Anti-Virus Comparative

Malware Removal Test

Language: English
Autumn 2011
Last Revision: 13th December 2011

www.av-comparatives.org

Table of Contents

Tested Products

- avast! Free Antivirus 6.0
- AVG Anti-Virus 2012
- AVIRA Free Antivirus 2012
- BitDefender Anti-Virus Plus 2012
- ESET NOD32 Antivirus 5.0
- F-Secure Anti-Virus 2012
- G DATA AntiVirus 2012
- K7 TotalSecurity 11.1
- Kaspersky Anti-Virus 2012
- McAfee AntiVirus Plus 2012
- Microsoft Security Essentials 2.1
- Panda Cloud Antivirus Free 1.5.1
- PC Tools Spyware Doctor with AV 2012
- Qihoo 360 Antivirus 2.0
- Sophos Anti-Virus 9.7
- Symantec Norton Anti-Virus 2012
- Trend Micro Titanium Antivirus+ 2012
- Webroot SecureAnywhere Antivirus 2012

Introduction

This test focuses only on the malware removal/cleaning capabilities, therefore all selected/used samples 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 was if the products are able to successfully remove malware from an already infected/compromised system. The test report is aimed to normal/typical home users and not Administrators or advanced users that 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Most often users come with infected PC's with no (or outdated AV-software) to computer repair stores.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 used methodology considers this situation: an already infected system that needs to be cleaned.

The test was performed in autumn 2011 under Microsoft Windows XP Professional SP3.

Test-Procedure

- Thorough malware analysis to know what to look for
- Administrator account was used with turned off system restore
- Infect native machine with one threat, reboot and make sure that threat is fully running
- Reboot Windows, 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 like a typical home user would do
- Manual inspection/analysis of the PC for malware removal and leftovers

Malware selection

The samples have been selected by following criteria:

- All Anti-Virus products must be able to detect the used malware dropper on-demand/on-access already at least since over half a year
- The sample must have been prevalent (according to metadata on exact hashes) in the order of at least thousands (and at least hundreds of thousands for their malware family / behavior they represent) of instances AND seen in the field on at least two PC’s of our local customers in 2011.
- 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 of replacing windows system files etc.) and show common malware behaviors (in order to represent also behaviors observed by many other malware samples). Due to that, the selected malware is representative of a very large amount of other samples which show similar behavior and system changes.
- We randomly took 10 malware samples from the pool of samples matching the above criteria

To avoid providing information to malware authors who could be potentially useful for them to improve their creations, this public report contains only general information about the malware/leftovers, without any technical instructions/details.

Used samples

Below is a list of the used samples. Please do not wonder about 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.

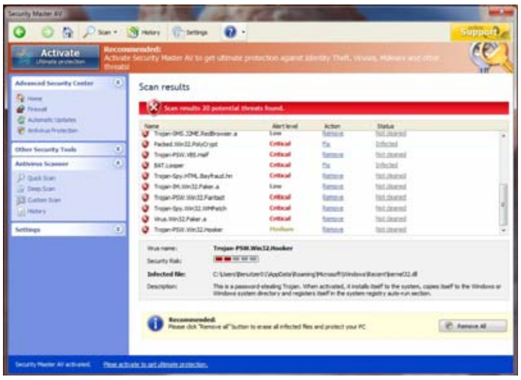
Sample 1 (BU/bd3752): This sample is a widespread trojan horse.

Sample 2 (RJ/1dbe9a): This sample is an extremely widespread worm.

Sample 3 (OF/998190): This sample is a very wide-spread trojan horse.

Sample 4 (DR/18d7cc): This sample is a widespread worm.

Sample 5 (FA/33299a): This sample is a widespread Fake Antivirus.



Recommended:
Activate Security Master AV to get ultimate protection against Identity Theft, Viruses, Malware and other threats!

Scan results

Scan results 20 potential threats found.

