Anti-Virus Comparative

Malware Removal Test

Language: English
October 2013
Last Revision: 21st November 2013

www.av-comparatives.org

Table of Contents

Tested Products

- AhnLab V3 Internet Security 8.0
- avast! Free Antivirus 2014
- AVIRA Internet Security 2014
- Bitdefender Internet Security 2014
- BullGuard Internet Security 2014
- Emsisoft Anti-Malware 8.1
- eScan Internet Security 14.0
- ESET Smart Security 7.0
- F-Secure Internet Security 2014
- Fortinet FortiClient 5.0
- G DATA Internet Security 2014
- Kaspersky Internet Security 2014
- Microsoft Security Essentials 4.3
- Panda Cloud Antivirus Free 2.2.1
- Sophos Endpoint Security 10.2
- ThreatTrack Vipre Internet Security 2014

Introduction

This test focuses only on the malware removal/cleaning capabilities, therefore all samples used were samples that the tested anti-virus products were able to detect. It has nothing to do with detection rates or protection capabilities. Of course, if an anti-virus is not able to detect the malware, it is also not able to remove it. The main question is if the products are able to successfully remove malware from an already infected system. The test report is aimed to typical home users and not administrators or advanced users who may have the knowledge for advanced/manual malware removal/repair procedures. Most often users come with infected PC's with no (or outdated) AV-software to computer repair stores. The methodology used considers this situation: an already infected system that needs to be cleaned.

The test was performed in October/November 2013 under Microsoft Windows 7 Professional SP1 64-Bit. Only products whose vendors subscribed to the 2013 public main test-series, and did not opt out of this test, were tested.

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

Malware selection

The samples have been selected according to the following criteria:

- All anti-virus products must be able to detect the malware dropper used when inactive
- The sample must have been prevalent (according to metadata) and/or seen in the field on at least two PC's of our local customers in 2013.
- The malware must be non-destructive (in other words, it should be possible for an anti-virus product to repair/clean the system without the need for replacing Windows system files etc.). It must also show common malware behavior under the operating system used, in order to represent also behaviors observed by many other malware samples.

We randomly took 10 malware samples from the pool of samples matching the above criteria. Additionally, we took one old sample that was used last year, to see if there was an improvement and/or if the removal capabilities changed.

Used samples

Below is a list of the used samples[1]. Readers can ignore the IDs in parenthesis; we mention them only as a reference for the tested AV vendors to identify them based on the samples they received from us after this test[2].

Sample 1 (2d1): This sample is a widespread trojan horse.

Sample 2 (7b6): This sample is a very widespread trojan horse.

Sample 3 (23e): This sample is a widespread trojan horse.

Sample 4 (28d): This sample is a very widespread worm.

Sample 5 (380): This sample is a widespread backdoor.

Sample 6 (0a3): This sample is a widespread worm.

Sample 7 (01b): This sample is a widespread trojan horse.

Sample 8 (002): This sample is a widespread backdoor.

Sample 9 (2f0): This sample is a widespread ransom trojan horse that threatens to encrypt files.

Sample 10 (851): This sample is a very old worm, which still works on Windows 7 64 bit.

Sample 11 (473): This sample is a typical widespread ransom trojan horse that takes the system hostage. This common malware shows the importance of rescue disks for home users.

[1] Initially we tested more samples, but we removed/replaced them with other samples afterwards, as e.g. their malware behaviour/disinfection process was identical to samples already included. The samples used were provided to the vendors after the test, for verification purposes.

[2] To avoid providing information to malware authors which could be potentially useful for them in improving their creations, this public 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 (e.g. error messages, compromised hosts file, disabled task manager, disabled folder options, disabled registry editor, detection loop, etc.) remaining (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)

Award system

The following award/scoring system has been used:

AA = 100
AB = 90
AC = 80
BA = 70
BB = 60
BC = 50
CA = 40
CB = 30
CC = 20
DD = 0

The awards are then given based on the rounded mean value reached:

86-100 points: ADVANCED+
71-85 points: ADVANCED
56-70 points: STANDARD
Lower than 56 points: TESTED

