

Remediation Testing Report

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

Date of the report: January 27th, 2011, last update: February 10th, 2011

Executive Summary

In January 2011, AV-Test performed a comparative review of 7 corporate endpoint security products to determine their remediation capabilities. In addition to the core product, dedicated removal tools 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 30 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 30 clean applications.

The best result in the described test was achieved by the Symantec product. It reached the highest overall score as well as the highest individual score for one of 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.

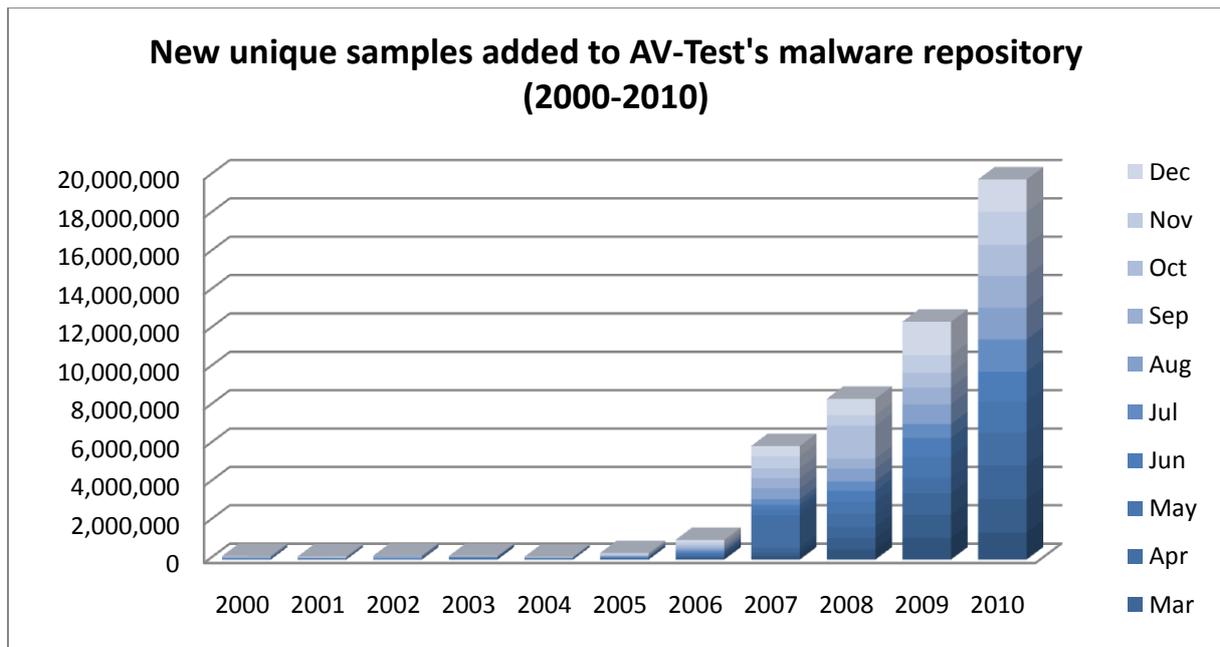


Figure 1: New samples added per year

In the year 2000, AV-Test received more than 170,000 new samples, and in 2009, the number of new samples grew to over 19,000,000 new samples. The numbers continue to grow in the year 2011. 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 testing occurred between December 2010 and January 2011. AV-Test used the latest releases available at the time of the test of the following seven products:

- Kaspersky Anti-Virus 6.0 for Windows Workstations
- Malwarebytes' Anti-Malware 1.50
- McAfee VirusScan Enterprise 8.7.0i
- Microsoft Forefront Client Security 2.0
- Sophos Endpoint Security and Control 9.5.4
- Symantec Endpoint Protection 12.1 (Pre-Beta Release)
- Trend Micro OfficeScan 10.5

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 3 with only those hotfixes that were part of SP3.

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 achieved the best overall removal score for, 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.

