

## Anti-Virus Comparative



## Malware Removal Test

Language: English

February - September 2017

Last Revision: 25<sup>th</sup> October 2017

[www.av-comparatives.org](http://www.av-comparatives.org)

# Table of Contents



Tested Products	3
Introduction	4
Test Procedure	4
Malware selection	4
Used samples	5
Ratings	6
Award system	6
Results	7
Additional Free Malware Removal Services/Utilities	8
Award levels reached in this test	9
Copyright and Disclaimer	10

## Tested Products

The following products were tested from February to September 2017 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).

- Adaware Pro Security
- Avast Free Antivirus
- AVG Free Antivirus
- AVIRA Antivirus Pro
- Bitdefender Internet Security
- BullGuard Internet Security
- Emsisoft Anti-Malware
- eScan Corporate 360
- ESET Internet Security
- F-Secure SAFE
- Fortinet FortiClient with FortiGate
- Kaspersky Internet Security
- Microsoft Windows Defender
- Seqrite Endpoint Security
- Tencent PC Manager
- Trend Micro Internet Security
- VIPRE Advanced 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 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 Most often users come with infected PC's with no (or outdated) AV-software to computer repair stores.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 September 2017 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<sup>1</sup>.

Sample 1 (0ccea30): OnionDuke trojan	Sample 21 (e138e724): Noxjasm worm
Sample 2 (2ad570f0): Yakes trojan	Sample 22 (af2f0148): Pazetus worm
Sample 3 (22d039bd): Boostro trojan	Sample 23 (1a99aee6): Esfury worm
Sample 4 (038924ce): Cult worm	Sample 24 (02888f73): Llac trojan
Sample 5 (0e55d72f): Poison backdoor	Sample 25 (e76cbe1d): Autorun worm
Sample 6 (0abf2e90): ClickTrans trojan	Sample 26 (f9fd23a6): Dothetuk trojan
Sample 7 (dc9458ea): Nanocore trojan	Sample 27 (30008b40): WBMA worm
Sample 8 (7fe7f60e): Brontok worm	Sample 28 (27689bcb): Fareit trojan
Sample 9 (82230668): Mothyfil worm	Sample 29 (c6027c14): Blocker ransomware
Sample 10 (f8fa0da3): Dogkild worm	Sample 30 (c77802d9): Mywife worm
Sample 11 (558f1861): Viking virus	Sample 31 (04abf409): VB worm
Sample 12 (03d04d50): Mofksys worm	Sample 32 (ab4fb5df): Expiro virus
Sample 13 (e93795ce): Shiz backdoor	Sample 33 (5032cc87): Sohanad worm
Sample 14 (20e71e7e): Nuqel worm	Sample 34 (08101e1e): Crypmod ransomware
Sample 15 (f5075326): Pronny worm	Sample 35 (a81e112c): Malas worm
Sample 16 (ff5e5f14): Slugin virus	Sample 36 (1016035b): Bladabindi backdoor
Sample 17 (08059cff): Klez worm	Sample 37 (bdb7e8dd): Killproc trojan
Sample 18 (c238d0c4): Vexral worm	Sample 38 (ad150626): Qvervar worm
Sample 19 (26a9f1e5): Sven worm	Sample 39 (443403e5): Vilsel trojan
Sample 20 (f7520204): Methoaf worm	Sample 40 (0971e61e): Delf 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.

