

Anti-Virus Comparative



Malware Removal Test

Language: English

March - October 2014

Last Revision: 1st December 2014

www.av-comparatives.org

Table of Contents



Tested Products	3
Introduction	4
Test-Procedure	4
Malware selection	4
Used samples	5
Ratings	7
Award system	7
Results	8
Additional Free Malware Removal Services/Utilities	9
Award levels reached in this test	10
Copyright and Disclaimer	11



Tested Products

The following products were tested from March to October 2014 concerning their malware removal capabilities. During this period, we always used the most up-to-date product version available before testing against the malware samples (due to that, no version numbers are given).

- AhnLab V3 Internet Security
- avast! Free Antivirus
- AVG Internet Security
- AVIRA Internet Security
- Bitdefender Internet Security
- BullGuard Internet Security
- Emsisoft Anti-Malware
- eScan Internet Security
- ESET Smart Security
- F-Secure Internet Security
- Fortinet FortiClient
- Kaspersky Internet Security
- Lavasoft Ad-Aware Free Antivirus+
- Microsoft Windows Defender
- Panda Cloud Antivirus Free
- Sophos Endpoint Security
- ThreatTrack Vipre Internet Security

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 Most often users come with infected PC's with no (or outdated) AV-software to computer repair stores.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 from March to October 2014 under Microsoft Windows 8.1 64-Bit (English). Only products whose vendors subscribed to the 2014 public main test-series, and did not opt-out of this test, are included in this report.

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 (full) security 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 2014.
- 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.).

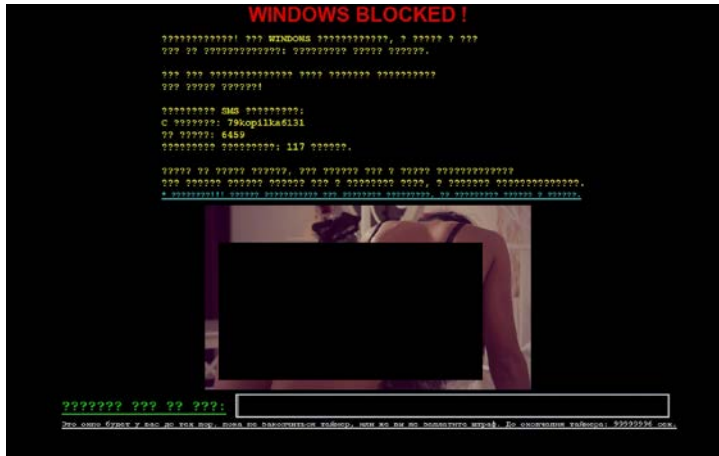
We randomly took 30 malware samples from the pool of samples matching the above criteria. Additionally, we took one old sample that was used last year, to see if there was an improvement and/or if the removal capabilities changed.

Used samples

Below is a list of the used samples¹. 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 test².

Sample 1 (5860): This sample is a very old widespread worm.

Sample 2 (81c9): This sample is a widespread trojan horse which locks the screen. This common malware shows the importance of rescue disks for home users.



Sample 3 (98bc): This sample is a widespread trojan horse.

Sample 4 (8ecf): This sample is a widespread trojan horse.

Sample 5 (ee44): This sample is a widespread trojan horse.

Sample 6 (7f91): This sample is a widespread trojan horse which locks the screen.



Sample 7 (9c13): This sample is a widespread trojan horse which encrypts files.

Sample 8 (74c1): This sample is a widespread backdoor.

Sample 9 (53b1): This sample is a widespread backdoor.

Sample 10 (3d35): This sample is a widespread trojan horse.

¹ The samples used were provided to the vendors after the test, for verification purposes.

² To avoid providing to malware authors information that 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.

- Sample 11 (37e2):** This sample is a widespread backdoor.
- Sample 12 (ef6e):** This sample is a widespread trojan horse.
- Sample 13 (7c8a):** This sample is a widespread trojan horse.
- Sample 14 (e636):** This sample is a widespread trojan horse.
- Sample 15 (b0c0):** This sample is a widespread trojan horse.
- Sample 16 (a2e7):** This sample is a widespread trojan horse.
- Sample 17 (ea5e):** This sample is a widespread trojan horse.
- Sample 18 (2d00):** This sample is a widespread trojan horse.
- Sample 19 (d135):** This sample is a widespread trojan horse.
- Sample 20 (c0aa):** This sample is a widespread backdoor.
- Sample 21 (769a):** This sample is a very widespread backdoor.
- Sample 22 (712e):** This sample is a widespread trojan horse.
- Sample 23 (5a4c):** This sample is a widespread backdoor.
- Sample 24 (6d54):** This sample is a widespread password-stealing trojan horse.
- Sample 25 (dd7c):** This sample is a widespread backdoor.
- Sample 26 (b4a2):** This sample is a widespread backdoor.
- Sample 27 (719c):** This sample is a widespread trojan horse.
- Sample 28 (8a23):** This sample is a widespread backdoor.
- Sample 29 (efe7):** This sample is a widespread ransom trojan horse.
- Sample 30 (ed5e):** This sample is a widespread trojan horse, which locks the screen.



