Anti-Virus Comparative

Malware Removal Test

Language: English

February - October 2018
Last Revision: 1st November 2018

www.av-comparatives.org

Table of Contents

Tested Products

The following products were tested from February to October 2018 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**
- **AVIRA Antivirus Pro**
- **Bitdefender Internet Security**
- **BullGuard Internet Security**
- **Emsisoft Anti-Malware**
- **ESET Internet Security**
- **F-Secure SAFE**
- **Kaspersky Internet Security**
- **Tencent PC Manager**
- **VIPRE Advanced Security**

This Malware Removal Test was optional, i.e. before the test was run, individual vendors could state that they did not want to participate in it. 8 out of 18 vendors opted out of this test.

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 usually 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 Most often users come with infected PC's with no (or outdated) AV-software to computer repair stores.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 February to October 2018 on an up-to-date Microsoft Windows 10 64-Bit (English) system.

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 (or malware family) must have been still prevalent (according to our metadata)
- 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 40 malware samples from the pool of samples matching the above criteria.

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 vendors to identify them based on the samples they received from us after this test[1].

Sample 1 (479f79a9): CosDuke backdoor
Sample 2 (b5e46dd7): Lydra trojan
Sample 3 (084529f5): Autoit worm
Sample 4 (b1e332cf): Lmir trojan
Sample 5 (eb09fa29): Sohanad worm
Sample 6 (eea4e023): Ibashade worm
Sample 7 (dcf3ff58): Hamweq worm
Sample 8 (2516b078): Pepe trojan
Sample 9 (c137b153): Ekidoa trojan
Sample 10 (f474237c): FrauDrop trojan
Sample 11 (0519edd5): Tepfer trojan
Sample 12 (d5f7ad0b): NanoBot backdoor
Sample 13 (c363ac0c): Abaddon trojan
Sample 14 (e70a92b6): Pyramid trojan
Sample 15 (3da61617): Dukrit trojan
Sample 16 (d636cc4a): Blocker ransomware
Sample 17 (1ecd556a): IRCBot trojan
Sample 18 (ae5998c8): Lamooc trojan
Sample 19 (1015aa2a): Mestepy trojan
Sample 20 (17c424cc): Buzus trojan
Sample 21 (770964fd): Khalesi trojan
Sample 22 (e66c5dd3): Rebhip trojan
Sample 23 (23bddba7): Hpomaneat trojan
Sample 24 (37b8a3c8): Kora trojan
Sample 25 (2091fe8a): Palevo worm
Sample 26 (9da151ad): DarkComet backdoor
Sample 27 (394903ee): EmotetEG trojan
Sample 28 (3d092975): Gotango trojan
Sample 29 (08b5a042): Farfli backdoor
Sample 30 (9b2666e3): Fuerboos trojan
Sample 31 (17dfadb6): Tpyn trojan
Sample 32 (47b3f5b8): Injector trojan
Sample 33 (799d851e): Scarsi trojan
Sample 34 (6675e3db): Agent trojan
Sample 35 (57210fa9): Boloid backdoor
Sample 36 (4d8edd91): Tinukebot trojan
Sample 37 (41e87e94): Zurgop trojan
Sample 38 (018dcbf6): Delf trojan
Sample 39 (336f3595): Limitail backdoor
Sample 40 (673a8f83): EmotetGA 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] 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 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	Avira	Bitdefender	BullGuard	Emsisoft	ESET	F-Secure	Kaspersky Lab	Tencent	VIPRE
Sample	1	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
	2	AA	AA	AA	BA	AA	BA	AA	AA	AA	AA
	3	BA	AA	AA	AA	AA	AA	BA	AA	AA	CA
	4	BA	AA	AA	AA	AB	AA	AA	AA	AA	BA
	5	BA	BA	AA	AA	AA	AA	BA	AA	AA	CA
	6	AA	AA	AA	AA	AA	AA	AA	AA	AA	BA
	7	AA	AA	AA	AA	BA	AA	BA	AA	AA	BA
	8	AA	AA	AA	AA	AA	BA	BA	AA	AA	AA
	9	AA	AA	AA	AA	AA	AA	BA	AA	AA	AA
	10	BA	AA	AA	AA	AA	AA	AA	AA	AA	AA
	11	AA	AA	AA	AA	AA	AA	BA	AA	AA	BA
	12	AA	AA	AA	BA	BA	AA	BA	AA	AA	AA
	13	AA	AA	AA	BA	AA	AA	AA	AA	AA	BA
	14	AA	AA	AA	AA	AA	AA	BA	AA	AA	BA
	15	AA	AA	AA	BA	AA	AA	BA	AA	AA	AA
	16	BA	CA	BA	BA	BA	AA	BA	AA	BA	BA
	17	AA	AA	AA	AA	AA	BA	AA	BA	AA	AA
	18	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA
	19	AA	BA	AA	BA	BA	AA	DD	AA	AA	AA
	20	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA
	21	AA	AA	AA	AA	AA	BA	AA	AA	AA	DD
	22	AA	AA	AA	BA	AA	BA	AA	AA	AA	BA
	23	AA	AA	AA	AA	AA	AA	AA	AA	AA	AA
	24	AA	AA	AA	BA	AA	AA	AA	AA	BA	AA
	25	AA	AA	AA	CA	CA	CA	AA	AA	AA	AA
	26	AA	AA	AA	AA	AA	AA	AA	AA	AA	BA
	27	AA	AA	DD	DD	DD	AA	DD	AA	DD	DD
	28	AA	AA	AA	BA	BA	AA	DD	AA	AA	AA
	29	AA	AA	AA	AA	AA	AA	DD	AA	AA	AA
	30	BA	AA	AA	BA	BA	BA	BA	AA	AA	BA
	31	BA	AA	AA	BA	BA	AA	AA	AA	AA	AA
	32	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA
	33	AA	AA	AA	BA	DD	AA	AA	AA	BA	BA
	34	AA	AA	AA	BA	BA	BA	BA	AA	AA	BA
	35	AA	AA	AA	BA	AA	AA	BA	AA	AA	AA
	36	BA	BA	AA	BA	BA	BA	BA	AA	BA	BA
	37	AA	CA	AA	CA	CA	CA	CA	AA	CA	CA
	38	AA	BA	AA	BA	BA	BA	BA	BA	BA	BA
	39	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA
	40	AA	AA	DD	AA	DD	AA	DD	AA	AA	DD
Points	**Ø**	**94**	**94**	**94**	**80**	**82**	**90**	**75**	**99**	**92**	**78**

Additional Free Malware Removal Services/Utilities offered by the vendors

	Boot-Disk[2] available	Free Removal-Tools
Avast	**YES**	-
AVIRA	**YES**	https://www.avira.com/en/downloads#tools
Bitdefender	**YES**	-
BullGuard	**-**	-
Emsisoft	**-**	https://www.emsisoft.com/en/software/eek/
ESET	**YES**	https://www.eset.com/int/download-utilities/
F-Secure	**-**	-
Kaspersky Lab	**YES**	https://support.kaspersky.com/viruses/utility#kasperskyvirusremovaltool
Tencent	**YES**	-
VIPRE	**-**	https://www.vipre.com/support/rescue/

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.)
- check for active malware before attempting installation
- 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

[2] 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 in this specific test[3]:

AWARDS	PRODUCTS
	Kaspersky Lab Bitdefender Avast AVIRA Tencent ESET
	Emsisoft BullGuard VIPRE F-Secure
	-

[3] There was a very high standard in the Malware Removal Test this year, with all tested products reaching a good level.

Copyright and Disclaimer

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

AV-Comparatives (November 2018)