Anti-Virus Comparative

Malware Removal Test

Language: English
September 2009
Last Revision: 24th October 2009

www.av-comparatives.org

Table of Contents

Tested Products

- avast! Professional Edition 4.8
- AVG Anti-Virus 8.5
- AVIRA AntiVir Premium 9.0
- BitDefender Anti-Virus 2010
- eScan Anti-Virus 10.0
- ESET NOD32 Antivirus 4.0
- F-Secure Anti-Virus 2010
- G DATA AntiVirus 2010
- Kaspersky Anti-Virus 2010
- Kingsoft AntiVirus 9
- McAfee VirusScan Plus 2009
- Microsoft Security Essentials 1.0
- Norman Antivirus & Anti-Spyware 7.10
- Sophos Anti-Virus 7.6
- Symantec Norton Anti-Virus 2010
- Trustport Antivirus 2009

Conditions for participation and test methodology

The conditions for participation in our tests are listed in the methodology document at http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf. Before proceeding with this report, readers are advised to first read the above-mentioned document.

Products included in our tests constitute some very good anti-virus software with relatively high on-demand detection rates, as this is one of the requirements needed to be included in our tests. The participation is usually limited to not more than 18 well-known and worldwide used quality Anti-Virus products with relatively high detection rates, which vendors agreed to get tested and included in the public main test reports of 2009. The 16 products that were included in this public test are listed on the previous page.

Introduction

This test focuses only on the malware removal/cleaning capabilities, therefore all 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. A further question was if the products are able to remove what they are able to detect.

Most often user come with infected PC's with no or outdated AV-software to computer repair stores; in our case they brought the compromised machines to the Innsbrucker Computernotdienst, a local partner company of AV-Comparatives. The used methodology considers this situation: an already infected system that needs to be cleaned.

The Test ran between 1st September and 15th September and was run under Microsoft Windows XP Professional SP3 32Bit with latest updates of 1st September 2009. The used Hardware were Hewlett Packard PC's, dc7600 SFF, P4 2.8 GHz, 1GB RAM, sATA-II HDD.

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
- Boot Windows
- if not possible, we started in safe mode; if safe mode was not possible, the BootCD of the AV-Products was used where available
- Install and update the Anti-Virus Product
- Follow instructions of Anti-Virus product to remove the malware
- Run thorough/full scan with highest settings
- Run AV again in safe mode if necessary
- Run AV again from BootCD is necessary
- Manual inspection/analysis of the PC for malware removal and leftovers

Used Malware

The samples have been selected by following criteria:

- all Anti-Virus products were able to detect the used inactive malware on-demand/on-access already at least since begin of August 2009 (in most cases the malware is well-known and detected already since over a half year or longer by all the tested Anti-Virus products)
- the sample must have been seen in the field on at least two PC's of customers who brought their PC for virus cleaning to the local Computernotdienst (a partner company of AV-Comparatives) in the last 12 months
- we selected 50 users-infection cases randomly. After this, we took 10 different malware samples from them (different family, payloads, etc.)
- 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.)
- at least 25% of the samples should be still listed on the WildList[1]

Malware	**Prevalence**[2]
NetSky!30	on the WildList / in-the-field
RJump!38	on the WildList / very widespread
Syrutrk!42	in-the-field
FakeAV!70	in-the-field
Autorun!93	in-the-field
Rontokbro!c5	on the WildList / widespread
Vundo!ca	very widespread
Rustock!e0	widespread
Agent!4d	widespread
ZBot!3d	in-the-field

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

Most Anti-Virus products use generic cleaning procedures for some malware/infections (e.g. heuristic detections or detection added by automation). For the user this does not make a difference, as the user wants to get rid of the malware no matter how the product is detecting it.

[1] http://www.wildlist.org/WildList/200908.htm

[2] Prevalence is based on exact file hash only, not malware families. This data has been consulted with prevalence information given by various vendors and a third party after the test was done. Prevalence is given in this order: in-the-field, widespread, very widespread.

