Anti-Virus Comparative

Enigma Software

SpyHunter 4 Malware Security Suite

Language: English
April 2017

Last Revision: 29th May 2017

www.av-comparatives.org

Commissioned by Enigma Software

Table of Contents

Enigma Software SpyHunter 4

This report was commissioned by Enigma Software. We have reviewed SpyHunter 4.25.6.4782 by Enigma Software, and tested its malware removal capabilities using the latest build and updates available at time of testing.

Which versions of Windows does it work with?

Windows XP, Vista, 7, 8, 8.1, 10

Where can I find more information about the product?

http://www.enigmasoftware.com/products/spyhunter/

Summary

We found SpyHunter to be an easy-to-use and effective tool for cleaning up malware infections. Installing the program, running scans and removing any malware infections found are all very straightforward tasks that could be performed by non-expert users. The program achieved a creditable score in our malware removal test, and we consider the *DNS Settings* feature to be very useful, as it helps to prevent changes to the DNS configuration by malware. We feel that SpyHunter could be a valuable addition to any computer user's security arsenal, if used in addition to a full antivirus program with real-time protection.

We note that the subscription period is 6 months.

Installing the product

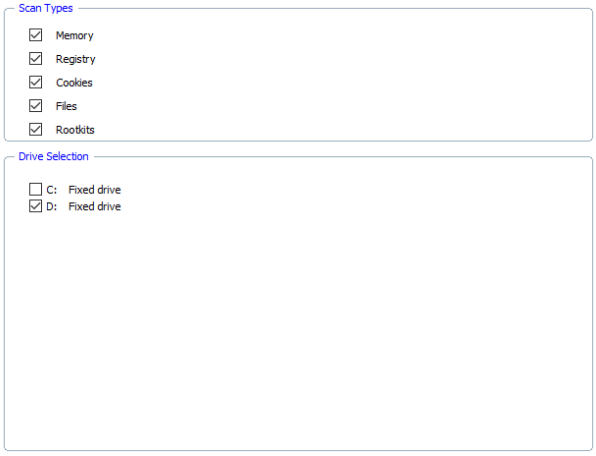
Installation of SpyHunter is very simple and takes only a few clicks. The user has to select the language to be used, and accept the end-user license agreement. The wizard displays the vendor's description of the product, along with information about the limitations of the trial version:

We feel that the description above may be confusing to some users, as it states that SpyHunter provides "rigorous protection against the latest spyware threats..." – which might imply that it prevents any spyware being installed, as opposed to removing it after the infection.

Main program window

The program's main functionality is accessed from the buttons in the left-hand pane of the window, these being *Malware Scan, Registry Scan, DNS Settings, System Guards, Spyware HelpDesk,* and *Settings*.

