

Remediation Testing Report

A test commissioned by Symantec Corporation and performed by AV-Test GmbH

Date of the report: August 18th, 2010, last update: August 24rd, 2010

Executive Summary

In August 2010, AV-Test performed a comparative review of 13 security products to determine their remediation capabilities. In addition to the core product, removal tools such as Symantec Norton Power Eraser or McAfee Stinger, as well as bootable rescue media (which are being offered by some of the vendors) were added to the test.

The malware test corpus consisted of 15 Fake Antivirus samples and 15 other assorted threats. The false positive corpus consisted of 15 known clean applications. To perform the single test runs, a clean Windows XP image was used on several identical PCs. This image was then infected with one of the malware samples. The next step was trying to install the security product, scanning the PC and removing any threats that have been found. If one of these steps could not be carried out successfully, additional removal tools or rescue media were used, if available, from the respective vendor. The false positive testing was performed in the same way. However, the desired result was to not detect any of the 15 clean applications.

The best result in the described test was achieved by the Symantec product. It reached both, the highest overall score as well as the highest individual scores for the two distinct malware sets. Furthermore, no false positives occurred for this product.

Overview

With the increasing number of threats that is being released and spreading through the Internet these days, the danger of getting infected is increasing as well. A few years back there were new viruses released every few days. This has grown to several thousand new threats per hour.

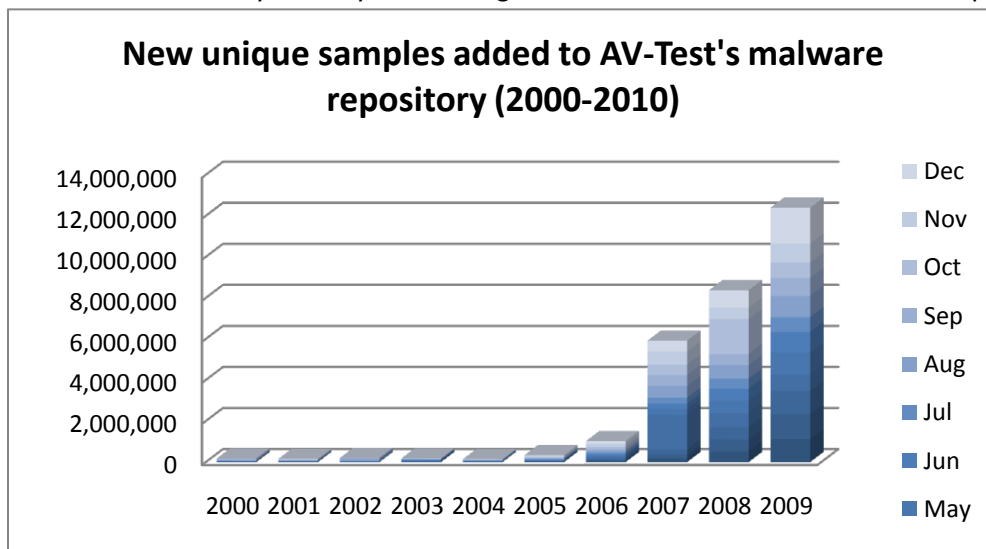


Figure 1: New samples added per year

In the year 2000, AV-Test received more than 170,000 new samples, and in 2009, the number of new samples grew to over 12,000,000 new samples. The numbers continue to grow in the year 2010. The growth of these numbers is displayed in Figure 1.

The volume of new samples that have to be processed by anti-malware vendors in order to protect their customers can create problems. It is not always possible to successfully protect a PC in time. It is possible that a PC can get infected, even if up-to-date anti-malware software is installed because signatures are provided only every few hours, which sometimes may be too late. Infections create financial loss, either because sensitive data is stolen or because the PC cannot be used for productive work anymore until the malware has completely removed from the system.

