-Rootkit detects and removes a rootkit from your computer, a restart is required to complete the cleaning process.
 - ❗ For instructions on how to scan your network with Sophos Anti-Rootkit, refer to the Sophos knowledgebase article 7004, located at <http://www.sophos.com/support/knowledgebase/article/7004.html>
1. In the initial dialog box, select areas you want to scan and click **Start scan**.



- Sophos Anti-Rootkit scans the selected areas and displays any suspicious files in the upper panel. When it is finished, a pop-up screen appears confirming the status and results of the scan. Click **OK** to continue.



- Click on the suspicious file to display more information about it in the lower panel. The information displayed includes whether the item is recommended for removal.

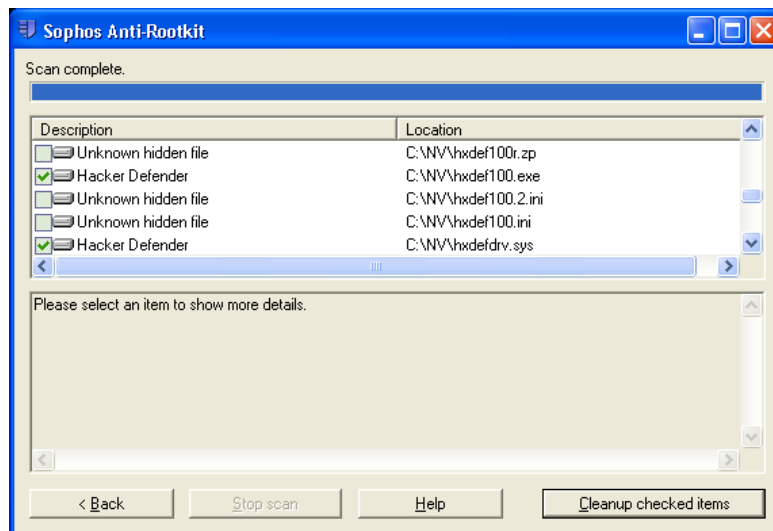
Files tagged as **Removable: No** are not marked for removal, and can not be removed.

Files tagged as **Removable: Yes (clean up recommended)** are marked for removal by default. Sophos strongly recommends you remove them.

Files tagged as **Removable: Yes (but clean up not recommended for this file)** are not marked for removal. Sophos does not recognize these files and recommends you do not remove them. If you are unsure of the status of these files, please follow the instructions in the Technical Support section of this manual to send the log and archive files to Sophos for further analysis.

- ⓘ Sometimes after the scan, the top panel displays a hidden process, registry key or value. When you clean up the rootkit(s), these entries will also disappear.

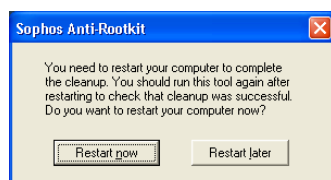
- The lower panel also states whether there is a description of the file. To check the information, access the Sophos website at www.sophos.com, enter the name of the file in the **Search** box at the top of the web page, and click the **Search** button.



- Click **Clean up checked items**. A pop up appears asking you to confirm the cleanup. Click **Yes** to continue. The file or process will be marked for removal and the cleanup will be done when you restart your computer.

❗ If Sophos Anti-Rootkit detects an item which was not recommended for removal, a warning appears. We strongly recommend you cancel the cleanup operation which includes those item(s). Select only item(s) recommended for removal (as shown in the lower details panel).

- A pop-up appears notifying you that the cleanup will be done when you restart your computer. It also advises you to run Sophos Anti-Rootkit again to check that the cleanup was successful. Click **Restart now**.

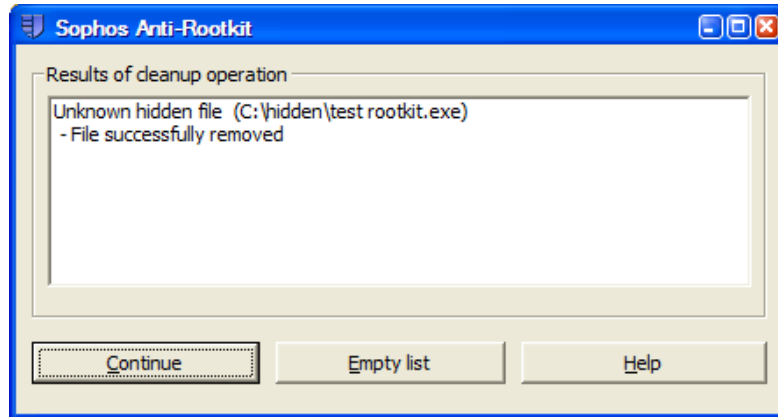


❗ If you run Sophos Anti-Rootkit again without restarting your computer, you will receive a warning and a further request to restart your system.