Test Results

Avast

When avast! finds active malware running on the computer, it automatically suggests running a boot-time scan at reboot, in order to be able to remove the running malware. We used this possibility.

Results

NetSky: Avast removed the malware completely from the system.

RJump: Avast removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries.

Syrutrk: Avast removed the malware, but some registry entries were left behind.

FakeAV: Avast removed the malware, but some leftovers (including a binary file) were left behind. A reboot was required to remove the malware.

Autorun: Avast removed the malware, but some traces are still present. The hosts file is still modified and blocks access to e.g. Google and various security related websites.

Rontokbro: Avast removed the malware, but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu).

Vundo: Avast removed the malware, but some registry entries were left behind.

Rustock: Avast removed the malware, but some registry entries that disable Windows Updates were left behind.

Agent: Avast removed the malware, but some registry entries were left behind.

ZBot: Avast required a boot-time scan in order to find (!) and remove the malware. Some non-malicious components and registry entries were left behind.

AVG

Results

NetSky: AVG removed the malware, but some worm components (with non-executable extension) were left behind.

RJump: AVG removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries.

Syrutrk: AVG removed the malware, but some registry entries were left behind.

FakeAV: AVG removed the malware, but some non-malicious leftovers were left behind. A reboot was required to remove the malware.

Autorun: AVG removed the malware, but the registry has not been cleaned (due which Windows Explorer cannot load anymore!). The hosts-file has also not been cleaned.

Rontokbro: AVG removed the malware, but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu).

Vundo: AVG removed the malware, but some registry entries were left behind. AVG required a system reboot to remove the malware.

Rustock: AVG failed to remove the malware.

Agent: AVG removed the malware completely from the system.

ZBot: AVG removed the malware, but some non-malicious components and registry entries were left behind.

AVIRA

AVIRA offers the possibility to create a bootable RescueCD.

Results

NetSky: AVIRA required the Boot-CD to remove the malware completely, as the normal scan did hang.

RJump: AVIRA removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries.

Syrutrk: AVIRA removed the malware, but some registry entries were left behind.

FakeAV: AVIRA removed the malware, but some leftovers (including a binary file) were left behind.

Autorun: AVIRA removed the malware, but the registry has not been cleaned (due which Windows Explorer cannot load anymore!). The hosts-file has also not been cleaned.

Rontokbro: AVIRA removed the malware, but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu).

Vundo: AVIRA removed the malware, but some registry entries were left behind. AVIRA required a system reboot to remove the malware.

Rustock: AVIRA removed the malware, but some registry entries that disable Windows Updates were left behind.

Agent: AVIRA removed the malware, but some registry entries were left behind.

ZBot: AVIRA removed the malware, but some non-malicious components and registry entries were left behind.

BitDefender

BitDefender offers the possibility to create a bootable RescueCD.

Results

NetSky: BitDefender removed the malware completely from the system.

RJump: BitDefender removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries.

Syrutrk: BitDefender removed the malware (a reboot was required), but some registry entries were left behind.

FakeAV: BitDefender removed the malware, but some non-malicious leftovers (including registry entries) were left behind.

Autorun: BitDefender removed the malware, but the registry has not been cleaned (due which Windows Explorer cannot load anymore!). The hosts-file has also not been cleaned.

Rontokbro: BitDefender required the Boot-CD to remove the malware.

Vundo: BitDefender removed the malware, but some registry entries were left behind. BitDefender required a system reboot to remove the malware.

Rustock: BitDefender required the Boot-CD to remove the malware. Some registry entries that disable Windows Updates were left behind.

Agent: BitDefender removed the malware completely from the system.

ZBot: BitDefender removed the malware, but some non-malicious components and registry entries were left behind.

eScan

eScan uses a third-party Anti-Virus engine, but also in-house malware removal routines.

Results

NetSky: eScan removed the malware completely from the system.

RJump: eScan removed the malware completely from the system.

Syrutrk: eScan removed the malware completely from the system. A reboot was required to remove the malware.

FakeAV: eScan removed the malware completely from the system.

Autorun: eScan removed the malware completely from the system.