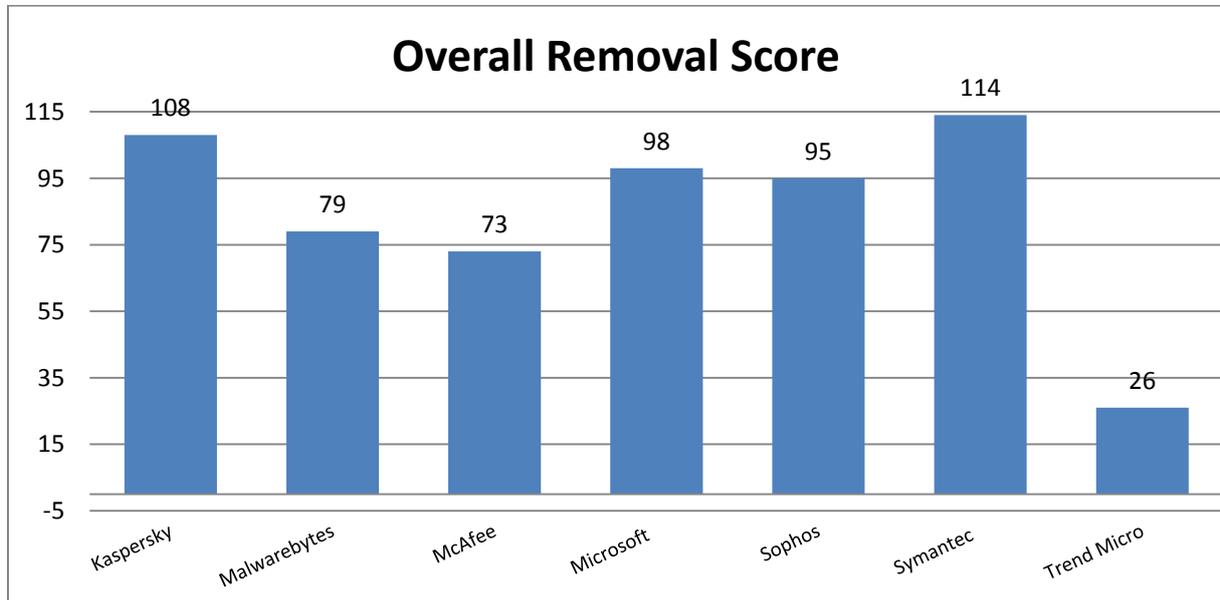


Figure 2: Overall Removal Score

The maximum score that could be reached was 155. The best score was 114, achieved by Symantec. The worst score was 26. The average score was 85 and the median score 95. This means that four products were better than the average and three products were worse than the average. The second best product is very close with 108 points and the third product reached 98 points, the fourth 95 points. All other products were equal to or below 79 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, Symantec again gained the highest score of all products with 73.

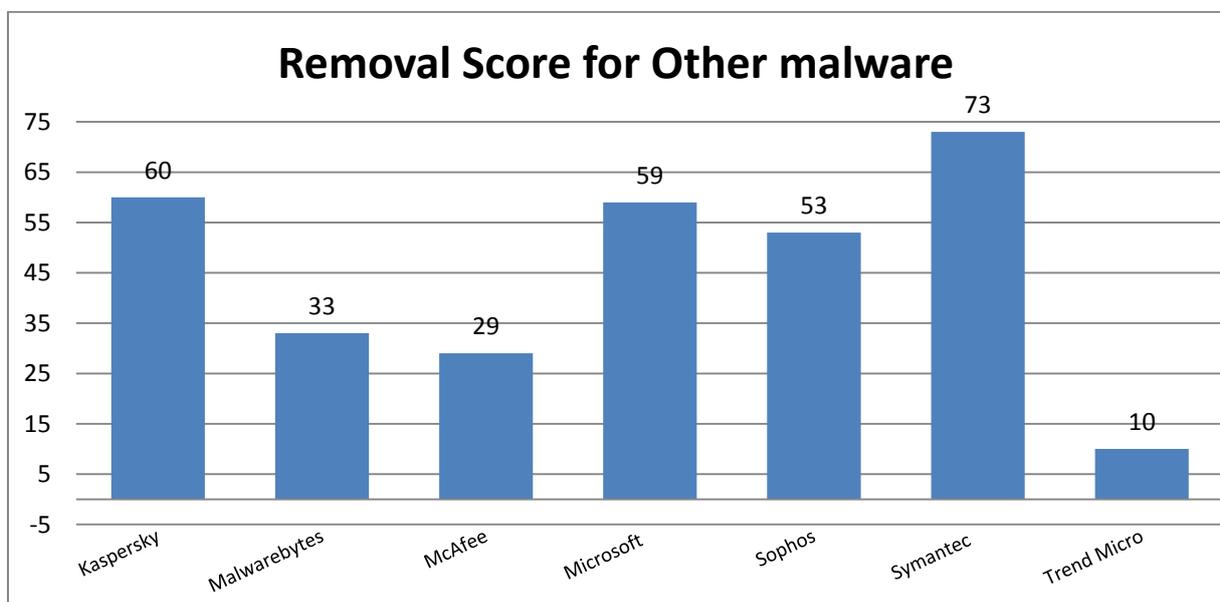


Figure 3: Removal score for other malware

Out of a maximum achievable score of 80, the worst result was 10, while the average was at 45 and the median at 53. Four products scored better than the average and three were worse. Kaspersky achieved the second place with 60 points and Microsoft the third place with 59. Sophos scored 53 points. All other products were below 35 points.