---

<sup>1</sup> 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:

		Adaware	Avast	AVG	Avira	Bitdefender	BullGuard	Emsisoft	eScan	ESET	F-Secure	Fortinet	Kaspersky Lab	Microsoft	Segrite	Tencent	Trend Micro	VIPRE
Sample	1	CA	AA	AA	AA	AA	CA	CA	AA	AA	CA	DD	AA	AA	CA	AA	AA	AA
	2	AA	AA	AA	CA	AA	CA	BA	CA	BA	BA	BA	AA	AA	BA	AA	DD	AA
	3	AA	AA	AA	CA	AA	CA	CA	CA	AA	CA	CA	AA	AA	CA	AA	CA	AA
	4	AA	AA	AA	BA	AA	AA	AA	AA	BA	BA	AA	AA	AA	AA	AA	AA	AA
	5	BA	BA	BA	DD	BA	BA	BA	BA	DD	CA	AA	BA	AA	BA	BA	BA	BA
	6	AA	AA	AA	AA	AA	BA	AA	BA	BA	AA	AA	AA	AA	AA	AA	AA	AA
	7	CA	AA	AA	CA	CA	CA	BA	CA	CA	CA	CA	AA	CA	DD	CA	CA	CA
	8	BA	AA	AA	AA	AA	CA	AA	AB	AA	AA	CA	AA	CA	AA	AA	AA	CA
	9	CA	CA	CA	CA	AA	CA	CA	CA	CA	CA	CA	BA	BA	CA	AA	BA	CA
	10	DD	CA	CA	CA	AA	AA	AA	AA	CA	AA	CA	AA	CA	CA	AA	AA	CA
	11	CA	AA	AA	AA	AA	AA	AA	BA	AA	CA	AA	CA	AA	CA	BA	BA	AA
	12	AA	BA	BA	AA	AA	BA	AA	AA	AA	BA	AA	AA	AA	BA	AA	AA	AA
	13	AA	BA	BA	AA	AA	CA	AA	AA	AA	CA	AA	AA	CA	CA	AA	AA	BA
	14	AA	BA	BA	AA	AA	AA	AA	AA	AA	BA	CA	AA	BA	BA	AA	AA	AA
	15	AA	AA	AA	AA	AA	CA	AA	AA	AA	CA	CA	AA	CA	CA	AA	AA	AA
	16	BA	BA	BA	AA	AA	AA	BA	AA	BA	BA	CA	AA	AA	BA	AA	AA	AA
	17	AA	AA	AA	AA	AA	AA	AA	AA	BA	AA	AA	AA	BA	BA	AA	AA	AA
	18	BA	AA	AA	AA	AA	BA	BA	BA	AA	BA	BA	AA	BA	BA	BA	BA	AA
	19	AA	AA	AA	CA	AA	CA	BA	AA	AA	AA	CA	AA	AA	BA	AA	AA	CA
	20	AA	BA	BA	AA	AA	AA	BA	AA	AA	BA	BA	AA	AA	BA	AA	BA	BA
	21	AA	BA	BA	AA	AA	AA	BA	AA	BA	BA	CA	AA	AA	BA	AA	AA	AA
	22	AA	BA	BA	AA	AA	AA	BA	AA	AA	BA	CA	AA	CA	BA	AA	AA	AA
	23	CC	BA	BA	DD	DD	AA	BA	AA	AA	AA	CA	DD	CA	DD	AA	AA	AA
	24	AA	AA	AA	BA	AA	BA	AA	AA	AA	AA	AA	AA	BA	BA	AA	AA	BA
	25	AA	AA	AA	AA	AA	BA	AA	AA	AA	AA	BA	AA	AA	BA	AA	AA	AA
	26	AA	AA	AA	AA	AA	BA	AA	AA	AA	AA	DD	DD	AA	DD	AA	AA	AA
	27	AA	AA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	AA	BA	AA	AA	AA
	28	AA	AA	AA	AA	AA	BA	BA	AA	BA	AA	AA	AA	BA	AA	AA	BA	AA
	29	AA	AA	AA	AA	AA	BA	AA	AA	AA	AA	AA	AA	DD	BA	AA	AA	AA
	30	AA	BA	BA	AA	AA	AA	AA	AA	AA	BA	AA	AA	AA	BA	AA	AA	AA
	31	CB	AA	AA	CA	CA	CA	CA	AA	AA	CA	AA	AA	AA	CA	AA	BA	AA
	32	AA	AA	AA	AA	AA	AA	DD	AA	AB	AB	AA	AA	AA	AA	AA	AA	AA
	33	AA	BA	BA	AA	AA	AA	BA	AA	AA	BA	CA	AA	CA	BA	BA	AA	AA
	34	BA	BA	BA	BA	BA	BA	BA	BA	BA	BA	BA	AA	BA	BA	AA	AA	BA
	35	AA	BA	BA	BA	AA	BA	BA	AA	BA	BA	AA	AA	BA	BA	AA	BA	BA
	36	AA	AA	AA	AA	AA	AA	AA	AA	AA	BA	AA	AA	DD	BA	AA	AA	AA
	37	AA	BA	BA	AA	AA	BA	BA	BA	BA	AA	BA	AA	DD	BA	AA	AA	AA
	38	AA	AA	AA	CA	AA	CA	CA	CA	AA	CA	CA	AA	CA	CA	AA	CA	AA
	39	AA	BA	BA	BA	AA	AA	BA	AA	AA	BA	CA	AA	CA	BA	AA	DD	AA
	40	AA	AA	AA	AA	AA	CA	AA	AA	CA	CA	CA	AA	CA	CA	AA	AA	CA
Points	∅	84	85	85	79	93	72	78	88	83	72	67	92	70	61	96	85	87