Rontokbro: eScan removed the malware completely from the system.

Vundo: eScan removed the malware completely from the system.

Rustock: eScan failed to remove the malware.

Agent: eScan removed the malware completely from the system.

ZBot: eScan failed to remove the malware.

ESET

ESET offers the option of creating a bootable Rescue CD. Unlike other Rescue CDs, it is not based on Linux but on Windows (offering better handling of e.g. NTFS drives). Due to that, the creation of the Rescue CD requires a large download (over 1GB) and installation of third party applications.

Results

NetSky: ESET removed the malware, but some worm components (with non-executable extension) were left behind.

RJump: ESET removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries.

Syrutrk: ESET removed the malware (a reboot was required), but some registry entries were left behind.

FakeAV: ESET removed the malware, but some leftovers (including a binary file and some registry entries) were left behind.

Autorun: ESET removed the malware completely from the system.

Rontokbro: ESET removed the malware, but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu).

Vundo: ESET removed the malware, but some registry entries were left behind.

Rustock: ESET required the RescueCD to find (!) and remove the malware. ESET removed the malware, but some registry entries that disable Windows Updates were left behind.

Agent: ESET removed the malware completely from the system.

ZBot: ESET removed the malware, but some non-malicious components and registry entries were left behind.

F-Secure

F-Secure include a bootable RescueCD ready for use in its boxed product.

Results

NetSky: F-Secure removed the malware completely from the system.

RJump: F-Secure removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries.

Syrutrk: F-Secure removed the malware, but some registry entries were left behind.

FakeAV: F-Secure removed the malware, but some non-malicious leftovers were left behind.

Autorun: F-Secure removed the malware, but the registry has not been cleaned (due which Windows Explorer cannot load anymore!). The hosts-file has also not been cleaned.

Rontokbro: F-Secure required the Boot-CD to remove the malware.

Vundo: F-Secure removed the malware completely. During the removal process blue screens and system errors occurred, so that the removal needed several attempts until it was finally successful.

Rustock: F-Secure required the Boot-CD to remove the malware. Some registry entries that disable Windows Updates were left behind.

Agent: F-Secure removed the malware completely from the system.

ZBot: F-Secure removed the malware, but some non-malicious components and registry entries were left behind. F-Secure required a reboot, but instead of doing it automatically as proposed, a reboot had to be initiated manually.

G DATA

G DATA offers the possibility to create a bootable RescueCD.

Results

NetSky: G DATA removed the malware completely from the system.

RJump: G DATA removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries.

Syrutrk: G DATA removed the malware (a reboot was required), but some registry entries were left behind.

FakeAV: G DATA removed the malware, but some non-malicious leftovers (including registry entries) were left behind. A reboot was required to remove the malware.

Autorun: G DATA removed the malware, but the registry has not been cleaned (due which Windows Explorer cannot load anymore!). The hosts-file has also not been cleaned.

Rontokbro: G DATA reported the infection (crashed several times and restarted the OS), but was unable to remove the malware. In addition, the Boot-CD did not help in this case, as it was able to run only in read-only mode.

Vundo: G DATA removed the malware, but some registry entries were left behind.

Rustock: G DATA required the Boot-CD to remove the malware. Some registry entries that disable Windows Updates were left behind.

Agent: G DATA removed the malware, but some registry entries were left behind.

ZBot: G DATA failed to remove the malware. Even the Boot-CD did not help in this case, as it always hang during the scan.

Kaspersky

Kaspersky offers the possibility to create a bootable RescueCD. Furthermore, Kaspersky 2010 products include a feature that allows repairing some specific/common malware traces manually (Security+).

Results

NetSky: Kaspersky removed the malware completely from the system.

RJump: Kaspersky removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries.

Syrutrk: Kaspersky removed the malware, but some registry entries were left behind.

FakeAV: Kaspersky removed the malware, but some leftovers (including a binary file) were left behind. A reboot was required to remove the malware.

Autorun: Kaspersky removed the malware completely from the system.