The scores for the removal of Fake AV are a bit different. Most of the products achieved very similar scores. Out of the maximum score of 75 in the Fake AV category, Kaspersky achieved first place with 48 points, closely followed by Malwarebytes, with 46 points and McAfee as well as Sophos with 42 each. Symantec scored 41 and Microsoft 39 points. Only Trend Micro is considerably behind with 16 points. One product was worse than the average, and six products were better or equal to the average of 39. The numbers are shown below in Figure 4.

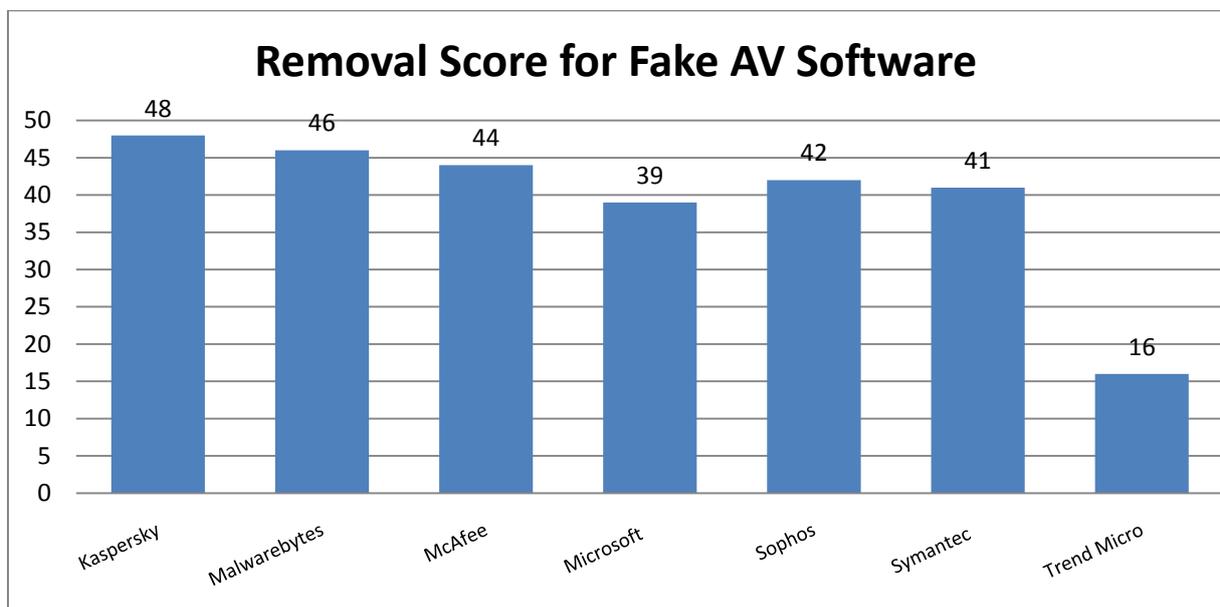


Figure 4: Removal score for Fake AV

In the false positive testing section, no serious problems occurred. Only the Orbit installer was reported by Kaspersky. It prompted the user to remove this software and only then the installation of the Kaspersky security solution could be finished.

However, since the executable was not widely distributed at the time of the test, the effect of this false detection should not be overrated.

A few observations can be made when looking at the individual results. Symantec and Kaspersky perform well on both test sets and therefore achieve the number one and number two places in the test. Microsoft and Sophos do also fine in both test tests and therefore come in as third and fourth product overall. Malwarebytes as well as McAfee show some problems in removing other malware but are good in removing Fake AV software, resulting in a fair overall score. Only Trend Micro is behind the other products for both test sets.