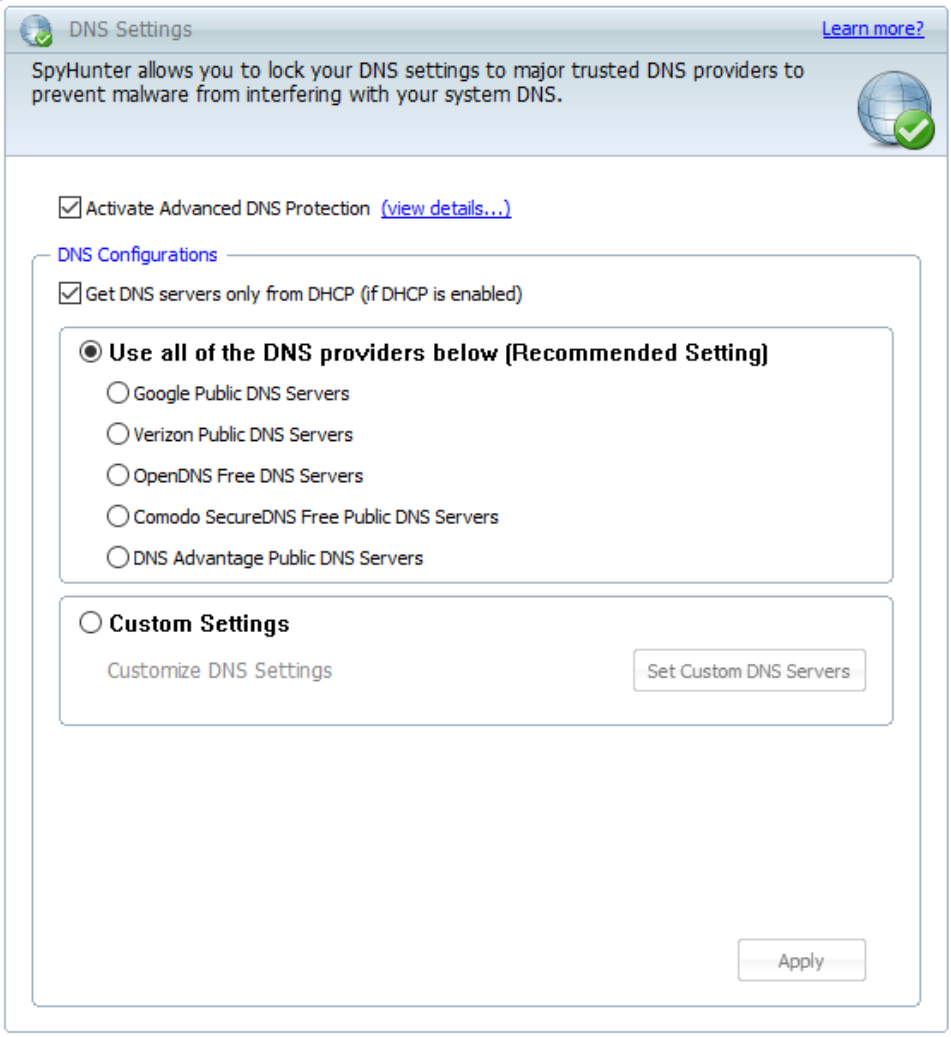
Malware Scan lets the user run a scan for malicious software, with the option of a quick or full scan. The submenu *Custom Scan* provides a choice of elements to be included in the scan; if *Files* is selected, the drives to be scanned can be selected:



We could not find a means of scanning individual folders or files, however.

Registry Scan does not in itself provide any functionality, but advertises another Enigma Software product, *RegHunter*.

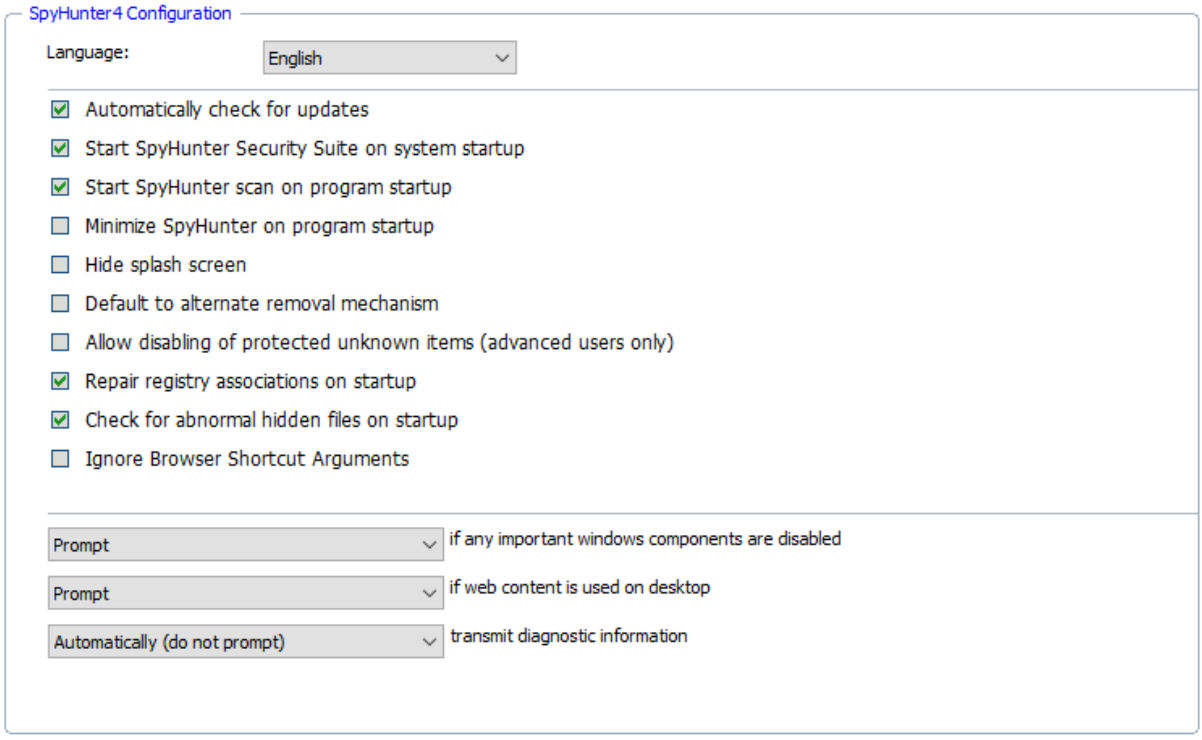
DNS Settings "allows you to lock your DNS settings to major trusted DNS providers to prevent malware from interfering with your system DNS", according to the feature's own description of itself. It provides a simple interface for adding a list of reliable public DNS servers to Windows' network connection settings, and warns of any attempt to change these. As many malicious programs change DNS settings, e.g. in order to prevent the download of antimalware tools by the user, protecting DNS settings is a potentially valuable tool in protecting the system against the effects of malware.