Rontokbro: Kaspersky removed the malware (a reboot was required), but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu). Those remaining annoying registry leftovers could be fixed using the repair feature inside the Kaspersky 2010 product.

Vundo: Kaspersky removed the malware completely. During the removal process system errors occurred and the system rebooted itself several times, so that the removal needed several attempts until it was finally successful.

Rustock: It was not possible to install the Kaspersky product on the infected system. We therefore tried to first install the AV product and then infect the machine. In that case, Kaspersky removed the malware, but some registry entries that disable Windows Updates were left behind.

Agent: Kaspersky removed the malware completely from the system.

ZBot: Kaspersky removed the malware, but some non-malicious components and registry entries were left behind.

Kingsoft

Results

NetSky: Kingsoft removed the malware, but some worm components (with non-executable extension) were left behind.

RJump: Kingsoft removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries.

Syrutrk: Kingsoft removed the malware, but some registry entries were left behind.

FakeAV: Kingsoft removed the malware, but some leftovers (including a binary file) were left behind.

Autorun: Kingsoft failed to remove the malware.

Rontokbro: Kingsoft removed the malware, but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu).

Vundo: Kingsoft failed to remove the malware.

Rustock: Kingsoft failed to remove the malware.

Agent: Kingsoft removed the malware completely from the system.

ZBot: Kingsoft failed to remove the malware.

McAfee

McAfee uses an online-installer for the installation of its product.

Results

NetSky: McAfee removed the malware completely from the system.

RJump: McAfee removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries.

Syrutrk: McAfee removed the malware (a reboot was required), but some registry entries were left behind.

FakeAV: McAfee removed the malware, but some non-malicious leftovers were left behind.

Autorun: It was not possible to install McAfee[3], as McAfee requires always an online-installation and does not offer an offline-installer or a Boot-CD. This is especially problematic when the malware blocks access to the AV vendor websites. For testing purposes, we modified the hosts-file in order to be able to install McAfee. In that case, McAfee removes the malware, but it does not fix the registry, due which Windows Explorer does not start anymore. We also tried to download from a third-party site the standalone STINGER utility from McAfee. While running STINGER with activated McAfee and highest settings, it reported 2 clean files as Trojans on standard preinstalled files on HP systems.

Rontokbro: McAfee removed the malware, but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu).

Vundo: McAfee removed the malware, but some registry entries were left behind. McAfee required a system reboot to remove the malware.

Rustock: McAfee removed the malware, but some registry entries that disable Windows Updates were left behind.

Agent: McAfee removed the malware completely from the system.

ZBot: McAfee had to be installed in safe-mode. McAfee removed the malware, but some non-malicious components and registry entries were left behind.

[3] If users have trouble while installing the product or cleaning their machines they can contact the McAfee technical support (first 30 days from purchase there is free phone support). Virtual Technician can help with many types of problems. http://service.mcafee.com/TechSupportHome.aspx?lc=1033&sg=TS

Microsoft

Results

NetSky: Microsoft removed the malware completely from the system.

RJump: Microsoft removed the malware, but some registry entries were left behind.

Syrutrk: Microsoft removed the malware completely from the system. A reboot was required to remove the malware.

FakeAV: Microsoft removed the malware, but a non-malicious leftover was left behind. Microsoft required a system reboot to remove the malware.

Autorun: Microsoft removed the malware, but some traces are still present. The hosts file is still modified and blocks access to e.g. Google and various security related websites. Only the access to some few major AV websites has been restored.

Rontokbro: Microsoft removed the malware, but some registry entries were left behind which have annoying consequences (e.g. regedit disabled, Folder Options are no longer visible/available in the menu).

Vundo: Microsoft removed the malware, but some registry entries were left behind. Microsoft required a system reboot to remove the malware.

Rustock: Microsoft removed the malware, but some registry entries that disable Windows Updates were left behind. Microsoft required a system reboot to remove the malware.

Agent: Microsoft removed the malware completely from the system.

ZBot: Microsoft removed the malware, but some non-malicious components and registry entries were left behind. Microsoft required a system reboot to remove the malware.

