

# Sophos Malware Remediation Toolkit (SMaRT)

## User Guide

Product version: 1.2

Document date: April 2012

## Contents

|  |    |
|--|----|
| About this guide.....  | 3  |
| About the SMaRT Tools.....   | 3  |
| What to do if you think there is malware on a computer .....         | 4  |
| Before you begin.....  | 5  |
| Remediation process .....  | 6  |
| 1. Has malware been detected? .....                                  | 6  |
| 2. How was the malware detected? .....                               | 6  |
| 3. Can a sample be identified?.....                                  | 7  |
| 4. Submit sample .....   | 7  |
| 5. Sophos creates new identity? .....                                | 7  |
| 6. Update, protect and run full system scan.....                     | 7  |
| 7. Up to date? Run Healthcheck .....                                 | 8  |
| 8. Run Sophos Anti-Rootkit, Source of Infection and SDU.....         | 8  |
| 9. Cleanup using SMaRT.....  | 10 |
| 10. Cleanup successful? .....  | 11 |
| 11. Is the computer isolated from the network?.....                  | 11 |
| 12. Is malware redetected? (computer not isolated from network)..... | 12 |
| 13. Isolate the computer from the network .....                      | 12 |
| 14. Is malware redetected? (computer isolated from network) .....    | 12 |
| 15. Reconnect the computer to the network .....                      | 12 |
| 16. Is malware redetected? (computer reconnected to network) .....   | 12 |
| 17. Run Source of Infection Tool.....                                | 13 |
| 18. Has the source of infection been identified?.....                | 13 |
| 19. Move to source machine(s) .....                                  | 13 |
| 20. Run Healthcheck .....  | 14 |
| 21. Healthcheck Passed?.....   | 14 |
| 22. Run malware SDU, contact Support .....                           | 14 |
| 23. Run full SDU, contact Support.....                               | 15 |
| Legal Notices .....  | 16 |

## About this guide

The SMaRT user guide describes a systematic process for dealing with malware, from first suspecting its presence on your system right through to removal. The guide is also available as an interactive tool, which you can find at <http://www.sophos.com/support/knowledgebase/article/116418.html>.

## About the SMaRT Tools

The SMaRT guide demonstrates the processes needed to remove malware using Sophos products. It advises on which tools should be used, under what circumstances and how best to use them.

### The SMaRT tools include:

*Source of Infection Tool (SOI)* – used to identify where persistent malware originates. This can be either a network location or a local process.

*Sophos Anti-Rootkit (SAR)* – used to detect malware that uses stealth (rootkit) technology to evade detection by normal anti-virus scanners.

*Sophos Bootable Anti-Virus (SBAV)* – used to detect and disinfect fully compromised computers by using an independent operating system.