System Guards allows the user to block or allow specific processes. Under *Malware and Threat Items*, known malware processes that have been blocked by the program are listed, while *Safe Items* shows Windows components that have been allowed. *User Added Items* shows processes which have been blocked or allowed by the user responding to the prompt shown by SpyHunter when an unknown process runs for the first time. Finally, *Active X Guarded Items* lists Active X controls (Internet Explorer customisations) known to be malicious, which will be blocked by SpyHunter.

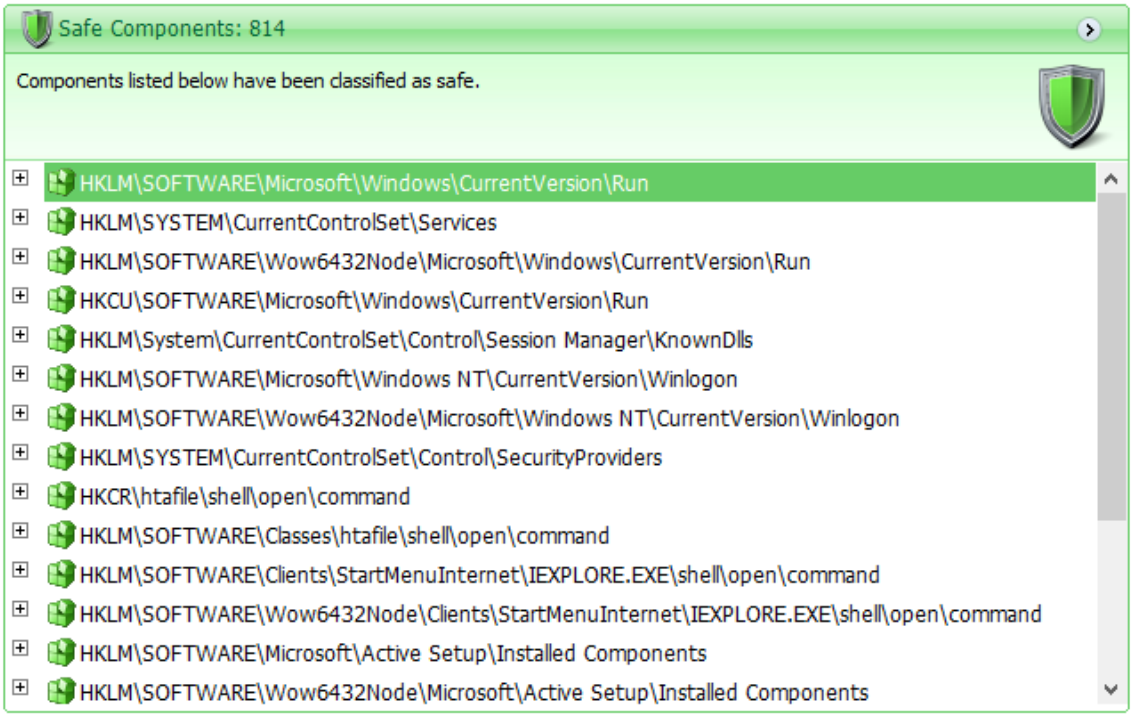
Spyware HelpDesk has support-related links, enabling the user to submit or view support tickets or open the support pages on the vendor's website.