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.

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	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		∅
AhnLab	BA	DD	BA	AA	AA	DD	BA	BA	BA	CA	BA	AA	BA	AA	DD	BA	AA	AA	AA	DD	AA	BA	AA	AA	CA	AA	BA	AA	BA	AA	DD	68
Avast	BA	DD	BA	AA	AA	AC	AA	AA	AA	AA	AA	AA	BA	DD	CC	AA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	BA	AA	BA	DD	81
AVG	BA	AB	BA	AA	AA	BC	CA	AA	AA	AA	AA	AA	BA	DD	AB	AA	AB	AA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AB	88
Avira	BA	AC	BA	AA	AA	BB	BA	AA	AA	CA	BA	AA	BA	AA	AC	BA	AB	AA	AA	BA	BA	AA	AA	AA	CA	AA	AA	AA	CA	DD	80	
Bitdefender	AA	BC	BA	AA	AA	AC	AA	AA	AA	CA	AA	AA	BA	AA	CC	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	DD	88
BullGuard	AA	AB	BA	AA	AA	BB	AA	AA	BA	CA	AA	AA	BA	DD	AA	AA	AA	AA	AA	AA	AA	BA	BA	BA	CA	AA	AA	BA	AA	DD	81	
Emsisoft	BA	AB	BA	BA	AA	BB	BA	AA	AA	CA	DD	AA	BA	AA	CB	BA	AB	AA	AA	BA	BA	BA	AA	AA	CA	AA	BA	AA	AA	DD	75	
eScan	BA	AB	BA	AA	AA	AB	AA	AA	AA	CA	AA	AA	BA	AA	CB	AA	AB	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	DD	87
ESET	BA	BC	BA	AA	AA	BC	AA	AA	AA	AA	AA	AA	BA	DD	CC	BA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AA	BA	BC	83
F-Secure	BA	BC	BA	AA	AA	BC	BA	AA	AA	AA	BA	AA	BA	DD	DD	AA	CB	AA	AA	BA	AA	BA	AA	AA	CA	AA	AA	AA	CA	DD	73	
Fortinet	BA	DD	BA	BA	AA	DD	CA	AA	AA	AA	BA	AA	BA	DD	CA	AA	AA	AA	AA	BA	AA	AA	AA	AA	CA	AA	BA	AA	CA	AB	75	
Kaspersky Lab	AA	AC	BA	AA	AA	AC	AA	DD	AA	AA	AA	AA	BA	AA	AC	AA	AC	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AA	BA	DD	87
Lavasoft	AA	BC	BA	BA	AA	DD	AA	AA	AA	CA	AA	AA	AA	AA	AC	AA	DD	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	DD	84
Microsoft	BA	AC	AA	AA	AA	AC	CC	AA	AA	CA	BA	AA	BA	DD	CC	AA	BA	DD	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AC	BA	DD	75
Panda	AA	AB	BA	AA	AA	AC	AA	DD	AA	CA	AA	AA	BA	AB	AB	AA	BB	AA	AA	DD	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AB	86
Sophos	BA	DD	BA	AA	AA	DD	BA	BA	AA	CA	BA	AA	BA	DD	DD	AA	DD	AA	AA	BA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	DD	70
ThreatTrack Vipre	BA	AB	BA	AA	AA	BB	CA	AA	BA	CA	BA	AA	BA	AA	DD	BA	DD	AA	AA	BA	AA	BA	AA	CA	AA	BA	BA	BA	BA	DD	70	

Additional Free Malware Removal Services/Utilities offered by the vendors

	Boot-Disk ³ available	Free Removal-Tools
AhnLab	-	http://global.ahnlab.com/en/site/download/removal/removalList.do
Avast	YES	-
AVG	YES	http://www.avg.com/eu-en/virus-removal
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=S0LN2372
F-Secure	YES	http://www.f-secure.com/en/web/labs_global/removal-tools
Fortinet	-	http://www.fortiguard.com/antivirus/malware_removal.html
Kaspersky Lab	YES	http://support.kaspersky.com/viruses
Lavasoft	YES	-
Microsoft	YES	http://www.microsoft.com/security/scanner/en-us/default.aspx
Panda	YES	http://www.pandasecurity.com/usa/homeusers/support/tools.htm
Sophos	YES	https://www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx
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 products⁴ in this specific test:

AWARDS	PRODUCTS
	Bitdefender AVG eScan Kaspersky Lab Panda
	Lavasoft ESET Avast BullGuard Avira Emsisoft Fortinet F-Secure
	ThreatTrack Vipre Sophos AhnLab
	-

⁴ Microsoft Windows Defender was tested out-of-competition and is therefore not included in the awards page.

Copyright and Disclaimer

This publication is Copyright © 2014 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives (December 2014)