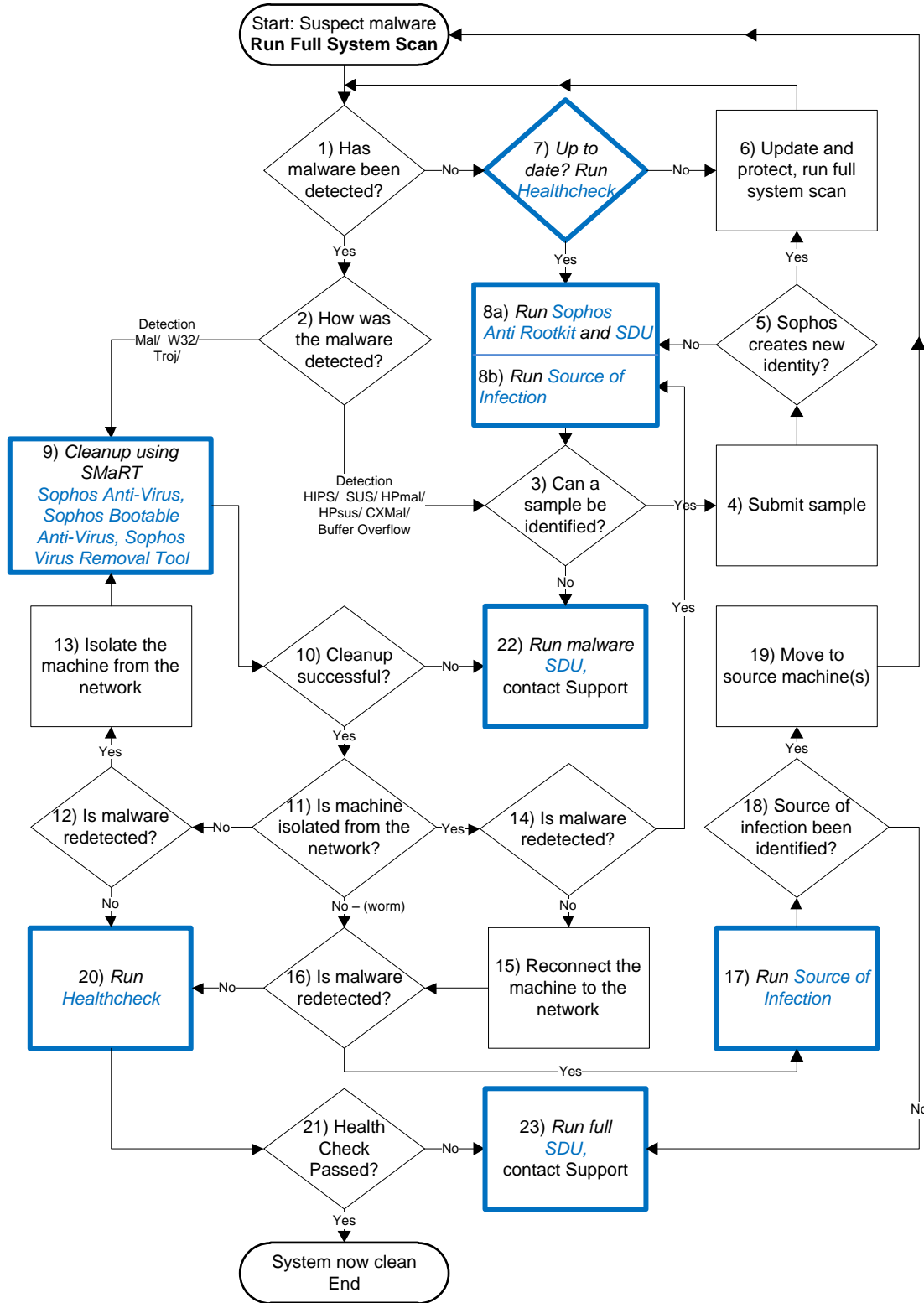
*Sophos Healthcheck (SHC)* – used to check the status of the Sophos installation on the computer.

*Sophos Virus Removal Tool (SVRT)* – used to clean up malware in standalone situations. It is can be used when other anti-virus vendor products are installed.

*Sophos Diagnose Utility (SDU)* – used to collect logs for Sophos technical support so support can assist further with the infection.

# What to do if you think there is malware on a computer

When there is a possibility of malware existing then follow the below process to troubleshoot the issue.



## Before you begin

There are a few settings that should be configured on the computer. (N.B All configuration settings are described for Sophos Endpoint Security and Control v10. Earlier versions might have slight changes in terms and settings: consult the product manual for further information.)

**If you suspect malware on the computer, ensure that you have completed a full scan.**

- To complete a full system scan:
  - I. Right click the Sophos shield in the system tray.
  - II. Click **Open Sophos Endpoint Security and Control**.
  - III. Click **Scan my computer**.

If Tamper Protection is enabled, before any configuration changes can be made the user will need to authenticate using the **Authenticate User** option.

Enable the On-Access scanner with on-read, on-write, on-rename , detect suspicious files and scan system memory.

- To edit the on-access settings:
  - I. Right click the Sophos shield in the system tray.
  - II. Click **Open Sophos Endpoint Security and Control**.
  - III. Click **Configure anti-virus and HIPS**.
  - IV. Click **On-access scanning**.
  - V. Check the tick box for **On read, On write, On rename , Suspicious files and Scan system memory**.
  - VI. Click **OK**.

Enable Behavior Monitoring, detect malicious behavior, suspicious behavior and buffer overflows.

- To edit the Suspicious Behavior Detection settings:
  - I. Right click the Sophos shield in the system tray.
  - II. Click **Open Sophos Endpoint Security and Control**.
  - III. Click **Configure Anti-Virus and HIPS**.
  - IV. Click **Behavior monitoring**.
  - V. Check the tick box for **Enable behavior monitoring**.
  - VI. Check the tick boxes for **Detect malicious behavior, Detect suspicious behavior and Detect buffer overflows**.
  - VII. Uncheck the tick boxes for **Alert only**.
  - VIII. Click **OK**.