Settings provides configuration and scheduling options:



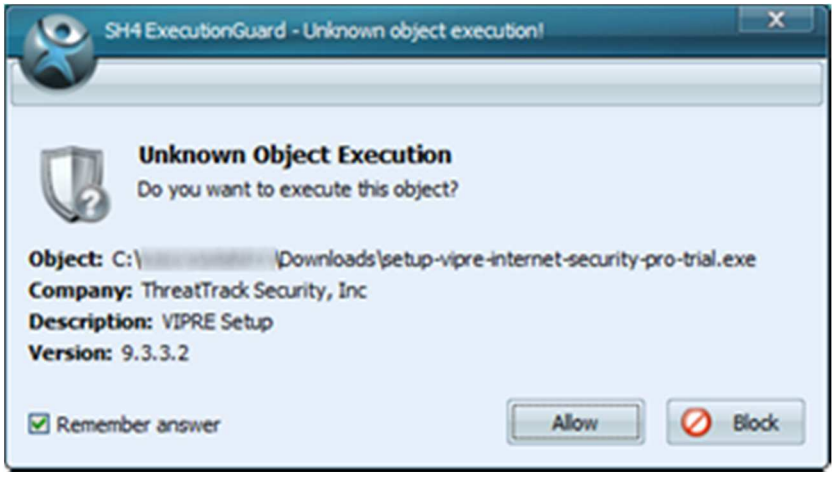
Using the program

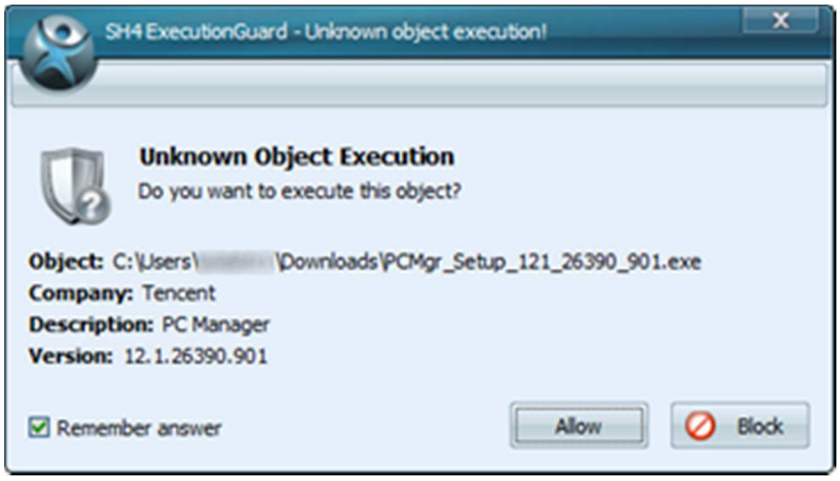
After installation, an initial scan is run, which takes about 15 minutes. No malware was found on our clean test system, as was to be expected. An overview of the registry keys scanned is displayed:



When we scanned a USB flash drive containing the dropper ("installer") files for our 10 malware samples, we found that only one of them was detected, even though SpyHunter detected all 10 samples post-execution.

As part of this user-interface review (and separately from the actual malware removal test described in the next section), we actually infected the test system with one of the malware samples and then ran a scan with SpyHunter to remove it. When doing this, we noted that when any program unknown to SpyHunter (which includes all the malware samples used in our test) is first run, SpyHunter asks the user whether to allow or block the program. Only a relatively small selection of clean programs is known/allowed by default, and installers for two very popular and digitally signed antivirus programs (for example) produce the prompt when executed:





The user can run the program – whatever it is – by simply clicking *Allow*. Once we had executed the malware and run a SpyHunter scan, SpyHunter displayed a list of the threats found, along with a big green *Fix Threats* button, which removed all of the malware items found.

When the scan results are displayed, the user can deselect any items to be removed by clearing the tick (checkmark) from the appropriate box in the results list:

Once cleaning is complete, the program informs the user that a reboot is required, and provides a convenient button for doing this.

What are the program's help features like?