Appendix

Version information of the tested software

Developer, Distributor	Product name	Program version	Engine/ signature version
Kaspersky Lab	Kaspersky Anti-Virus 6.0 for Windows Workstations	6.0.4.1424d	n/a
Malwarebytes	Malwarebytes' Anti-Malware	1.50	n/a
McAfee	McAfee VirusScan Enterprise	8.7.0i	5400.1158 / 6196.0000
Microsoft	Microsoft Forefront Client Security	2.0.522.0	1.1.6402.0 / 1.95.1764.0
Sophos	Sophos Endpoint Security and Control	9.5.4	3.14.1 / 4.60G
Symantec	Symantec Endpoint Protection (Pre-Beta Release)	12.1.175.3818	20101.3.0.103 / 121213ah
Trend Micro	Trend Micro OfficeScan	10.5.1083	9.205.1002 / 1.271.00

Table of rescue media and removal tools

Developer, Distributor	Removal Tool	Rescue Media	Comment
Kaspersky Lab	Virus Removal Tool 9.0.0.722	Boot CD	
Malwarebytes	-	-	
McAfee	Stinger 10.1.0.1009	-	
Microsoft	-	-	MSRT has not been included in the test
Sophos	-	-	
Symantec	Symantec Power Eraser 1.0.4020.230	Boot CD	
Trend Micro	SysClean 1.2.0.1005	-	

List of used malware samples

Other malware	Fake AV
0x000c798b0ace41a51530b23f865b4cb3	0x004af73b77610cbcc4301d34641ad8e1
0x00958427a2bd13a3b6fd48d74d860a7b	0x05e6347319a6b30a8e959f900771eb53
0x018f4edcf37f217894c6e2f548f51717	0x23f7ce16a0f647fbd4705f44304f1769
0x0236a71d9aad6d7b0eb8055c8562ebf	0x25cafe8728efae3851a25f82586b2b31
0x0746d7f2f923098950659e5f568a51f6	0x276fc99ab00a2a091ada493b88836344
0x118d5d3ea1cb4c9d5ac18136e5a2dc47	0x4d089138b5fa2079300a6e3fa4a6920e
0x19da1ef9467bf1bd9461de3b46faa047	0x501dcf3240b4061ed5c26a423a58f37c
0x1c2f028905ba3ee61eba7fffe429494e	0x57f2790bb72ae10810b1e4b605f65628
0x2df2689ff11158f2f61a0ffb52a787f	0x5c2dae037565cf2093fada59b306424d
0x55650825a9f3e82f6505c8d76fdc29c3	0x5ce790fa8e13aea320241ffcf8e5a820
0x9848d80a1cda738ada7787cf93f7be9c	0x5d5e232b71fa10402fd59742e30f8c83
0xa5166ae7d08127d6e46de051d7db4bdc	0x8b9fb9467ce02b7f13e0e52b935e69c1
0xb4e0b338f7b6964c19058e03a75103e6	0xaf124dfe1242002289f6a296ad94d38b
0xd95344cc0224c7ab6f0bb41c437aeb47	0xb9d0af3af8e3ba393b5d9cee0e031aab
0xe4bd67176ad7d0393645e6b9ce530844	0xcd333bfb71623cb1be1e9dbd4c15962d
0xf548c42a67b4296466515064a53a96b9	

List of used clean samples

Program name	Distribution
Sandra 2010 v17.25	Hundreds of users
Skype 5.0	Hundreds of users
Thunderbird 3.1.7	Hundreds of users
Orbit Downloader 4.0.0.5	Thousands of users
Free Mp3 Wma Converter 1.91	Thousands of users
Total Commander 7.56	Thousands of users
Wise Registry Cleaner Free 5.88	Thousands of users
7-Zip	Tens of thousands of users
Divx 8.1.2 Build 10.2.1-20	Tens of thousands of users
Firefox 3.6.13	Tens of thousands of users
GIMP 2.6.11	Tens of thousands of users
mIRC 7.15	Tens of thousands of users
Yahoo Messenger 10.0.0.1270	Tens of thousands of users
Notepad++ 5.8.5	Tens of thousands of users
Paint.NET 3.5.6	Tens of thousands of users
TeamViewer 6.0.9947	Tens of thousands of users
True Crypt 7.0a	Tens of thousands of users
Winamp 5.6	Tens of thousands of users
Adobe Reader 10.0	Hundreds of thousands of users
CCleaner 3.01.1327	Hundreds of thousands of users
DAEMON Tools Lite 4.35.6.0091	Hundreds of thousands of users
Google Talk 1.0.0.104 Beta	Hundreds of thousands of users
iTunes 10.1.0.56	Hundreds of thousands of users
IrfanView 4.27	Hundreds of thousands of users
Open Office 3.2.1	Hundreds of thousands of users
Photoscape 3.5	Hundreds of thousands of users
VLC Player 1.1.5	Hundreds of thousands of users
WinRAR 3.93	Hundreds of thousands of users
Google Desktop 5.9.1005.12335	Millions
Spybot Search & Destroy 1.6.2	Millions