Anti-Virus Comparative
No. 23, August 2009

On-demand Detection of
Malicious Software
includes false alarm and on-demand scanning speed test

Language: English
August 2009
Last Revision: 2009-09-19

www.av-comparatives.org
# Table of Contents

Tested Products 3

Conditions for participation and test methodology 4

Tested product versions 4

Comments 5

Test results 6

Graph of missed samples 7

Summary results 9

False positive/alarm test 10

Scanning speed test 11

Award levels reached in this test 12

Copyright and Disclaimer 13
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 Live OneCare 2.5
- 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 already 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 this public report.

Tested Product Versions

The Malware sets, system sets and the products were updated and frozen on the 10th August 2009. The following 16 up-to-date products\(^1\) were included in this public test:

- avast! Professional Edition 4.8.1348
- AVG Anti-Virus 8.5.406
- AVIRA AntiVir Premium 9.0.0.446
- BitDefender Anti-Virus 13.0.13.254
- eScan Anti-Virus 10.0.997.491
- ESET NOD32 Antivirus 4.0.437.0
- F-Secure Anti-Virus 10.00.246
- G DATA AntiVirus 20.0.4.9
- Kaspersky Anti-Virus 9.0.0.463
- Kingsoft AntiVirus 2009.08.05.16
- McAfee VirusScan Plus 13.11.102
- Microsoft Live OneCare 2.5.2900.28
- Norman Antivirus & Anti-Spyware 7.10.02
- Sophos Anti-Virus 7.6.10
- Symantec Norton Anti-Virus 17.0.0.136
- Trustport Antivirus 2.8.0.3017

Some products may offer additional features e.g. to provide additional protection against malware during its execution (if not detected in advance on-access or on-demand).

Please try the products on your own system before making a purchase decision based on these tests. There are also some other program features and important factors (e.g. price, ease of use/management, compatibility, graphical user interface, language, HIPS / behaviour blocker functions, etc.) to consider.

Although extremely important, the detection rate of a product is only one aspect of a complete Anti-Virus product. AV-Comparatives will publish in the next months the results of its full product / dynamic test, as well as other test reports which cover different aspects/features of the products.

\(^1\) The August test allows the submission of RTM-versions if the (same) final version is going to be released before the report is published. Beta versions are not accepted.
Comments

As almost all products run nowadays in real life with highest protection settings by default or switch automatically to highest settings in case of a detected infection, we tested all products with highest settings (except Sophos and F-Secure).

Below are some notes about the used settings (scan of all files etc. is always enabled) and some technologies which need to be explained:

**AVG, BitDefender, eScan, ESET, Kingsoft, Microsoft, Norman:**
Runs with highest settings by default.

**avast:**
Runs (in case of an infection) by default automatically with highest settings.

**G DATA:**
Runs (depending from hardware) with highest settings by default.

**AVIRA, Kaspersky, Symantec, TrustPort:**
Asked to get tested with all extended categories enabled and with heuristic set to high/advanced. Due to that, we recommend users to consider also setting the heuristics to high/advanced, as those products do not use their highest settings by default.

**F-Secure, Sophos:**
Asked to get tested and awarded based on its default settings (without deep heuristic / suspicious detections). Due that, we suggest users to consider to also do not set the settings to high (except in case of an existing infection).

**McAfee:**
Uses an in-the-cloud technology (Artemis / Active Protection) which is enabled by default and working while an Internet connection is available. Artemis was tested at the same time as other products were updated so it did not have any time advantage over other products. For informational purposes, we noted also the results without the in-the-cloud technology (offline).
# Test Results

Below are the test results tables containing the detection rate details of the various products.

## Detection of virus/malware:

<table>
<thead>
<tr>
<th>Company</th>
<th>AVIRA Antivir Premium</th>
<th>Avast Software</th>
<th>AVG Anti-Virus</th>
<th>ESDags Defender</th>
<th>ESDags Defender AV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows viruses</td>
<td>22.79</td>
<td>23.608</td>
<td>22.377</td>
<td>22.700</td>
<td>22.451</td>
</tr>
<tr>
<td>Macro viruses</td>
<td>1.198</td>
<td>1.196</td>
<td>1.188</td>
<td>1.059</td>
<td>1.176</td>
</tr>
<tr>
<td>Script malware</td>
<td>4.466</td>
<td>4.410</td>
<td>4.402</td>
<td>2.003</td>
<td>4.243</td>
</tr>
<tr>
<td>Worms</td>
<td>95.681</td>
<td>95.350</td>
<td>94.764</td>
<td>92.016</td>
<td>94.266</td>
</tr>
<tr>
<td>Backdoor/Bots</td>
<td>323.723</td>
<td>322.389</td>
<td>317.211</td>
<td>309.579</td>
<td>316.584</td>
</tr>
<tr>
<td>Trojan</td>
<td>1094.082</td>
<td>1077.546</td>
<td>1062.424</td>
<td>1016.589</td>
<td>1050.672</td>
</tr>
<tr>
<td>Other malware</td>
<td>28.431</td>
<td>28.134</td>
<td>27.969</td>
<td>23.175</td>
<td>27.597</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>1,562,092</strong></td>
<td><strong>1,552,727</strong></td>
<td><strong>1,531,515</strong></td>
<td><strong>1,460,023</strong></td>
<td><strong>1,520,053</strong></td>
</tr>
</tbody>
</table>