Therefore remediation techniques become more important to get an infected PC up and running again. In that process it is imperative that the cleaning process is reliable in two ways:

1. The malware and all of its components have to be removed and any malicious system changes have to be reverted
2. No clean applications or the system itself must be harmed by the cleaning process

Fulfilling these two requirements is not easy. In order to be able to handle the high volume of different malware samples and different behavior it would be necessary to apply more generic cleaning techniques, because there is simply no time to deploy a dedicated cleaning routine for every single malware sample. As soon as generic techniques are used, the risk of false positives (and therefore the risk of harming the system and clean software) increases. On the other hand, malware uses a lot of techniques to avoid successful detection (e.g. rootkit techniques are used to hide files, registry entries and processes) or removal (e.g. the anti-malware software is blocked from starting up). In order to cope with these problems, some vendors provide specific removal tools and rescue media, that don't face the problems of the regular anti-malware software.

All these aspects have been considered in this test and the corresponding details will be presented on the next few pages.

Products Tested

The latest versions (at the time of the test) of the following 13 products were tested:

- Avast! Free AntiVirus 5.0
- AVG Anti-Virus Free Edition 9.0
- Avira Antivir Personal Version – Free Antivirus 10.0
- BitDefender Internet Security 2010
- ESET Smart Security 4
- GDATA Internet Security 2011
- K7 Total Security 10.0
- Kaspersky Internet Security 2011
- McAfee Internet Security 2010
- Microsoft Security Essentials 1.0
- Norton Internet Security 2011
- Panda Internet Security 2011
- TrendMicro Internet Security 2010 Pro

Methodology and Scoring

Platform

All tests have been performed on identical PCs equipped with the following hardware:

- Intel Xeon Quad-Core X3360 CPU
- 4 GB Ram
- 500 GB HDD (Western Digital)
- Intel Pro/1000 PL (Gigabit Ethernet) NIC

The operating system was Windows XP Service Pack 2 with only those hotfixes that were part of SP2.

Testing methodology

The test has been performed according to the methodology explained below.

1. **Clean system for each sample.** The test systems should be restored to a clean state before being exposed to each malware sample.
2. **Physical Machines.** The test systems used should be actual physical machines. No Virtual Machines should be used.
3. **Internet Access.** The machines had access to the Internet at all times, in order to use in-the-cloud queries if necessary.
4. **Product Configuration.** All products and their accompanying remediation tools or bootable recovery tools were run with their default, out-of-the-box configuration.
5. **Infect test machine.** Infect native machine with one threat, reboot and make sure that threat is fully running.
6. **Sample Families and Payloads.** No two samples should be from the same family or have the same payloads.
7. **Remediate using all available product capabilities.**
 - a. Try to install security product in default settings. Follow complete product instructions for removal.
 - b. If a. doesn't work, try *standalone fixtool/rescue tool* solution (if available).
 - c. If b. doesn't work, boot standalone *boot solution* (if available) and use it to remediate.
8. **Validate removal.** Manually inspect PC to validate proper removal and artifact presence.
9. **Score removal performance.** Score the effectiveness of the tool and the security solution as a whole using the agreed upon scoring system.
10. **Overly Aggressive Remediation.** The test should also measure how aggressive a product is at remediating. For example some products will completely remove the hosts file or remove an entire directory when it is not necessary to do so for successful remediation. This type of behavior should count against the product.
11. **False Positive Testing.** The test should also run clean programs and applications to make sure that products do not mistakenly remove such legitimate software.

In addition to the above, the following items had to be considered:

Fixtools: No threat-specific fixtools should be used for any product's remediation. Only generic remediation standalone/fixtools and bootable tools should be used.

Licensed vs. Unlicensed Bootable or Remediation tool: Only licensed bootable or other generic remediation tools offered by vendors as part of their security product or pointed to by their infection UI workflow should be included in the test. No unlicensed tools should be used in the test

Microsoft's Malicious Malware Removal Tool: This is part of the windows update and as such a part of the Windows OS. This tool should not be used as a second layer of protection for any participating vendor's products.