Enable Sophos Live Protection.

- To edit the Live Protection settings:
  - I. Right click the Sophos shield in the system tray.
  - II. Click **Open Sophos Endpoint Security and Control**.
  - III. Click **Configure Anti-Virus and HIPS**.
  - IV. Click **Sophos Live Protection**.
  - V. Check the tick box for **Enable Live Protection**.
  - VI. Click **OK**.

Enable Web Protection with both block access to malicious websites and download scanning.

- To edit the Web protection settings:
  - I. Right click the Sophos shield in the system tray.
  - II. Click **Open Sophos Endpoint Security and Control**.
  - III. Click **Configure Anti-Virus and HIPS**.
  - IV. Click **Web protection**.
  - V. Select **On** for the pull down menu for **Block access to malicious websites** and **Download scanning**.
  - VI. Click **OK**.

For further information, see the following knowledgebase article:

<http://www.sophos.com/support/knowledgebase/article/63923.html>

## Remediation process

### 1. Has malware been detected?

Check Sophos Anti-Virus Quarantine Manager to see if an item has been detected.

To view the quarantine:

- I. Right click the Sophos shield in the system tray.
- II. Click **Open Sophos Endpoint Security and Control**.
- III. Click **Manage Quarantine Items**.
- IV. If an item is detected proceed to step 2. How was the malware detected?
- V. If no detection exists, go to step 7. Up to date? Run Healthcheck.

### 2. How was the malware detected?

Sophos uses a mixture of identity detections and runtime behavior detections to protect against malware.

- If you have a Buffer Overflow, HIPS/, Sus/, HPsus/, HPmal/ or CXmal/ prefixed detection, go to step 3. Can a sample be identified?
- If you have any other detection prefixes (Mal/, Troj/ and W32/), go to step 9. Cleanup using SMaRT.

*To see further information on the classifications see Article 113342 Comparison of Sophos's Malicious File Detection Technologies*

<http://www.sophos.com/support/knowledgebase/article/113342.html>.

### 3. Can a sample be identified?

The Quarantine Manager will provide details about a detection including the location of the file.

- If a sample can be identified, go to step 4. Submit sample.
- If a sample cannot be identified, go to step 22. Run malware SDU, contact Support

### 4. Submit sample

Submit a sample to Sophos at <http://www.sophos.com/support/samples>.

For further information see knowledgebase article

<http://www.sophos.com/support/knowledgebase/article/11490.html>.

You may be required to submit more than one unique sample to identify the malware.

Go to step 5. Sophos creates new identity?

### 5. Sophos creates new identity?

Once the analysis of the sample has completed an email will be sent with the outcome.

- If the sample submission results in the creation of a new identity then proceed to step 6. Update, protect and run full system scan.
- If the sample analysis has determined that the file is not malicious or is an exploitable file then go to step 7. Up to date? Run Healthcheck.

For more information on exploitable files see Article 112898 Exploitable Files.

<http://www.sophos.com/support/knowledgebase/article/112898.html>.

### 6. Update, protect and run full system scan

If an issue has been resolved for the Sophos installation or a sample submission results in the creation of a new malware detection:

- I. Update the Sophos installation:
  - a. Right click the Sophos shield in the system tray.
  - b. Click **Update Now**.
  - c. If a new malware detection was created, check that the IDE file the detection was released in is now present on the computer:
    - i. Open Computer.
    - ii. Navigate to the location %programfiles%\Sophos\Sophos Anti-Virus.

- iii. Check for the presence of the file detailed in the response from SophosLabs for the sample submission.
- II. Run a full system scan:
  - a. Right click the Sophos shield in the system tray.
  - b. Click **Open Sophos Endpoint Security and Control**.
  - c. Click **Scan my computer**.

In the event of updating problems, contact your system administrator or move to step 22. Run malware SDU, contact Support

Go to step 1. Has malware been detected?

## 7. Up to date? Run Healthcheck

Check the Sophos shield in the system tray. If it has a red cross or yellow warning triangle then the computer may not be up to date or Sophos not working correctly.

