Anti-Virus Comparative

Summary Report 2006

Results, winners, comments

Date: December 2006

Last revision: 8th December 2006

Author: Andreas Clementi

Website: http://www.av-comparatives.org

1. Introduction

From now on, at the end of every year, AV-Comparatives will release a summary report to show and comment the various tested Antivirus products and to determine who are the „winners“ in the various tests.
Please keep in mind that this report considers the results reached during all the various tests of 2006 and not only the latest ones. Comments and conclusions are based on the results contained in the various test reports of AV-Comparatives. You can find them on www.av-comparatives.org/seiten/comparatives.html.

2. Overview of levels reached during 2006

Only products with good detection rates can participate in the regular test-series of AV-Comparatives. It is important that readers understand that also the STANDARD level/award is already a good score, as to get it it is required to detect a minimum percentage of malware. Many products that are not listed on AV-Comparatives would by far not reach the minimum requirements to participate; therefore the ones that are included in the tests of AV-Comparatives can be considered to be already a selection of good Antivirus products.
Below the overview of levels/awards reached by the various Antivirus in the main tests of AV-Comparatives during 2006:

	February 2006 On-demand test	**May 2006** *Retrospective test*	**August 2006** On-demand test	**November 2006** *Retrospective test*
Avast	ADVANCED	*ADVANCED*	ADVANCED	*STANDARD*
AVG	STANDARD	*STANDARD*	STANDARD	▨
AVIRA	ADVANCED+	*ADVANCED*	ADVANCED+	*ADVANCED+*
BitDefender	ADVANCED	*ADVANCED+*	ADVANCED	*ADVANCED+*
Dr.Web	STANDARD	*ADVANCED*	STANDARD	*STANDARD*
F-Prot	STANDARD	*STANDARD*	STANDARD	*STANDARD*
F-Secure	ADVANCED+	*ADVANCED*	ADVANCED+	*STANDARD*
Gdata AVK	ADVANCED+	*ADVANCED+*	ADVANCED+	*ADVANCED+*
Kaspersky	ADVANCED+	*ADVANCED*	ADVANCED+	*STANDARD*
McAfee	ADVANCED+	*ADVANCED*	ADVANCED	*STANDARD*
NOD32	ADVANCED+	*ADVANCED+*	ADVANCED+	*ADVANCED+*
Norman	STANDARD	*ADVANCED*	ADVANCED	*ADVANCED*
Symantec	ADVANCED+	*STANDARD*	ADVANCED+	*STANDARD*
TrustPort	ADVANCED+	*ADVANCED+*	ADVANCED+	*ADVANCED+*
VBA32	▨	*ADVANCED*	▨	*STANDARD*

Note: ‘grey’ means ‘certification level not reached’.

3. “Winners”

If you plan to buy an Anti-Virus, please visit the vendor's site and evaluate their software by downloading a trial version, as there are also many other additional features (e.g. firewall, behaviorblocker, spamfilter, etc.) and important things (e.g. compatibility, graphical user interface, system impact, managebility, language, price, license size, etc.) for an Anti-Virus that you should evaluate by yourself.
As explained above, a perfect Antivirus or the „best“ Antivirus for all needs and for every user does not exist. The here determined „winners“ take in consideration only the objective test data and do not evaluate or consider other factors that may be of importance for specific users need or preference.

a) Overall winner(s) of 2006 based on the reached levels and subtest results:

The following products received the ADVANCED+ award in all 4 main tests of AV-Comparatives during 2006: AVK 2006, NOD32, TrustPort (AVK 2006 takes here a special position, as AVK 2007 would not have earned an ADVANCED+ award in the last retrospective test).
AVK 2006 and TrustPort are multiengine products (both use e.g. the BitDefender engine along with another engine, e.g. Kaspersky, Norman), while NOD32 is a single engine product. The negative thing of multiengine products is their negative impact on the scanning speed, as well as the multiplied false alarm occurence.
Therefore, the Overall Anti-Virus product winner of 2006 is: **NOD32**.

b) On-Demand detection winner(s):

The following products received the ADVANCED+ award in both overall on-demand detection tests of February and August 2006: AVIRA, GDATA AVK, F-Secure, Kaspersky, NOD32, Symantec and TrustPort.
The following products had in both tests results over 99%: GDATA AVK, F-Secure, Kaspersky.
Therefore, the On-Demand detection winners are all Antivirus that are powered by the Kaspersky engine: **GDATA AVK**, **F-Secure** and **Kaspersky**.