Efficacy Rating

For each sample tested, apply points according to the following schedule:

- a. Malware completely removed (5)
- b. Malware removed, some unimportant traces left (4)
- c. Malware removed, but annoying or potentially dangerous problems remaining (2)
- d. Malware not removed (0)
- e. Product is overly aggressive (e.g. takes out the entire hosts file, entire directory containing threat file etc.) (-2)
- f. Product's remediation renders the machine unbootable or unusable (-5)

The scoring should not take into consideration which of the available techniques were needed to remove the malware. All techniques should however, be applied. When a product cleans out the entries in the hosts file that relate to that very product and leave the machine uninfected and the product functional and updateable, it should be given full credit for remediation even if entries for other security vendors remain in the hosts file.

Samples

Two distinct sets of malware were used for the testing. The first set contained 15 Fake Antivirus programs and the second set contained 15 other assorted threats. In addition to this, 15 known clean programs were used for the false positive testing. The details of the samples used can be found in the appendix.

Test Results

Symantec Norton Internet Security achieved the best score for both test sets, Fake AV and other malware, and as such also the best overall score, as can be seen in Figure 2. It should be kept in mind that the numbers shown here are the result of the combined effort of the core product and additional removal tools and rescue media, if available.

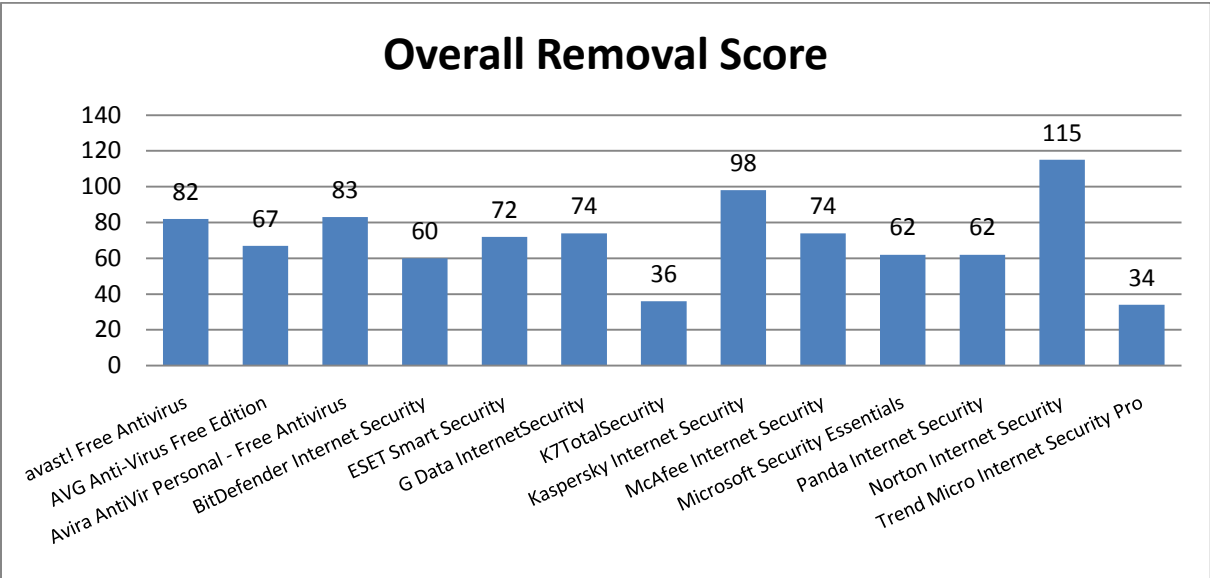


Figure 2: Overall Removal Score

The maximum score that could be reached was 150. The best score was 115, achieved by Norton Internet Security. The worst score was 34. The average score was 68 and the median score 72. This means that seven products were better than the average and six products were worse than the average. The second best product is already considerably behind with 98 points and the third product reached 83 points, the fourth 82 points. All other products were below 75 points.

When looking at the individual scores similar observations can be made. In the case of the removal of other malware, as shown in Figure 3, Norton again gained the highest score of all products with 51.