Download the Healthcheck Tool from <http://www.sophos.com/misc/SophosHealthCheck.exe> and then run the program from the command line. If using Windows Vista or above, the command prompt needs to be run as an administrator. This will confirm if Sophos Anti-Virus is working correctly. For further information on the Sophos Healthcheck tool see [Article 112843 Sophos Healthcheck Tool](http://www.sophos.com/support/knowledgebase/article/112843.html)

- If the computer is not up to date go to step 6. Update, protect and run full system scan.
- If the computer is up to date and there are no problems detected with the Sophos installation, go to step 8\_a) Run Sophos Anti-Rootkit and SDU.

## 8. Run Sophos Anti-Rootkit, Source of Infection and SDU

The tools Sophos Anti-Rootkit, Source of Infection and SDU can each be used to identify the location of malware. Once located, a sample can be submitted to Sophos. The different tools and the circumstances they are used in are described below.

| Tool                | Scenario  |
|---------------------|---|
| Sophos Anti-Rootkit | Malicious symptoms are seen, but there are no malware detections or a sample cannot be identified         |
| Source of Infection | When malware returns to a known location the Source of Infection tool can be used to identify the origin. |
| SDU                 | Collects information on malware loadpoints, can be used to identify malicious file locations.             |

### **a) Run Sophos Anti-Rootkit and SDU**

Run Sophos Anti-Rootkit scanner to determine if there are any hidden items on the computer that require investigation:

- I. Click Start | All Programs | Sophos | Sophos Anti-Rootkit | Sophos Anti-Rootkit.
- II. Check all the tick boxes.
- III. Click **Start Scan**.
- IV. Once the scan has completed select the items you wish to cleanup.
- V. Click **Clean up checked items** to remove the files (a reboot may be required).

For information on how to use the Sophos Anti-Rootkit tool see [Article 17125 Sophos Anti-Rootkit Tool](http://www.sophos.com/support/knowledgebase/article/17125.html) <http://www.sophos.com/support/knowledgebase/article/17125.html>.

The latest version of the SDU tool should always be used. To download the latest version, go to article <http://www.sophos.com/support/knowledgebase/article/33533.html>. Collect an SDU log from the computer using the `-malware` switch:

- I. Click Start | Run | type "cmd" and click **OK**.
- II. In the command prompt window browse to the SDU directory:  

```
cd C:\Program Files\Sophos\Sophos Diagnostic Utility
```
- III. Run the SDUCLI application with the `-malware` switch:  

```
sducli.exe -malware
```

For further information on running the SDU logging utility, see [Article 116537 Sophos Diagnostic Utility \(SDU\): Using the malware command line switch](http://www.sophos.com/support/knowledgebase/article/116537.html) <http://www.sophos.com/support/knowledgebase/article/116537.html>.

Once the tools have been run go to step 3. Can a sample be identified?

### **b) Run Source of Infection**

Run the steps from 8 a) Run Sophos Anti-Rootkit and SDU and in addition run the Sophos Source of Infection tool.

- I. Download the Source of Infection Tool  
<http://downloads.sophos.com/misc/SourceOfInfection.exe>.
- II. Click Start | Run | type "cmd" and click **OK**.
- III. Change the directory to the location of the Source of infection tool (cd C:\doc... e.t.c).
- IV. Run to tool with the switches:  

```
sourceofinfection.exe -p -a "[path]"
```

where the [path] is the location of where you are expecting the malware to create or modify a file.

- IV. To locate the log file click Start | Run | type “%temp%” and click **OK**, the filename will be called Sourceofinfection.csv.

For further information on how to use the Sophos Source of Infection tool, see [Article 111505 Sophos Source of Infection Tool](http://www.sophos.com/support/knowledgebase/article/111505.html)  
<http://www.sophos.com/support/knowledgebase/article/111505.html>.

Once the tools have been run go to step 3. Can a sample be identified?

## 9. Cleanup using SMaRT

If you have come from step 2. How was the malware detected? use Sophos Anti-Virus to Cleanup. To attempt cleanup on a detected threat:

- I. Right click the Sophos shield in the system tray.
- II. Click **Open Sophos Endpoint Security and Control**.
- III. Click **Manage quarantine items**.
- IV. Check the tick box for the detected malware.
- V. Click the **Perform action** drop down box and select **Clean up**.
- VI. Click **Yes** to confirm the cleanup.
- VII. Click **Close** .

If you have come from step 13. Isolate the computer from the network, then the choice of SMaRT tools will depend on the type of infection to be dealt with. See the table below for information when the different tools can be used to remediate malware.

