Anti-Virus Comparative

Malware Removal Test

Language: English

March - September 2015
Last Revision: 28th September 2015

www.av-comparatives.org

Table of Contents

Tested Products

The following products were tested from March to September 2015 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).

- Avast Free Antivirus
- AVG Internet Security
- AVIRA Antivirus Pro
- 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 Free Antivirus
- 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 Most often users come with infected PC's with no (or outdated) AV-software to computer repair stores.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 September 2015 under Microsoft Windows 8.1 64-Bit (English). Only products whose vendors subscribed to the 2015 public main test-series, and did opt-in for 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 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 2015.
- 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 and kept 35 malware samples from the pool of samples matching the above criteria.

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 (dbd8e1): Crowti trojan
Sample 2 (0beb7c): ServStart trojan
Sample 3 (0be60b): Redosdru trojan
Sample 4 (0f0623): Miuref trojan
Sample 5 (2804a8): Fareit trojan
Sample 6 (ab36a4): Neurevt.C trojan
Sample 7 (6121fc): Delf trojan
Sample 8 (af7a5d): Dumaru worm
Sample 9 (e70d1d): Necurs trojan
Sample 10 (14253e): Exchrom trojan
Sample 11 (43c7ab): Xtrat backdoor
Sample 12 (9e3efc): Neurevt.A trojan
Sample 13 (d69dc1): Zbot.A trojan
Sample 14 (23cce1): Androm backdoor
Sample 15 (e31774): Vawtrak backdoor
Sample 16 (ed831d): Zbot.V trojan
Sample 17 (2e0356): Dorkbot worm
Sample 18 (e7f74a): Simda backdoor
Sample 19 (46e08a): Jenxcus worm
Sample 20 (bcae54): Carberp trojan
Sample 21 (0123df): Killav trojan
Sample 22 (97d025): Shutdowner trojan
Sample 23 (1e6b3a): Yoof worm
Sample 24 (632b17): FrauDrop trojan
Sample 25 (dc0308): Slipafext trojan
Sample 26 (a0aa11): Tinba trojan
Sample 27 (ff2d77): Bunitu trojan
Sample 28 (a808c6): Crugup backdoor
Sample 29 (c0d9ab): Fynloski backdoor
Sample 30 (c09b90): Banload trojan
Sample 31 (9811b1): FakeAV trojan
Sample 32 (154c0d): Tepfer trojan
Sample 33 (5599dc): Injector trojan
Sample 34 (1018f7): DarkKomet backdoor
Sample 35 (5e3354): Betabot trojan

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.

[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.

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:

		Avast	AVG	Avira	Bitdefender	BullGuard	Emsisoft	eScan	ESET	F-Secure	Fortinet	Kaspersky Lab	Lavasoft	Microsoft	Panda	Sophos	ThreatTrack Vipre
Sample	1	AA	AA	AA	AA	BA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA
	2	BA	BA	AA	AA	BA	BA	AA	BA	AA	AA	AA	AA	AA	BA	BA	AA
	3	AA	AA	AA	AA	AA	AA	AA	BA	AA	AA	AA	DD	AA	BA	AA	AA
	4	AA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
	5	CA	CA	CA	CA	CA	CA	CA	CA	CA	CA	CA	CA	CA	BA	CA	CA
	6	AA	AA	AA	AA	AA	AA	BA	AA	AB	DD	AA	AA	BA	AB	AA	BA
	7	AA	AA	BA	AA	AA	AA	AA	BA	BA	AA	AA	AA	AA	AA	BA	BA
	8	AA	AA	AA	AA	AA	BA	AA	AA	BA	BA	AA	AA	AA	BA	BA	AA
	9	CC	AC	BC	BC	BB	CA	CC	AA	DD	DD	AC	DD	AA	CA	DD	CB
	10	AA	BA	AA	AA	AA	AA	BA	AA	BA	BA	AA	AA	AA	BA	BA	BA
	11	BA	BA	BA	BA	BA	BA	BA	BA	BA	BA	AA	BA	BA	BA	BA	BA
	12	AA	AA	AA	AA	AA	AB	AA	AA	AB	AA	AC	AA	AA	AB	AA	DD
	13	AA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	DD	AA	AA	AA
	14	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	BA
	15	AA	AA	AA	AA	BA	AA	BA	BA	AA	AA	AA	AA	AA	AA	AA	AA
	16	AA	AA	AA	AA	BA	AA	AA	AA	BA	DD	AA	AA	DD	AA	AA	DD
	17	BA	BA	AA	AA	BA	BA	AA	AA	BA	BA	AA	AA	BA	AA	BA	BA
	18	BA	BA	BA	BA	BA	AA	BA	BA	BA	DD	AA	BA	AA	DD	DD	AA
	19	AA	AA	DD	DD	DD	DD	BA	DD	DD	DD	AA	DD	AA	DD	DD	DD
	20	AA	AA	AA	AA	AA	AA	BA	AA	AA	AA	AA	BA	BA	AA	AA	AA
	21	AA	CA	BA	AA	AA	BA	AA	AA	BA	CA	AA	AA	CA	BA	BA	CA
	22	DD	DD	DD	DD	DD	DD	DD	DD	DD	DD	DD	DD	DD	DD	DD	DD
	23	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	BA	BA	BA
	24	AA	AA	AA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AA
	25	BA	BA	BA	BA	BA	BA	AA	BA	BA	BA	AA	BA	BA	AA	BA	BA
	26	AA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
	27	AA	BA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
	28	AA	AC	AA	AA	BA	DD	BA	AA	BC	AA	AA	AA	AA	AA	AC	DD
	29	AA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
	30	AA	AA	AA	AA	BA	AA	BA	AA	AA	AA	AA	AA	AA	AA	AA	AA
	31	AA	AA	BA	AA	BA	BA	BA	BA	AA	BA	AA	AA	AA	BA	AA	BA
	32	AA	AA	AA	AA	BA	BA	BA	BA	AA	AA	AA	BA	AA	BA	AA	BA
	33	AA	AA	AA	AA	AA	DD	AA	BC	AA	AA	AC	BC	AA	AC	DD	DD
	34	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA	BA	BA	BA
	35	AA	AA	AA	AA	AA	AA	AB	AC	AA	AA	AC	BC	AA	AB	DD	DD
Points	Ø	**89**	**87**	**86**	**89**	**78**	**77**	**83**	**83**	**79**	**74**	**93**	**80**	**84**	**79**	**72**	**65**

Additional Free Malware Removal Services/Utilities offered by the vendors

	Boot-Disk[3] available	Free Removal-Tools
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=SOLN2372
F-Secure	**YES**	https://www.f-secure.com/en/web/labs_global/tools-beta
Fortinet	**-**	http://www.fortiguard.com/antivirus/malware_removal.html
Kaspersky Lab	**YES**	http://support.kaspersky.com/viruses/utility#kasperskyvirusremovaltool
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 products[4] in this specific test:

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

[4] Microsoft Windows Defender was tested out-of-competition and is therefore not included in the awards page. The score of Microsoft Windows Defender would be equivalent to ADVANCED.

Copyright and Disclaimer

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

AV-Comparatives (September 2015)