c) Proactive On-Demand detection winner(s):

The retrospective tests show how good the on-demand proactive detection of the various Antivirus products is. It is possible that main products like Kaspersky, McAfee and Symantec are not good in these tests not only because their heuristic/generic detections are not as good as other products, but also because some malware authors may release their creations only if they are not detected proactivly by such main Anti-Virus products. Therefore, users of mainstream Antivirus products could be more exposed than users using other antivirus software. Kaspersky, F-Secure, McAfee, Symantec and some others try to solve this gap with other proactive detection mechanisms, but which work only when the malware is executed: which can be a risky thing and not be applicable in every situation, and lead to more false alarms than heuristics.
The following products received the ADVANCED+ award in both retrospective tests of May and November 2006: AVK 2006, BitDefender, NOD32, TrustPort.
The following product had in both tests results over 50%: NOD32.
Therefore, the Proactive On-Demand detection winner is: **NOD32**.

d) False Positives winner(s):

False positives can cause as much troubles as a real infection. Due that, it is important that Antivirus products have stringent Quality Assurunce testing before release to public (in order to avoid false positives).
The products with the lowest rate of false positives during 2006 were: Symantec (0), McAfee (2), AVG (4) and Norman (6).
Therefore, the product with the lowest rate of false positives in the AV-Comparatives tests of 2006, with the exceptional score of zero false alarms in both tests is: **Symantec**.

e) <u>On-Demand Scanning Speed test winner(s)</u>:

The products with the highest througput rate (green bar) were: AVIRA, NOD32, AVG, Symantec and McAfee. The fastest products - with a througput rate over 7 MB/sec - were in both tests (with best possible detection settings): AVIRA, NOD32. Between those two products, AVIRA was a bit faster than NOD32 in scanning the set of clean files with best possible detection settings. With default settings NOD32 is faster than AVIRA.

Therefore, the On-Demand Scanning Speed winner with best possible detection settings is: **AVIRA** and the On-Demand Scanning Speed winner with default settings is: **NOD32**.

f) <u>Polymorphic Virus detection test winner(s)</u>:

The following products were able in both tests to detect 100% of all polymorphic viruses included in the test-set: Symantec. AVIRA was only in the last polymorphic test able to detect all samples.

Therefore, the Polymorphic Virus detection winner is: **Symantec**.

<u>Summary</u>:

a) Overall: **NOD32**
other candidates were: TrustPort, AVK 2006

b) On-Demand detection: **KAV powered AV’s: AVK, F-Secure, Kaspersky**
other candidates were: AVIRA, NOD32, Symantec, TrustPort

c) Proactive on-demand detection: **NOD32**
other candidates were: BitDefender, TrustPort, AVK2006

d) Lowest false positive rate: **Symantec**
other candidates were: McAfee, AVG, Norman

e) Highest on-demand scanning speed (with best settings): **AVIRA**
Highest on-demand scanning speed (with default settings): **NOD32**
other candidates were: AVG, Symantec, McAfee

f) Most reliable polymorphic virus detection: **Symantec**
other candidates were: AVIRA

4. Comments

Below some comments about the various products included in the test-series of 2006, regarding their results, capabilities and future prospectives:

Avast (www.avast.com): Avast earned during 2006 3 ADVANCED awards and 1 STANDARD award. Since the last on-demand test of August 2006, Avast is adding many malware which was before undetected. This will very probably be noticied in an improvement in Avast detection rates during 2007. Anyway, in order to continue to improve, Avast will probably need to further improve also their heuristic/generic detections.

AVG (www.grisoft.com): AVG is a fast scanner with a low rate of false positives incidents. During 2006 the detection rates in the various tests were not very high (STANDARD) and it did not reached good results in the retrospective tests. This may change during 2007, as Grisoft acquired during 2006 the Ewido company and is now offering a new product which combines AVG Antivirus with the Antimalware product of Ewido. AV-Comparatives will include this new product (AVG AntiMalware) which offers more protection against viruses, malware and spyware and also an improved heuristic.

AVIRA (www.avira.com): AVIRA was the most improving product of 2006, being able to surpass in the second half of 2006 most of the tested products in various tests. In the first retrospective test AVIRA reached high results, but it still had many false positives and therefore got only the ADVANCED award. In the last retrospective test AVIRA was with best possible detection settings on par with NOD32 (ADVANCED+) and got also few false positives and had the fastest on-demand scanning speed. The overall on-demand detection rate of AVIRA also improved much (ADVANCED+). If AVIRA is able to keep this level also during all tests of 2007, it will be a strong candidate for the „overall winner“ of next years tests.