For further information on the malware being remediated we recommend looking up the details at the Sophos Threat Center <http://www.sophos.com/en-us/threat-center/threat-monitoring/malware-dashboard.aspx> to help to make an informed decision on the best tool to use.

| Tool              | Virus Type/Scenario  | Prefix      |
|-------------------|----------------------|-------------|
| Sophos Anti-Virus | Exploit              | Exp         |
|                   | Malicious behavior   | Mal & HPmal |
|                   | Trojan               | Troj        |
|                   | Win32 worm           | W32         |
|                   | All other detections |             |

| Tool                               | Virus Type/Scenario  | Prefix      |
|------------------------------------|--|-------------|
| Sophos Bootable Anti-Virus         | Win32 executable file virus  | W32         |
|                                    | Fully compromised operating system   |             |
|                                    | Rootkit/MBR infections   | Troj        |
| Sophos Virus Removal Tool          | Standalone Sophos Virus Removal Tool, can be used with existing anti-virus |             |
| Not required – no local infection* | URL detected as malicious  | Troj or Mal |

**\*Note:**

If a URL is detected as malicious and if no further items (or malicious symptoms) are shown during the full system scan the computer is clean. Go straight to step [20. Run Healthcheck](#).

For further information on how to use the Sophos Virus Removal Tool, see [Article 113298 Sophos Virus Removal Tool](#)  
<http://www.sophos.com/support/knowledgebase/article/113298.html>.

For further information on how to use the Sophos Bootable Anti-Virus, see [Article 52053 Sophos Bootable Anti-Virus](#)  
<http://www.sophos.com/support/knowledgebase/article/52053.html>.

## 10. Cleanup successful?

Has cleanup with SMaRT tools successfully removed the infection?

- If cleanup is successful, go to step [11. Is the computer isolated from the network?](#)
- If cleanup is not successful, go to step [22. Run malware SDU, contact Support](#)

## 11. Is the computer isolated from the network?

- If the computer is not isolated, go to step [12. Is malware redetected? \(computer not isolated from network\)](#).
- If the computer is not isolated but are dealing with a network worm, go to step [16. Is malware redetected? \(computer reconnected to network\)](#).
- If the computer is isolated, go to step [14. Is malware redetected? \(computer isolated from network\)](#).
- If you are unsure if the computer was isolated or not, go to step [12. Is malware redetected? \(computer not isolated from network\)](#).

As a rough guide to know if the item of malware has worm capabilities:

If the estate has more than 20 computers with the same detection within a similar timeframe, this may be a sign of a network worm.

## 12. Is malware redetected? (computer not isolated from network)

After a successful cleanup of the infection, does another detection occur on the computer when the computer is not isolated?

- If the computer does show another detection, then go to step 13. Isolate the computer from the network.
- If the computer does not show another detection, then go to step 20. Run Healthcheck.

## 13. Isolate the computer from the network

Stop all network traffic to the computer, preferably disable the network connection and remove the network cable. Go to step 9. Cleanup using SMaRT.

For assistance with disabling the network connection see the Microsoft article:

<http://windows.microsoft.com/en-GB/windows7/Enable-or-disable-a-network-adapter>

## 14. Is malware redetected? (computer isolated from network)

Does the computer report another detection while in isolation?

- If the computer does see another detection this would indicate an undetected component, possibly a rootkit existing on the computer, go to step 8 b) Run Source of Infection.
- If the computer does not show another detection, go to step 15. Reconnect the computer.

## 15. Reconnect the computer to the network

Put the computer back onto the network, enable the network connection and/or reconnect the network cable. Go to step 16. Is malware redetected? (computer reconnected to network)

## 16. Is malware redetected? (computer reconnected to network)

Does the computer become infected when it is reconnected to the network?

- If detection does occur this indicates that there is network infecting malware attempting to spread, go to step 17. Run Source of Infection Tool.

- If detection does not occur go to step 20. Run Healthcheck.

## 17. Run Source of Infection Tool

Use the Source of Infection (SOI) tool to identify where the malicious files are being distributed from.

- I. Download the Source of Infection Tool  
<http://downloads.sophos.com/misc/SourceOfInfection.exe>.
- II. Start | Run | type "cmd" and click **OK**.
- III. Change the directory to the location of the Source of infection tool (cd C:\doc... etc.)
- IV. Run to tool with the switches:  
`sourceofinfection.exe -n -a "[path]"`  
where the [path] is the location of where you are expecting the malware to create or modify a file.
- V. To locate the log file click Start | Run | type "%temp%" and click **OK**, the filename will be called Sourceofinfection.csv.