Name	Alert level	Action	Status
Trojan-SMS.J2ME.RedBrowser.a	Low	Remove	Not cleaned
Packed.Win32.PolyCrypt	Critical	Fix	Infected
Trojan-PSW.VBS.Half	Critical	Remove	Not cleaned
BAT.Looper	Critical	Fix	Infected
Trojan-Spy.HTML.Bayfraud.hn	Critical	Remove	Not cleaned
Trojan-IM.Win32.Faker.a	Low	Remove	Not cleaned
Trojan-PSW.Win32.Fantast	Critical	Remove	Not cleaned
Trojan-Spy.Win32.WMPatch	Critical	Remove	Not cleaned
Virus.Win32.Faker.a	Critical	Remove	Not cleaned
Trojan-PSW.Win32.Hooker	Medium	Remove	Not cleaned

Virus name: Trojan-PSW.Win32.Hooker
Security Risk:
Infected file: C:\Users\Benutzer01\AppData\Roaming\Microsoft\Windows\Recent\kernel32.dll
Description: This is a password-stealing Trojan. When activated, it installs itself to the system, copies itself to the Windows or Windows system directory and registers itself in the system registry auto-run section.

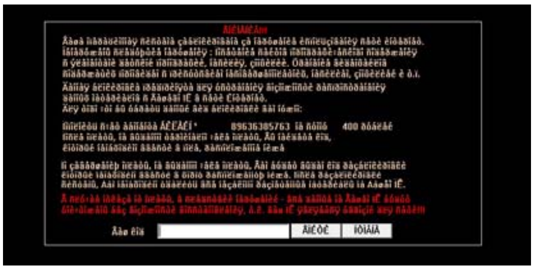
Recommended:
Please click "Remove all" button to erase all infected files and protect your PC

Security Master AV activated. Please activate to get ultimate protection.

Sample 6 (BR/c81db0): This sample is an extremely widespread worm.

Sample 7 (SO/70a001): This sample is a widespread worm.

Sample 8 (PO/aef331): This sample is a typical widespread ransom Trojan which takes the system as hostage. This common malware shows the importance of rescue disks for home users. Rescue disks which only delete the file but do not fix the registry will not solve the problem, as in that case Windows Explorer will not load.



Sample 9 (YA/1f4086): This sample is a widespread worm.

Sample 10 (IM/64f6b6): This sample is an extremely widespread worm.

Ratings

This year we were more “tolerant” when evaluating the leftovers and allowed certain negligible/unimportant traces to be left behind. Furthermore, we combined the “removal of malware” and “removal of leftovers” into one dimension and took this year into consideration also the “convenience”. It should now be easier for readers to get an overview.

The ratings are given as follows:

a) Removal of malware

- Malware removed, only negligible traces left (A)
- Malware removed, but some executable files 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, etc.) remaining (C)
- Only the malware dropper has been deleted and all other dropped malicious files/changes were not removed or system is no longer usable / Removal failed (D)

b) Convenience:

- Removal could be done easily in normal mode (A)
- Removal requires booting in safe-mode or other build-in utilities and manual actions (B)
- Removal requires Rescue Disk (C)
- Removal or install requires contacting support or similar / Removal failed (D)

Award system

We have been thinking how to make one for users easy to understand point system and came to the following solution:

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 reached mean value:

85-100: Advanced+
70-85: Advanced
50-70: Standard
Lower than 50: 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	∅
Avast	BA	AA	AA	BB	DD	CA	CA	DD	BA	CA	52
AVG	AA	AA	BA	BC	DD	CA	CA	DD	AA	BA	57
AVIRA	AA	BA	AA	BC	AC	AA	AA	DD	AA	AA	80
Bitdefender	AA	AA	AA	AA	AA	AA	AA	DD	AA	AA	90
ESET	AA	AA	BA	BC	CA	CA	CA	DD	BA	BA	58
F-Secure	AA	AA	AA	DD	DD	AA	AA	DD	AA	BA	67
G DATA	BA	BA	BA	BC	CA	CA	CA	DD	AA	BA	55
K7	AA	AA	AA	DD	CA	CA	AA	DD	AA	BA	65
Kaspersky	AA	AA	AA	AA	CA	AA	AA	CC	AA	AA	86
McAfee	AA	AA	BA	DD	DD	BA	AA	DD	AA	BA	61
Microsoft	AA	AA	AA	AC	CC	CA	CA	CC	AA	AA	70
Panda	AA	AA	BA	BC	DD	AA	CA	DD	AA	BA	63
PC Tools	AA	AA	AA	AC	AA	AA	AA	DD	AA	AA	88
Qihoo	AA	AA	AA	BA	BA	CA	CA	DD	AA	BA	69
Sophos	AA	CA	BA	DD	CA	AA	AA	DD	AA	AA	65
Symantec	AA	AA	AA	AA	CA	AA	AA	CC	AA	AA	86
Trend Micro	BA	AA	AA	BA	CA	AA	CA	DD	AA	AA	72
Webroot	AA	CA	AA	CA	AA	AA	AA	DD	AA	AA	78