Norman

Results

NetSky: Norman removed the malware, but some worm components (with non-executable extension) were left behind.

RJump: Norman removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries. A reboot was required to remove the malware.

Syrutrk: Norman removed the malware (a reboot was required), but some registry entries were left behind.

FakeAV: Norman removed the malware, but some non-malicious leftovers (including registry entries) were left behind.

Autorun: Norman removed the malware, but the registry has not been cleaned (due which Windows Explorer cannot load anymore!). The hosts-file has also not been cleaned.

Rontokbro: Norman removed the malware, but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu).

Vundo: Norman removed the malware, but some registry entries were left behind. Norman required a system reboot to remove the malware.

Rustock: Norman removed the malware, but some registry entries that disable Windows Updates were left behind.

Agent: Norman removed the malware, but some registry entries were left behind.

ZBot: Norman failed to remove the malware.

Sophos

Sophos offers the possibility to create a bootable RescueCD.

Sophos is a corporate product. Due that, it does not restore e.g. some registry entries by design, as in a managed environment, some of these settings are typically enforced centrally by system administrators.

Results

NetSky: Sophos removed the malware, but some worm components (with non-executable extension) were left behind.

RJump: Sophos removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries. A reboot was required to remove the malware.

Syrutrk: Sophos removed the malware completely from the system.

FakeAV: Sophos removed the malware, but some non-malicious leftovers were left behind.

Autorun: Sophos removed the malware, but some traces are still present. The hosts file is still modified and blocks access to e.g. Google and various security related websites. Only the access to some few major AV websites has been restored.

Rontokbro: Sophos removed the malware, but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu).

Vundo: Sophos removed the malware, but some registry entries were left behind. During the removal process blue screens and system errors occurred and the system rebooted several times by itself, so that the removal needed several attempts until it was finally successful.

Rustock: Sophos had to be installed in safe-mode. In that case, Sophos removed the malware, but some registry entries that disable Windows Updates were left behind.

Agent: Sophos removed the malware completely from the system.

ZBot: Sophos removed the malware, but some non-malicious components and registry entries were left behind. Sophos required a system reboot to remove the malware.

Symantec

Symantec includes a bootable RescueCD ready for use in its boxed product.

Results

NetSky: Symantec removed the malware completely from the system.

RJump: Symantec removed the malware completely from the system.

Syrutrk: Symantec removed the malware completely from the system. A reboot was required to remove the malware.

FakeAV: Symantec removed the malware, but some non-malicious leftovers were left behind. Symantec had to be installed in safe-mode.

Autorun: Symantec removed the malware, but some traces are still present. The hosts file is still modified and blocks access to e.g. Google and various security related websites. Only the access to some few major AV websites has been restored.

Rontokbro: Symantec removed the malware (the scan had to be done in safe mode, as in normal mode the system continued to reboot continuously after installation), but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu).

Vundo: Symantec removed the malware, but some registry entries were left behind. Symantec required a system reboot to remove the malware.

Rustock: Symantec removed the malware, but some registry entries that disable Windows Updates were left behind.

Agent: Symantec removed the malware completely from the system.

ZBot: Symantec removed the malware, but some non-malicious components and registry entries were left behind.

Trustport

Trustport offers the possibility to create a bootable RescueCD.

Results

NetSky: Trustport removed the malware, but some worm components (with non-executable extension) were left behind.

RJump: Trustport removed the malware, but some non-malicious malware traces were left behind, as well as some registry entries. A reboot was required to remove the malware.

Syrutrk: Trustport removed the malware (a reboot was required), but some registry entries were left behind.

FakeAV: Trustport removed the malware, but some non-malicious leftovers (including registry entries) were left behind.

Autorun: Trustport removed the malware, but the registry has not been cleaned (due which Windows Explorer cannot load anymore!). The hosts-file has also not been cleaned.

Rontokbro: Trustport removed the malware, but some registry entries were left behind which have annoying consequences (e.g. showing an error message at every system restart, regedit disabled, Folder Options are no longer visible/available in the menu). Additionally, an Autostart entry was only renamed instead of deleted, giving an additional pop-up at system start.