The *Help* button in the top right-hand corner of the main window opens the product's online User Guide, which is like an online manual.[1]

[1] http://www.enigmasoftware.com/sh4help/index.php

Malware Removal Test

In order to evaluate the malware removal capabilities of SpyHunter, we tested it against 10 different malware samples. The test was performed with the latest available definitions at the time of testing under Microsoft Windows 10 64-Bit RS1 (English).

Used samples

Below is a list of the used samples. Readers can ignore the IDs in parenthesis; we mention them only as a reference for the tested AV vendor to identify them based on the samples they received from us after this test[2].

Sample 1 (f365f6): Banker trojan

Sample 2 (c68610): Tescrypt ransomware

Sample 3 (3d0f56): Bunitu trojan

Sample 4 (169e15): Omaneat trojan

Sample 5 (ab05af): CeeInject trojan

Sample 6 (586b59): Dodiw backdoor

Sample 7 (00ab96): Sality virus

Sample 8 (0a912f): Kovter trojan

Sample 9 (449001): Dacic trojan

Sample 10 (22d039): Boostro trojan

Test Procedure

- Thorough malware analysis for each sample, to see exactly what changes are made
- Infect physical machine with one threat, reboot and make sure that threat is fully running
- Install and update the anti-virus product
- *If not possible, reboot in safe mode; if safe mode is not possible and in case a rescue disk of the corresponding AV-Product is available, use it for a full system scan before installing*
- Run thorough/full system scan and follow instructions of the anti-virus product to remove the malware, as a typical home-user would do
- Reboot machine
- Manual inspection/analysis of the system for malware removal and remnants

[2] To avoid providing to malware authors information that could be potentially useful for them in improving their creations, this report contains only general information about the malware/remnants, without any technical instructions/details.

Ratings

We allowed certain negligible/unimportant traces to be left behind, mainly because a perfect score can't be reached due to the behaviour/system-modifications made by some of the malware samples used. The "removal of malware" and "removal of remnants" are combined into one dimension and we took into consideration also the convenience. The ratings are given as follows:

a) Removal of malware/traces

- Malware removed, only negligible traces left (A)
- Malware removed, but some executable files, MBR and/or registry changes (e.g. loading points, etc.) remaining (B)
- Malware removed, but annoying or potentially dangerous problems remaining (e.g. error messages, compromised hosts file, disabled task manager, disabled folder options, disabled registry editor, detection loop, etc.) (C)
- Only the malware dropper has been neutralized and/or most other dropped malicious files/changes were not removed, or system is no longer normally usable; dropped malicious files are still on the system; removal failed (D)

b) Convenience:

- Removal could be done in normal mode (A)
- Removal requires booting in Safe Mode or other built-in utilities and manual actions (B)
- Removal requires Rescue Disk (C)
- Removal or install requires contacting support or similar; removal failed (D)

Scoring system

The following scoring system has been used:

AA = 100	
AB = 90	The scoring is then given based on the rounded mean value reached:
AC = 80	
BA = 70	
BB = 60	86-100 points: Very good
BC = 50	71-85 points: Good
CA = 40	56-70 points: Mediocre
CB = 30	Lower than 56 points: Bad
CC = 20	
DD = 0	

Results

Based on the above scoring system, we get the following summary results:

		SpyHunter	Comments
Sample	1	AA	Malware removed
	2	AA	Malware removed
	3	AA	Malware removed
	4	BA	Loading point not removed
	5	AA	Malware removed
	6	AA	Malware removed
	7	CA	Annoying problems remaining
	8	CA	Annoying problems remaining
	9	AA	Malware removed
	10	BA	Dropped malware not removed
Points	**ø**	**82**	

Scores between 71 and 85 points are considered to represent "Good" malware removal capabilities.

Our test indicated that under some circumstances, a Quick Scan by SpyHunter could possibly miss older infections (based on the timestamp of registry entries created by the malware), so running a Full Scan is advisable if the infection is not very recent.

Summary

Good points

- Quick and easy to install
- Running scans and removing (installed) malware found is simple
- DNS protection feature is valuable, and easy to use
- Good malware removal capability

Areas for improvement

- Malware droppers rarely detected before or during execution
- "Unknown Object Execution" alerts displayed for common clean software installers
- Timestamps of registry entries impact the ability to detect/remove malware

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (May 2017)