## Additional Free Malware Removal Services/Utilities offered by the vendors

	Boot-Disk <sup>2</sup> available	Free Removal-Tools
Adaware	YES	-
Avast	YES	<a href="http://www.avast.com/ransomware-decryption-tools">http://www.avast.com/ransomware-decryption-tools</a>
AVG	YES	<a href="http://www.avg.com/eu-en/virus-removal">http://www.avg.com/eu-en/virus-removal</a>
AVIRA	YES	<a href="http://www.avira.com/en/downloads#tools">http://www.avira.com/en/downloads#tools</a>
Bitdefender	YES	<a href="http://www.bitdefender.com/free-virus-removal/">http://www.bitdefender.com/free-virus-removal/</a>
BullGuard	-	-
Emsisoft	-	<a href="http://www.emsisoft.com/en/software/eeek/">http://www.emsisoft.com/en/software/eeek/</a>
eScan	YES	<a href="http://escanav.com/english/content/products/MWAV/escan_mwav.asp">http://escanav.com/english/content/products/MWAV/escan_mwav.asp</a>
ESET	YES	<a href="https://www.eset.com/int/download-utilities/">https://www.eset.com/int/download-utilities/</a>
F-Secure	YES	<a href="https://www.f-secure.com/en/web/labs_global/tools-beta">https://www.f-secure.com/en/web/labs_global/tools-beta</a>
Fortinet	-	-
Kaspersky Lab	YES	<a href="https://support.kaspersky.com/viruses/utility#kasperskyvirusremovaltool">https://support.kaspersky.com/viruses/utility#kasperskyvirusremovaltool</a>
Microsoft	YES	<a href="https://www.microsoft.com/en-us/wdsi/products/scanner">https://www.microsoft.com/en-us/wdsi/products/scanner</a>
Seqrite	-	-
Tencent	YES	-
Trend Micro	YES	-
VIPRE	-	<a href="https://www.vipre.com/support/rescue/">https://www.vipre.com/support/rescue/</a>

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

---

<sup>2</sup> 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:

AWARDS	PRODUCTS
 <p>AV comparatives 2017 ADVANCED+ MALWARE REMOVAL ★★★</p>	<p>Tencent Bitdefender Kaspersky Lab eScan VIPRE</p>
 <p>AV comparatives 2017 ADVANCED MALWARE REMOVAL ★★</p>	<p>Avast AVG Trend Micro Adaware ESET AVIRA Emsisoft BullGuard F-Secure</p>
 <p>AV comparatives 2017 STANDARD MALWARE REMOVAL ★</p>	<p>Microsoft Fortinet Seqrite</p>

## Copyright and Disclaimer

This publication is Copyright © 2017 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 (October 2017)