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.

Some users may wrongly assume that Anti-Virus products just delete binary files (probably because most Anti-Virus products usually list only infected files in their logs) and do not fix anything else, like e.g. the registry etc. 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 do regular backups of their important data and to use e.g. image restoring software.

Most AV vendors should by now already have addressed and fixed/improved the next releases of their products based on our findings in this report.

Additional Free Malware Removal Services/Utilities offered by the vendors

	Boot-Disk[1] available	Free Removal-Tools for specific malware
Avast	**-**	-
AVG	**YES**	http://www.avg.com/virus-removal
AVIRA	**YES**	http://www.avira.com/en/support-download-avira-antivir-removal-tool
Bitdefender	**YES**	http://www.bitdefender.com/site/Downloads/browseFreeRemovalTool
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/easy-clean
G DATA	**YES**	http://www.gdata.de/support/downloads/tools.html
K7	**-**	http://www.k7computing.com/en/Free-Tools/Free-Tools.php
Kaspersky	**YES**	http://support.kaspersky.com/viruses
McAfee	**-**	http://www.mcafee.com/us/downloads/free-tools/how-to-use-stinger.aspx
Microsoft	**YES**	-
Panda	**YES**	http://www.pandasecurity.com/usa/homeusers/downloads/repair-utilities/
PC Tools	**YES**	-
Qihoo	**-**	-
Sophos	**-**	http://www.sophos.com/support/disinfection/
Symantec	**YES**	http://us.norton.com/security_response/removaltools.jsp
Trend Micro	**YES**	http://www.trendmicro.com/products/personal/free-tools-and-services/
Webroot	**-**	-

The customer support of AV vendors may help the users in the malware removal process. In most cases such support services are nowadays charged separately, but some may provide in some circumstances the malware removal help for free. We suggest to users with a valid license to try contacting in any case the AV vendor support 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 point to links where to download it)
- provide up-to-date offline-installers (e.g. if malware blocks access to the vendors website)
- not require to login to 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 provided free malware removal utilities and free malware removal procedures/support on the website, manuals, inside the product or when an active infection is found

[1] Included in the standard package without extra charging (and without the need to contact/request it from the vendor support personnel).

Awards reached in this test

The following awards / certification levels have been reached by the various products in this specific test:

AWARDS	PRODUCTS
AV comparatives ADVANCED+ ★★★ MALWARE REMOVAL NOV 2011	Bitdefender PC Tools Kaspersky Symantec
AV comparatives ADVANCED ★★ MALWARE REMOVAL NOV 2011	AVIRA Webroot Trend Micro Microsoft
AV comparatives STANDARD ★ MALWARE REMOVAL NOV 2011	Qihoo F-Secure K7 Sophos[2] Panda McAfee ESET AVG G DATA Avast

[2] Sophos is a corporate product. Due to that, it may not restore e.g. some registry entries by design, as in a managed environment, some of these settings may be enforced centrally by system administrators. In case of home user products, such settings should be fixed as part of the malware removal process (or at least the possibility to fix them should be given in the products).

Copyright and Disclaimer

AV-Comparatives e.V. 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 e.V. 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. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

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

AV-Comparatives e.V. (December 2011)