SOPHOS

Sophos Anti-Rootkit
user manual

Product version: 1.5
Document date: July 2009

Contents

1 About Sophos Anti-Rootkit

Sophos Anti-Rootkit 1.5 enables you to scan for and clean up any rootkits that may be hidden on your computer.

A rootkit is a Trojan or technology that is used to hide the presence of a malicious object (process, file, registry key, or network port) from the computer user or administrator.

There are Windows-interface and command-line versions of Sophos Anti-Rootkit. Both versions are installed when you run the installer.

The command-line version can be used over a network to remove rootkits. For instructions on how to do this, see *http://www.sophos.com/support/knowledgebase/article/17004.html*.

2 System requirements

Sophos Anti-Rootkit is supported on the following operating systems:

- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- 64-bit platforms

For detailed system requirements, go to the Sophos Anti-Rootkit product page at *http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html*.

You must have internet access in order to download the installer from the Sophos website.

3 Install Sophos Anti-Rootkit

Sophos Anti-Rootkit does not update itself, so make sure that you always download the latest version from the Sophos website. Sophos cannot guarantee that versions obtained from other sources will find the latest rootkits. You also run the risk of downloading a version that has been tampered with.

1. Go to the Sophos Anti-Rootkit product page at *http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html*.

2. Follow the link to download and save the installer to one of the following places:
   - A drive that can be accessed from the computer on which you want to install Sophos Anti-Rootkit
   - A CD or DVD
3. Locate the Sophos Anti-Rootkit installer that you downloaded earlier and double-click it.
   A wizard guides you through installation.

4 Remove Sophos Anti-Rootkit

❖ To remove Sophos Anti-Rootkit from your computer, click **Start** > **Programs** > **Sophos** > **Sophos Anti-Rootkit** > **Uninstall Sophos Anti-Rootkit**.

5 About scanning for rootkits

- You are strongly recommended to close down all non-essential applications and allow Windows Update to complete before scanning for rootkits.
- Depending on the computer being scanned, a Sophos Anti-Rootkit scan may take anywhere between a few minutes and over an hour to complete. Scans generally take significantly longer to complete on a server computer. You can stop a scan at any time, but the results will be incomplete, so run a scan at a time when it will cause least inconvenience.
- When Sophos Anti-Rootkit cleans up a rootkit from your computer, a restart is required to complete the process.

6 Run Sophos Anti-Rootkit from the command line

1. Open a command prompt and change to the Sophos Anti-Rootkit installation folder by typing:
   ```
   cd C:\Program Files\Sophos\Sophos Anti-Rootkit
   ```
2. To run a full scan, type:
   ```
   sarcli
   ```
3. To view the command line help, type:
   ```
   sarcli -help
   ```

For more information on using the command-line version of Sophos Anti-Rootkit, see *http://www.sophos.com/support/knowledgebase/article/17091.html*.

7 Start Sophos Anti-Rootkit using the Windows interface

❖ Click **Start** > **Programs** > **Sophos** > **Sophos Anti-Rootkit** > **Sophos Anti-Rootkit**.

8 Scan for rootkits

To scan your computer for rootkits:

1. Select the check boxes next to the areas of your computer that you want to scan.
2. Select the **Extensive scan** check box to scan every file on your computer during the **Local hard drives** scan instead of just the hidden ones.

   Note: Selecting this option will potentially find more rootkits, but the scan will take longer to complete. Depending on your computer, the time taken for this may be over an hour.

3. Click **Start scan** or press **Enter**.

When the scan is complete, a dialog box is displayed showing whether Sophos Anti-Rootkit has found any suspicious files.

9 Clean up rootkits

The names of suspicious files are displayed in the results list in the upper panel of the Sophos Anti-Rootkit window.

The results list may also display registry keys or values. These items cannot be marked for removal. However, after you have cleaned up any rootkits, these items will disappear from the results list.

To clean up rootkits:

1. Click the name of a suspicious file or process to display information about it. The information displayed includes whether the item is recommended for removal:

Option	Description
Removable: No	These files cannot be marked for removal.
Removable: Yes (clean up recommended)	These files are automatically marked for removal by default. Sophos recommends that you remove them.
Removable: Yes (but clean up not recommended for this file)	These files are **not** automatically marked for removal. Sophos does not recognize these files and recommends that you*do not remove them*. If you are unsure what to do about some of these files, follow the instructions in *Technical Support* (page 7) to send the log and archive files to Sophos for further analysis.

   The information displayed may also tell you whether there is a description of the file. To view the description of the file, go to the Sophos website at *www.sophos.com*, type the name of the file in the **Search** box at the top of the home page, and then click the **Search** button.

2. Click **Clean up checked items.** When the dialog box appears, click **Yes**.

   The checked items are marked for removal and will be cleaned up when you restart your computer.

3. When the dialog box appears, click **Restart now** or **Restart later**.

10 View results of rootkit cleanup

Once you have restarted your computer, the **Results of cleanup operation** window displays the files that were originally selected for removal and the action taken.

- To empty the contents of the panel, click **Empty list**.
- To return to the **Scan for hidden objects** dialog box so that you can rescan your computer, click **Continue**.

Rootkits are often used to hide other malware. Sophos recommends that you do the following after cleanup:

- Rescan your computer with Sophos Anti-Rootkit to make sure that all unauthorized files have been removed.

- Confirm that your computer is totally clean by running anti-virus software such as Sophos Anti-Virus.

11 Technical support

For technical support, visit *http://www.sophos.com/support*.

If you contact technical support, provide as much information as possible, including the following:

- Sophos software version number(s)
- Mail server or gateway details
- Operating system(s) and patch level(s)
- The exact text of any error messages

To send the Sophos Anti-Rootkit hidden archive file and log files to technical support:

1. Go to *https://secure.sophos.com/support/samples/* and complete the **Sample submission form**. Follow the instructions on screen, except as shown below.
2. For **I want to submit a**, select **File sample**.
3. Under **File 1**, click **Browse**, and then navigate to the following files in turn:

   `%TEMP%\samples.sar`

   `%TEMP%\sarscan.log`

   `%TEMP%\sarclean.log`

samples.sar is an encrypted archive of all hidden files detected by the scan and sarscan.log is a text file listing the hidden files contained in samples.sar.

Before you send sarscan.log to technical support, check that it does not contain any confidential information. To view sarscan.log, type the following from either the Windows **Run** dialog box or the command prompt:

`%TEMP%\sarscan.log`

Any submission of files and/or data to Sophos is covered by the Sophos End User License Agreement, which is available at *www.sophos.com/legal*.

12 Copyright