7. Once you have restarted your computer, a dialog box displays the files you selected for removal and the action taken.

Click **Empty list** if you want to clear the dialog box.

Click **Continue** to return to the initial dialog box. Return to [step 1](#) to re-scan your computer.



- ❗ Rootkits are often used to hide other malware. When you have re-scanned your computer to check there are no rootkits, Sophos recommends you confirm that your computer is totally clean by running anti-virus software, such as Sophos Anti-Virus.

4 Running Sophos Anti-Rootkit from the command line

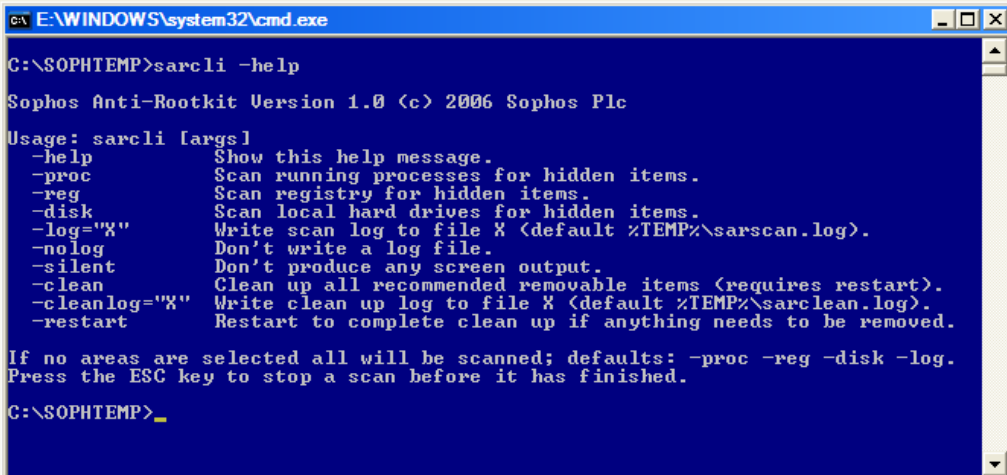
1. Open a command prompt.
2. Go the directory in which SARCLI .exe is installed (by default this is C:\SOPHTEMP).
3. To run a full scan, type

```
sarcli
```

4.1 Accessing the command line help

From the command prompt, type

```
sarcli -help
```



```

C:\WINDOWS\system32\cmd.exe
C:\SOPHTEMP>sarcli -help
Sophos Anti-Rootkit Version 1.0 (c) 2006 Sophos Plc
Usage: sarcli [args]
-help          Show this help message.
-proc         Scan running processes for hidden items.
-reg         Scan registry for hidden items.
-disk        Scan local hard drives for hidden items.
-log="X"     Write scan log to file X (default %TEMP%\sarscan.log).
-nolog      Don't write a log file.
-silent     Don't produce any screen output.
-clean      Clean up all recommended removable items (requires restart).
-cleanlog="X" Write clean up log to file X (default %TEMP%\sarclean.log).
-restart    Restart to complete clean up if anything needs to be removed.

If no areas are selected all will be scanned; defaults: -proc -reg -disk -log.
Press the ESC key to stop a scan before it has finished.
C:\SOPHTEMP>_
```

5 Removing Sophos Anti-Rootkit

Sophos Anti-Rootkit installs files in C : \SOPHTEMP, but does not make any changes to system files or registry files.

To remove Sophos Anti-Rootkit, delete the program files listed below:

```
helper.exe  
MEMSWEEP.SYS  
readsar.txt  
sar1.dll  
sar2.dll  
sar3.dll  
sar4.dll  
sar5.dll  
sar6.dll  
sarcli.exe  
sargui.cnt  
sargui.exe  
SARGUI.HLP  
sarman.pdf  
SophosBootTasksR.exe  
vdl.dat.
```

Technical support

- ❗ If you are an existing customer, Sophos offers telephone and email support. If you are not a Sophos customer, please use the Sophos web site for any technical support.

For technical support, visit

www.sophos.com/support

If you contact technical support, provide as much information as possible, including Sophos software version number(s), mail server or gateway details, operating system(s) and patch level(s), and the exact text of any error messages.

You can also send support the log file and hidden archive files. To access these files type the following from either the Windows **Run** dialog box or the command prompt:

- %TEMP%\sarscan.log
- %TEMP%\sarclean.log
- %TEMP%\samples.sar

- ❗ The file samples.sar is an encrypted archive of all hidden files detected by the scan. Sarscan.log is a text file listing all the hidden files contained in samples.sar. Please check the information in the text file before you send both files to Sophos in case it is confidential, or something you otherwise do not wish to disclose.

Any submission of files and/or data to Sophos is covered by the Sophos Licence Agreement for Anti-Rootkit Tool, available at URL: www.sophos.com/legal.

Copyright 2004-2006 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Rootkit are trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

Document version
200608