Vundo: Trustport removed the malware, but some registry entries were left behind. A reboot was required to remove the malware, but it had to be initiated manually.

Rustock: Trustport required the Boot-CD to find (!) and remove the malware. Trustport removed the malware, but some registry entries that disable Windows Updates were left behind.

Agent: Trustport removed the malware completely from the system.

ZBot: Trustport removed the malware, but some non-malicious components and registry entries were left behind.

Ratings

The ratings (and the resulting awards) are calculated based on

a) Removal of malware
    a. Malware completely removed (10)
    b. Malware removed, some unimportant traces left (8)
    c. Malware removed, but annoying or potentially dangerous problems remaining (4)
    d. Malware not removed (0)

b) Removal of leftovers
    a. No remaining leftovers (4)
    b. Innocent non-executable files or unimportant registry entries remaining (3)
    c. Non-malicious, but visible executable files remaining (2)
    d. Registry entries (e.g. loading points, etc.) remaining (1)
    e. Malicious executable files remaining or registry entries which cause problems/annoyance (like pop-ups, error messages, windows not booting, windows updates disabled, hosts file blocking websites, registry disabled, etc.) (0)

c) Convenience:
    a. Removal could be done easily in normal mode (5)
    b. Reboot (or manual actions) required to remove the malware or some entries (4)
    c. Errors/BSOD during malware removal (3)
    d. Removal required booting in safe-mode (2)
    e. Removal required creation of a Boot-CD (1)
    f. Detection required a scan from Boot-CD/safe mode or install required contacting support or similar (0)

Points are given according to the above system, averaged and categorized as follow:

a) Removal of malware
    a. 0.0 – 5.0 (poor)
    b. 5.1 – 6.6 (average)
    c. 6.7 – 8.0 (good)
    d. 8.1 – 10.0 (very good)

b) Removal of leftovers
    a. 0.0 – 1.0 (poor)
    b. 1.1 – 2.0 (average)
    c. 2.1 – 3.0 (good)
    d. 3.1 – 4.0 (very good)

c) Convenience
    a. 0.0 – 2.5 (poor)
    b. 2.6 – 3.5 (average)
    c. 3.6 – 5.0 (good)

Convenience: All products were more or less same convenient, therefore this category was this time not counted for the awards.

Even if not observed during this test, over-aggressive cleaning has not been specifically considered/evaluated during the test, but may be an interesting point to consider in the next test.

Based on the above scoring system, we get the following summary results:

	Removal of malware	Removal of leftovers
Avast	average	average
AVG	average	average
AVIRA	average	average
BitDefender	good	average
eScan	good	good
ESET	average	average
F-Secure	good	average
G DATA	average	poor
Kaspersky	good	average
Kingsoft	poor	poor
McAfee	average	average
Microsoft	good	good
Norman	average	poor
Sophos	average	average
Symantec	good	good
Trustport	average	average

None of the products performed "very good" in malware removal or removal of leftovers, based on those 10 samples. eScan, Symantec and Microsoft (MSE) were the only products to be good in removal of malware AND removal of leftovers.

Due the sample size, the final ratings may be generous, but we applied the scoring tables strictly. We tried to give different values for different types of leftovers, although this was very difficult in some grey area cases. This was the first public malware removal test of AV-Comparatives and due the lack of generally accepted ways to rate malware removal abilities, we did our best to give fair ratings based on the observed overall malware removal results and to do not look / base our ratings on e.g. the deletion of the binary malware only.

Some products do not remove all registry entries on purpose (as long as they do not have any visible side effect for the user), e.g. if that helps to prevent reinfection by the same malware. Furthermore, in some cases it is not possible to know if the registry values (or the hosts file) were modified by the malware or by the user itself (or third-party utilities used by the user). Therefore, some AV products may decide to do not touch those values and to do not restore default/standard values. For most home users it may be OK to reset to default, but in some cases, especially in corporate environments, restoring default settings could break the security policy of the company. We think that giving an option to the user to restore such values after a malware infection (during malware removal) could be useful to clean up completely a PC.