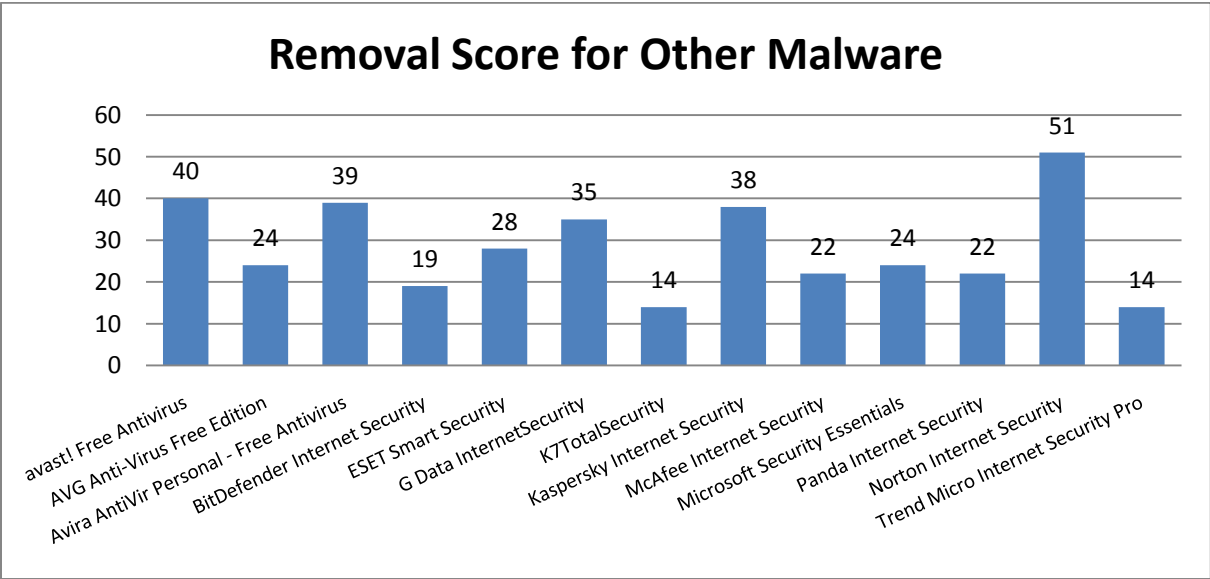


Figure 3: Removal score for other malware

Out of a maximum achievable score of 75, the worst result was 14, while the average was at 27 and the median at 24. Six products scored better than the average and seven were worse. Avast achieved the second place with 40 points and Avira the third place with 39. Kaspersky scored 38 points and G Data was only 3 points behind, with a score of 35. All other products were below 20 points.

The scores for the removal of Fake AV are a bit different. Out of the maximum achievable score of 75 in the Fake AV category, once again Norton achieved first place with 64 points, but this time they were closely followed by Kaspersky, with 60 points. The only other notable result comes from McAfee, with 52 points. All other products scored below 45. The minimum for this test set was 20, the average was 42, and the median was 42. Six products were worse than the average, and seven products were better or equal to the average. The numbers are shown below in Figure 4.