Results

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

	Sample											Points
	1	2	3	4	5	6	7	8	9	10	11	∅
AhnLab	DD	AA	AA	AA	BA	BA	AA	AA	AA	AB	DD	75
Avast	AA	AA	AA	AA	AA	AA	BA	AA	CA	AA	BC	87
AVIRA	AA	AA	AA	AA	AA	AA	AA	AA	BA	BB	AC	92
Bitdefender	AA	AA	AA	AA	AA	AA	AA	AA	AA	AB	AC	97
BullGuard	AA	BA	BA	BA	BA	AA	AA	BA	AA	BC	DD	73
Emsisoft	AA	AA	AA	AA	BA	AA	AA	AA	CA	BB	DD	79
eScan	AA	AA	AA	AA	BA	BA	AA	AA	AA	AB	DD	85
ESET	AA	AA	AA	AA	AA	AA	BA	AA	AA	BC	BC	88
F-Secure	AA	DD	AA	AA	AA	AA	AA	AA	AA	BC	BC	82
Fortinet	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	DD	91
G DATA	AA	AA	AA	BA	BA	BA	AA	AA	CA	DD	BC	73
Kaspersky Lab	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AC	98
Microsoft	AA	AA	BA	AA	AA	AA	AA	BA	AA	BA	DD	83
Panda	AA	AA	AA	AA	AA	AA	BA	AA	AA	AB	DD	87
Sophos	AA	AA	AA	AA	BA	AA	AA	AA	BA	BC	BC	85
ThreatTrack Vipre	BA	BA	BA	AA	BA	BA	BA	BA	CA	AB	DD	65

Good malware detection is very important to find existing malware that is already on a system. However, a high protection or detection rate of a product does not necessarily mean that a product has good removal abilities. On the other hand, a product with low detection rate may not even find the infection and therefore not be able to remove it. Most AV vendors may by now already have addressed and fixed/improved the next releases of their products based on our findings in this report.

Some users may wrongly assume that anti-virus products just delete binary files and do not fix anything else, e.g. the registry. This report is also intended as a little informational document to explain that professional anti-virus products do much more than just deleting malicious files.

We advise users to make regular backups of their important data and to use e.g. imaging software so that they can restore their systems if necessary.

Additional Free Malware Removal Services/Utilities offered by the vendors

	Boot-Disk[3] available	Free Removal-Tools
AhnLab	**-**	-
Avast	**YES**	-
AVIRA	**YES**	http://www.avira.com/en/downloads#tools
Bitdefender	**YES**	http://www.bitdefender.com/free-virus-removal/
BullGuard	**-**	-
Emsisoft	**-**	http://www.emsisoft.com/en/software/eek/
eScan	**YES**	http://escanav.com/english/content/products/MWAV/escan_mwav.asp
ESET	**YES**	http://kb.eset.com/esetkb/index?page=content&id=SOLN2372
F-Secure	**YES**	http://www.f-secure.com/en/web/labs_global/removal-tools
Fortinet	**-**	http://www.fortiguard.com/antivirus/malware_removal.html
G DATA	**YES**	http://www.gdata.de/support/downloads/tools.html
Kaspersky Lab	**YES**	http://support.kaspersky.com/viruses
Microsoft	**YES**	http://www.microsoft.com/security/scanner/en-us/default.aspx
Panda	**YES**	http://www.pandasecurity.com/homeusers/downloads/repair-utilities/
Sophos	**YES**	-
ThreatTrack Vipre	**-**	http://www.vipreantivirus.com/live/

The customer support of AV vendors may help the users in the malware removal process. In most cases, such support services are charged separately, but several vendors may provide their customers with malware removal help for free (i.e. service included in the charged product fee). We suggest that users with a valid license try contacting the AV vendor's support service by email if they have problems in removing certain malware or issues while installing the product.

How some AV vendors could improve the help provided for home users with an infected system:

- provide/include a rescue disk in the product package (or provide links to download it)
- provide up-to-date offline-installers (e.g. if malware blocks access to the vendors website)
- do not require the user to login into accounts to install products or to activate the cleaning features (as malware could intercept passwords etc.) and provide cleaning abilities in trial mode too (for infections which do not allow the product to be registered/activated)
- check for active malware before attempting installation
- provide the possibility to download installers which get random names at each download (in order to avoid that malware hinders the installation of security software based on file names
- point to standalone tools if installation fails or if malware could not be successfully removed
- include tools/features inside the product to fix/reset certain registry entries/system changes
- promote more prominently the availability of additional free malware-removal utilities provided, and free malware-removal procedures/support on the website, manuals, inside the product or when an active infection is found

[3] Included in the standard package without extra charges (and without the need to contact/request it from the vendor's support personnel).

Awards reached in this test

The following awards/certification levels were reached by the various products[4] in this specific test:

AWARDS	PRODUCTS
	Kaspersky Lab Bitdefender AVIRA Fortinet ESET Avast Panda
	eScan Sophos F-Secure Emsisoft AhnLab BullGuard G DATA
	ThreatTrack Vipre
	-

[4] Microsoft Security Essentials was tested out-of-competition and is therefore not included in the awards page.

Copyright and Disclaimer