Leaving behind leftovers (even if just non-malicious components/files or some entries in the registry) could lead to make users believe to have still active malware on their PC, e.g. when they run another Anti-Virus product or more probably some other Anti-Spyware product. Anti-Spyware products very often report traces/leftovers and then claim to be able to detect malware which other Anti-Virus products are not able to find, without saying that the leftovers were not doing anything malicious. Beside that, it does not even mean that those products would be able to remove the real malware running on the PC, as the Anti-Virus product may have been able to do.

Good malware detection is very important to find existing malware that is already on a system. However, a high detection rate of a product does not necessarily correspond/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 removed 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.

Additional Free Malware Removal Services/Utilities offered by the vendors

	Boot-Disk[4]	Free Online Scanner with removal ability[5]	Free Removal-Tools for specific malware
Avast	No	No	http://www.avast.com/eng/avast-virus-cleaner.html
AVG	No	No	http://www.avg.com/virus-removal
AVIRA	YES	No	http://www.avira.com/en/support/antivir_removal_tool.html
Bitdefender	YES	http://www.bitdefender.com/scanner/online/free.html	http://www.bitdefender.com/site/Downloads/browseFreeRemovalTool
eScan	No	No	http://www.mwti.com/products/mwav/mwav.asp
ESET	YES	http://www.eset.com/onlinescan	http://www.eset.com/download/free-virus-remover.php
F-Secure	YES	http://www.f-secure.com/en_EMEA/security/security-lab/tools-and-services/online-scanner/index.html	http://www.f-secure.com/en_EMEA/security/security-center/easy-clean/index.html
G DATA	YES	No	No
Kaspersky	YES	No	http://support.kaspersky.com/viruses/avptool?level=2
Kingsoft	No	No	No
McAfee	No	No	http://home.mcafee.com/VirusInfo/VirusRemovalTools.aspx
Microsoft	No	http://onecare.live.com/site/en-US/center/howsafe.htm	http://www.microsoft.com/security/malwareremove
Norman	No	No	http://www.norman.com/support/support_tools/58732/en-us
Sophos	YES	No	http://www.sophos.com/support/disinfection
Symantec	YES	No	http://www.symantec.com/norton/security_response/removaltools.jsp
Trustport	YES	No	No

In some cases the above mentioned additional free malware removal utilities are in our opinion not advertised enough, in other words most users may not know about their availability when they need it. They should be promoted inside the user manuals, inside the product, provided thru an information box in case of a specific infection (or in case of unsuccessful malware removal) or be better placed on the vendors' website.

[4] Included in the standard package without extra charging.

[5] Must be free, not requiring registration, must provide free removal (not just detection) and be able to scan a PC (not only single files).

Awards reached in this test

AV-Comparatives provides a 3-level-ranking-system (STANDARD, ADVANCED and ADVANCED+). As this report contains also the raw results and not only the awards, users can evaluate the results by themselves if they prefer.

AWARDS (based on removal capabilities)	**PRODUCTS** (in no specific order)[6]
AV comparatives ADVANCED+ ★★★ MALWARE REMOVAL OCT 09	eScan Symantec Microsoft[7] F-Secure Kaspersky Bitdefender
AV comparatives ADVANCED ★★ MALWARE REMOVAL OCT 09	ESET Sophos AVG McAfee Avast AVIRA Trustport
AV comparatives STANDARD ★ MALWARE REMOVAL OCT 09	Norman G DATA
AV comparatives TESTED MALWARE REMOVAL OCT 09	Kingsoft

Please keep in mind, that the ten used prevalent samples were selected randomly, based on infected user PC's from the real world. With other samples, the results could be completely different.

It may not look fair to give awards in a test with only ten randomly selected samples. However, malware is also not fair and users cannot select which malware hits their PC's. Therefore, it could be exactly that one not removed malware sample, which kills your PC.

[6] We suggest to consider products with same the award to be as good as the other products with same award.
[7] Microsoft OneCare would have scored Advanced.

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. (October 2009)