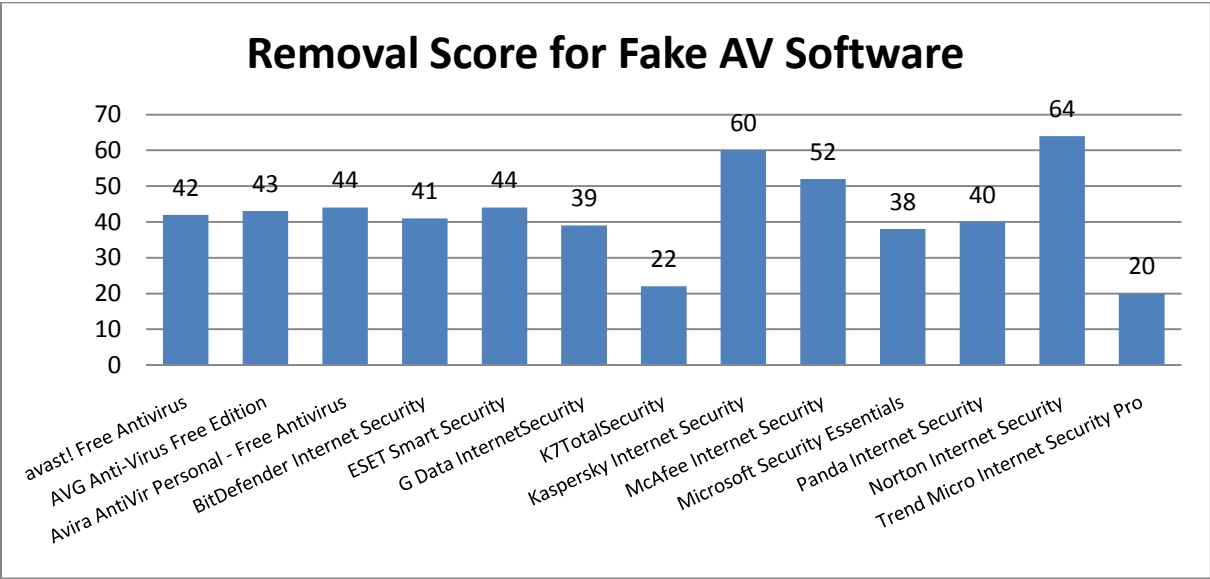


Figure 4: Removal score for Fake AV

In the false positive testing section, no serious problems occurred. Of the installed files, none was detected by any of the programs. However, the VLC installer was reported by both Kaspersky and Panda. However, since the executable was not widely distributed at the time of the test, the effect of these false detections should not be overrated.

A few observations can be made when looking at the individual results. Norton and Kaspersky perform well on both test sets and therefore achieve the number one and number two places in the test. The other products are lacking in a few areas. While Avira does well on other malware, they fall a bit behind for Fake AV. On the other hand, McAfee is doing pretty good on Fake AV but is worse than the average for other malware. Also, the overall scores are considerably lower for other malware compared to Fake AV. This may be related to the fact that “normal” malware often makes use of rootkit techniques, which complicate the detection and removal of their components. On the other hand, Fake AV is very visible on the users system and therefore doesn’t put any effort into hiding itself, which makes the detection easier. The removal can still be tricky, depending on the number and type of the changes performed by the malware.

Another observation is related to the additional removal tools and rescue media. The best scores are achieved by products that offer a removal tool or rescue media. The two products with the best

scores, Kaspersky and Norton, offer both. The products ranked 3rd (Avira) and 4th (shared by G Data and McAfee) do offer either a removal tool or rescue media.

Appendix

Version information of the tested software

Developer, Distributor	Product name	Program version	Engine/ signature version
Alwil Software	avast! Free Antivirus 5.0	5.0.594	100802-0
AVG	AVG Anti-Virus Free Edition 9.0	9.0.851	271.1.1/3045
Avira	Avira AntiVir Personal - Free Antivirus 10.0	10.0.0.567	8.02.04.32/ 7.10.10.26
BitDefender	BitDefender Internet Security 2010	13.0.21.347	7.33151
ESET	ESET Smart Security 4	4.2.58.3	5334
G Data	G Data InternetSecurity 2011	21.0.2.1	Engine A (AVA 21.1806), Engine B (AVB 21.229)
K7 Computing	K7TotalSecurity 10.0	10.0.0039	10.0.0039/ 10.0.0039
Kaspersky Lab	Kaspersky Internet Security 2011	11.0.1.400 (a)	n/a
McAfee	McAfee Internet Security 2010	10.5.194	5400.1158/ 6061.0000
Microsoft	Microsoft Security Essentials	1.0.1963.0	1.1.6004.0/ 1.87.1016.0
Panda Security	Panda Internet Security 2011	16.00.00	2.3.1511.0
Symantec	Norton Internet Security 2011	18.1.0.22	n/a
Trend Micro	Trend Micro Internet Security 2010 Pro	17.50.1647	9.120.1004/ 7.355.50