For information on how to use the Sophos Source of Infection tool, see *Article 111505 Sophos Source of Infection Tool* <http://www.sophos.com/support/knowledgebase/article/111505.html>.

Go to step 18. Has the source of infection been identified?

## 18. Has the source of infection been identified?

Using the log created by the SOI tool it is possible to find the source of the infection.

- If the source of the infection can be identified, go to step 19. Move to source machine.  
*Note: There may be more than one source of infection.*
- If the source of the infection cannot be identified, go to step 23. Run full SDU, contact Support.

## 19. Move to source machine(s)

Having identified the computer(s) that are dropping the malware onto the network, move to the infection source and repeat the remediation process. Go to section "Before you begin".

## 20. Run Healthcheck

Download the Healthcheck Tool from <http://www.sophos.com/misc/SophosHealthCheck.exe> and then run the program from the command line. If using Windows Vista or above, the command prompt needs to be run as an administrator. This will confirm if Sophos Anti-Virus is working correctly. For further information on the Sophos Healthcheck tool see [Article 112843 Sophos Healthcheck Tool](#)  
<http://www.sophos.com/support/knowledgebase/article/112843.html>.

Go to step [21. Healthcheck Passed?](#)

## 21. Healthcheck Passed?

- I. To go Start | Run | type '%temp%' and click **OK**.
- II. Open the log file called 'SophosHealthCheckLog\_Date\_time.txt' to view the results of the Healthcheck tool.

The last line of the log file will summarise the results of the Healthcheck tool.

- If no errors are reported the system is now clean.
- If warnings are reported, review them and action as required. For assistance, go to step [23. Run full SDU, contact Support](#).
- If errors are reported, go to step [23. Run full SDU, contact Support](#).

## 22. Run malware SDU, contact Support

Collect an SDU log from the computer using the `-malware` switch:

- I. Start | Run | type "cmd" and click **OK**.
- II. In the command prompt window browse to the SDU directory:  
`cd C:\Program Files\Sophos\Sophos Diagnostic Utility`
- III. Run the SDUCLI application with the `-malware` switch:  
`sducli.exe -malware`

For further information on running the SDU logging utility see [Article 116537 Sophos Diagnostic Utility \(SDU\): Using the malware command line switch](#)  
<http://www.sophos.com/support/knowledgebase/article/116537.html>.

Contact Sophos Technical Support by phone, email or web:

- a. Get help on the SophosTalk Community Forums <http://community.sophos.com>.
- b. Ring your local support number, the relevant numbers are found <http://www.sophos.com/en-us/about-us/contact-us.aspx>.

- c. Send an email to [support@sophos.com](mailto:support@sophos.com).
- d. Send a web request via the address <https://secure.sophos.com/support/query>.

## 23. Run full SDU, contact Support

Collect a full SDU log from the computer

- I. Start | All Programs | Sophos | Sophos Diagnostic Utility | Sophos Diagnostic Utility.
- II. Select both options.
- III. Click **Continue**. The utility will take several minutes to collect all of the data that was selected.
- IV. When the utility has finished collecting the data, **Locate archive** shows the location of the zip archives of the collected files.
  - I. Click **Send mail to Sophos**. All the information collected will be saved in an archive file named COMPUTERNAME\_DDMMYYYY\_HHMMSS\_sdulog.zip.

For further information on running the SDU logging utility see [Article 33556 Sophos Diagnostic Utility \(SDU\): how to use it to send files to Sophos Technical Support](http://www.sophos.com/support/knowledgebase/article/33556.html)  
<http://www.sophos.com/support/knowledgebase/article/33556.html>.

Contact Sophos Technical Support by phone, email or web:

- a. Get help on the SophosTalk Community Forums <http://community.sophos.com>.
- b. Ring your local support number, the relevant numbers are found <http://www.sophos.com/en-us/about-us/contact-us.aspx>.
- c. Send an email to [support@sophos.com](mailto:support@sophos.com).
- d. Send a web request via the address <https://secure.sophos.com/support/query>.

## Legal Notices

Copyright © 2011-2012 Sophos Limited. 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 license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to [support@sophos.com](mailto:support@sophos.com) or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>