BitDefender (www.bitdefender.com): BitDefender showed in the retrospective test to have a very good heuristic (ADVANCED+) and a good overall on-demand detection rate (ADVANCED). During last months BitDefender improved further in both areas, and will show its improvements in the tests of 2007. The heuristic of BitDefender requires system resources and is not very fast. BitDefender includes a behaviorblocker (B-Have) which may show its full potential only while the malware is already executed. Tests of similar proactive detection technologies showed that they offer usually very high protection.

Dr.Web (www.drweb.com): Dr.Web is known for its powerful heuristic, but unfortunatly, it still causes too many false alarms (due that, the results of Dr.Web in the retrospective tests had to be penalized, as a product which causes many false positives do not deliver a reliable proactive detection) and the scanner is not very fast in on-demand scanning. In the overall on-demand detection tests Dr.Web reached during 2006 the STANDARD award. AV-Comparatives thinks that Dr.Web would be able to have higher results, but it is unclear why the improvements are made so slow. AV-Comparatives is in contact with a representative of Dr.Web which promised that Dr.Web will do its best to improve further the detection rates.

ESET (NOD32) (www.eset.com): NOD32 reached in the retrospective tests always the highest awards (ADVANCED+), due ist high proactive on-demand detection rate and the low rate of false alarms. Also in the overall on-demand detection tests NOD32 was able to reach the ADVANCED+ awards, but there is still area for further improvements. Additionally NOD32 was one of the fastest scanner in scanning on-demand the set of clean files. In total, NOD32 earned the status of overall winner of the tests of 2006.

F-Prot (www.f-prot.com): During 2006, F-Prot reached in the various tests always the STANDARD award. This will very probably change in the tests of 2007, when the new version 4 of F-Prot will be tested. F-Prot v4 will include e.g. a new heuristic engine, which - based on internal tests of AV-Comparatives – would have reached the ADVANCED+ award in the latest retrospective test and the ADVANCED award in the overall on-demand detection test of August 2006. Additionally, F-Prot v4 will also provide good on-demand detection of dialers.

F-Secure (www.f-secure.com): F-Secure uses many various engines in its product. Between them also the AVP engine (which uses the signatures of Kaspersky), with which F-Secure showed very high results in the overall on-demand detection tests (and very similar results like KAV). Like in most multi-engine AV products, a side-effect can be observed in the lower on-demand scanning speed.
F-Secure 2006 had like KAV not very good results in the retrospective tests: Anyway, the new F-Secure 2007 includes (beside an improved spyware detection) a proactive detection technology (DeepGuard) to protect against new/unknown malware (which works when the malware is already executed and not on-access/on-demand before the execution – therefore the results in our retrospective on-demand tests would not change). Tests of similar proactive detection technologies showed that they offer usually very high protection.

GDATA (AVK) (www.gdata.de): AVK 2006 version was tested in the tests of 2006. AVK 2006 used two engines in its product: Kaspersky engine and BitDefender engine. Thanks to this DoubleScan technology AVK 2006 earned the ADVANCED+ award in all 4 testss of 2006, showing high results in the overall on-demand detection tests and in the retrospective tests. A side-effect of using two scan engines in one product is the slow on-demand scanning speed. Recently GDATA changed one of the engines in AVK: the BitDefender engine has been replaced with the Avast engine. The benefits of this change are slightly higher overall on-demand detection rates and lesser system impact (incl. faster on-demand scanning). Unfortunatly, by taking out the BitDefender engine, the results of AVK 2007 in the retrospective tests are lower (in the retrospective test of November 2006, AVK 2007 would have received the STANDARD award, while AVK 2006 earned the ADVANCED+ award).

Kaspersky (www.kaspersky.com): Kaspersky is one of the products with the highest overall on-demand detection rates (along with the products which are powered by the KAV engine, like e.g. AVK, F-Secure, etc.). In the retrospective tests KAV did not reach very high results, but the version 6 of KAV includes a behaviorblocker (PDM) which will protect against malware during its execution. Tests of this proactive detection technology showed that it offers a very high protection.