Table of rescue media and removal tools

Developer, Distributor	Removal Tool	Rescue Media	Comment
Alwil Software	Boot-Time scan has been used when possible	-	A commercial rescue CD can be purchased (not used for the test)
AVG	-	Boot CD	
Avira	-	Boot CD	
BitDefender	-	Boot CD	
ESET	-	Boot CD	SysInspector has not been included in the test
G Data	-	Boot CD	
K7 Computing	-	-	K7 Pre-Install Scan has been used
Kaspersky Lab	Virus Removal Tool 9.0.0.722	Boot CD	
McAfee	Stinger 10.0.1.972	-	
Microsoft	-	-	MSRT has not been included in the test
Panda Security	-	Boot CD	
Symantec	Norton Power Eraser 1.3.0.9	Boot CD	
Trend Micro	SysClean 1.2.0.1005	-	

List of used malware samples

Other malware	Fake AV
0x07dd1f4579bf209c5c6b91a62d51ade9	0x01c77a3d6257ab0a00c33bb255f43386
0x093af61adf36160402784b37809119e5	0x0f324daab13a84b559df56b5bbc721fb
0x1e5261835ecc21fa279d461adf3f97c7	0x0f7474f1d20d5370ad0f57e4f59da249
0x2dfb106445ec06bd8c18969678e7ea1f	0x1ef3dd9e71bd07d0f32599b906198897

0x42ce5b2fa255f650192031e143bc3a45	0x261027d5324ea31fc708f7cb113c48ce
0x537a0d7a41b4dcca3c91e211a35b745	0x285a734327690fc75e066285ab12f5f2
0x8158642d44d011f9c800b97f0128f465	0x2ea42b26746a694a99b5b4cd2bf9f554
0x8e296ee4eb064492616dfcfd0a4c30bc	0x383894791f77313aab87415e3b10e008
0x8eda9c3174f10d43b01566a49c32de4a	0x505c2b2c8dee6c1ffb752709f95f77a2
0x99adf3a8993f4dd702cfaeb18ac4c0a0	0xa3e12ddc7d80b649a9e50672bb8a0d53
0xabd04b6443fb32c9597ffcb12f29b8e3	0xc548edc475d0cffa47ff6862a1552fae
0xbba386d33991fa143fe2898e6f2240f1	0xc85bb0444e3ccbee335b0d4268f8d834
0xdb39977690deac3aa51087f06b42bec5	0xd92ded99a93ab97a1197b99cc77e803b
0xf07f2f779b8257abecb5a172c70c02a3	0xf311ade508007a4590786623d49cb2c5
0xf57dc2e600e9482664c0605e2050745f	0xf77b6c14ccc238960b99014830de2acf

List of used clean samples

Program name	Distribution
Chrome 5.0.375.126	Fewer than 10 users
VLC 1.1.2	Fewer than 10 users
K-Lite Codec Pack 6.2 with Update 20100714	Hundreds of users
Autoit V3 3.3.6.1	Thousands of users
IsoBuster 2.8.0.0	Thousands of users
Java Runtime Environment 1.6.0 update 21	Thousands of users
TrueCrypt7.0	Thousands of users
Adobe Reader 9.3.3	Tens of thousands of users
DivX 8.1.0	Tens of thousands of users
Microsoft dotNetFramework 4.0	Tens of thousands of users
iTunes 9.2.1.5	Tens of thousands of users
IrfanView 4.27	Tens of thousands of users
Winamp 5.581	Tens of thousands of users
GoogleDesktop 5.9.1005.12335	Hundreds of thousands of users
WinZip 14.5 (9095)	Hundreds of thousands of users

Copyright © 2010 by AV-Test GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web <http://www.av-test.org>