McAfee (www.mcafee.com): During the second half of 2006, the detection rates of McAfee falled a bit down, both regarding the overall detection rate (from ADVANCED+ to ADVANCED) and the retrospective test (from ADVANCED to STANDARD). The reason may be in the higher focus in detection quality than quantity, in order to avoid false positives. In the false positives tests of 2006 McAfee had always only 1 false alarm, which is a very good score. The new scan engine of McAfee also showed to have improved regarding the scanning speed. The new version 2007 of McAfee VirusScan Plus is now only available bundled together with a better protection against spyware, a firewall (which can be disabled if not wanted) and some other tools. It also includes the SystemGuard intrusion prevention component, which does behaviorblocking / prevention. Advanced users may find McAfee VirusScan Plus 2007 offering too few settings and not like the screen about the SecurityCenter. We think that McAfee will during 2007 improve esp. the generic/heuristic detections and then be again on the same high levels like it was in past.

Norman (www.norman.com): Norman showed during 2006 to constantly improve, earning in last two tests the ADVANCED awards. Since the last on-demand test of August, Norman is adding a lot of malware it was missing to detect before, which could bring Norman in 2007 even higher results combined with its sandbox heuristic. In the on-demand retrospective tests of AV-Comparatives Norman reached the ADVANCED awards; anyway, Norman has a sandbox technology which shows its full potential only while the malware is executed. Tests of similar proactive detection technologies showed that they offer usually very high protection. Norman will soon release a new product version.

Symantec (www.symantec.com): Symantec (NAV) showed during 2006 to be Antivirus product with the best detection of polymorphic viruses, by remaining fast in on-demand scanning and by producing as only Antivirus product in our tests no false positives. In the overall on-demand detection tests Symantec had very high results (ADVANCED+), while in the retrospective tests it reached only the STANDARD award. Symantec Norton Internet Security 2007 includes a HIPS, which will block malicious software during the execution of malware based on its behaviour. Tests of similar proactive detection technologies showed that they offer usually very high protection.

TrustPort (www.aec.cz): TrustPort combines two antivirus engines in its product: BitDefender engine and Norman engine. Thanks to those engines, TrustPort had very high overall on-demand detection rates and high results in the retrospective tests, earning the ADVANCED+ award in each of the 4 tests of 2006. The side-effect of using the BitDefender and Norman engine is the slow on-demand scanning speed.

VBA32 (www.anti-virus.by): VBA32 has proved to have a very aggressive heuristic, but unfortunately it still produces many false positives (due to that fact, the results of VBA32 in the retrospective tests had to be penalized, as a product which causes many false positives expects a user to be well-qualified to make a final decision) and takes much time to scan on-demand if the thorough mode option is enabled. Thorough mode sets the excessive mode of file scan. At that, a user is warned as follows: "Caution: Excessive mode can seriously increase the time of file processing".
The thorough mode will be modified in the next version of VBA32, but will still provide the same level of protection.
In 2007 VBA32 will be probably tested within another group of antivirus products and not in the main group.

5. Future tests of 2007

During 2007, AV-Comparatives will (beside improving and expanding the various tests) update the Test-PC’s with newer and more powerful hardware in order to continue to carry out the tests in a timeful manner and also on Windows Vista Ultimate (probably second half of 2007).

Rootkits are becoming a major threat and Antivirus products are evolving to protect also against such nasty malware. A test of Antivirus products against active rootkits is planned to be done within next year.

More and more Antivirus vendors are adding proactive detection technologies (like Sandbox, HIPS, behaviorblocker, etc.) to their products, in order to try to protect against new/undetected malware when all other protection mechanism failed. A test of only Antivirus products which contain such technologies will be done within 2007.

Like in 2006, all those tests and possibly more tests can be found on http://www.av-comparatives.org/seiten/comparatives.html.

In the main test-series of 2007 (which number of participants is limited due time/resource limitations) the top products of the following vendors will probably be included: Avast, AVG, AVIRA, AVK, BitDefender, Dr.Web, eScan, ESET, F-Prot, F-Secure, Fortinet, Kaspersky, McAfee, Microsoft, Norman, Symantec and TrustPort.

There will be probably also an additional (limited) comparative where also other vendors can take part if they want to. Currently the following vendors will most probably take part in it: Comodo, Ikarus, K7, Rising, UNA, VBA32. Another dozen of vendors were also invited but were apparently not interested in taking part in the official tests of next year.

6. Copyright and Disclaimer

This publication is Copyright (c) 2006 by AV-Comparatives. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of AV-Comparatitves, 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.

Andreas Clementi, AV-Comparatives (December 2006)