## Detection of virus/malware:

<table>
<thead>
<tr>
<th>Company</th>
<th>MicroWorld eScan ISS</th>
<th>F-Secure Anti-Virus</th>
<th>G DATA Security</th>
<th>Kaspersky Labs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows viruses</td>
<td>23.79</td>
<td>23.466</td>
<td>23.460</td>
<td>22.776</td>
</tr>
<tr>
<td>Macro viruses</td>
<td>1.196</td>
<td>1.176</td>
<td>1.176</td>
<td>1.176</td>
</tr>
<tr>
<td>Worms</td>
<td>95.681</td>
<td>94.410</td>
<td>94.300</td>
<td>95.753</td>
</tr>
<tr>
<td>Backdoor/Bots</td>
<td>323.723</td>
<td>318.329</td>
<td>319.042</td>
<td>323.272</td>
</tr>
<tr>
<td>Trojan</td>
<td>1084.502</td>
<td>1057.669</td>
<td>1058.927</td>
<td>1082.163</td>
</tr>
<tr>
<td>Other malware</td>
<td>28.431</td>
<td>27.577</td>
<td>27.950</td>
<td>26.405</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>1,552,092</strong></td>
<td><strong>1,526,640</strong></td>
<td><strong>1,520,023</strong></td>
<td><strong>1,473,104</strong></td>
</tr>
</tbody>
</table>

## Detection of virus/malware:

<table>
<thead>
<tr>
<th>Company</th>
<th>Kingssoft Kingssoft AntiVirus</th>
<th>McAfee McAfee VirusScan+</th>
<th>Microsoft OneCare</th>
<th>ESET NOD32 Antivirus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows viruses</td>
<td>23.79</td>
<td>19.725</td>
<td>22.156</td>
<td>21.919</td>
</tr>
<tr>
<td>Macro viruses</td>
<td>1.196</td>
<td>8.7%</td>
<td>1.196</td>
<td>1.196</td>
</tr>
<tr>
<td>Script malware</td>
<td>4.465</td>
<td>29.0%</td>
<td>3.452</td>
<td>3.721</td>
</tr>
<tr>
<td>Worms</td>
<td>95.681</td>
<td>89.2%</td>
<td>94.322</td>
<td>91.190</td>
</tr>
<tr>
<td>Backdoor/Bots</td>
<td>323.723</td>
<td>90.2%</td>
<td>321.181</td>
<td>292.285</td>
</tr>
<tr>
<td>Trojan</td>
<td>1084.502</td>
<td>85.8%</td>
<td>1072.925</td>
<td>952.995</td>
</tr>
<tr>
<td>Other malware</td>
<td>28.431</td>
<td>71.2%</td>
<td>25.144</td>
<td>24.945</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>1,552,092</strong></td>
<td><strong>1,349,077</strong></td>
<td><strong>1,541,417</strong></td>
<td><strong>1,405,245</strong></td>
</tr>
</tbody>
</table>
The results of our on-demand tests are usually applicable also for the on-access scanner (if configured the same way), but not for on-execution protection technologies (like HIPS, behaviour blockers, etc.).

A good detection rate is still one of the most important, deterministic and reliable features of an antivirus product. Additionally, most products provide at least some kind of HIPS, behaviour-based or other functionalities to block (or at least warn about the possibility of) malicious actions e.g. during the execution of malware, when all other on-access and on-demand detection/protection mechanism failed.
Please do not miss the second part of the report (it will be published in a few months) containing the retrospective test, which evaluates how well products are at detecting new/unknown malware. Further test reports (cleaning test, performance test, PUA detection test, dynamic test, etc.) covering other aspects of the various products will be released soon on our website.

Even if we deliver various tests and show different aspects of Anti-Virus software, users are advised to evaluate the software by themselves and build their own opinion about them. Test data or reviews just provide guidance to some aspects that users cannot evaluate by themselves. We suggest and encourage readers to research also other independent test results provided by various well-known and established independent testing organizations, in order to get a better overview about the detection and protection capabilities of the various products over different test scenarios and various test-sets.

The awards on page 13 are given according to the table below:

<table>
<thead>
<tr>
<th>Detection Rates</th>
<th>&lt;87%</th>
<th>87 - 93%</th>
<th>93 - 97%</th>
<th>97 - 100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Few (0-15 FP’s)</td>
<td>tested</td>
<td>STANDARD</td>
<td>ADVANCED</td>
<td>ADVANCED+</td>
</tr>
<tr>
<td>Many (16-100 FP’s)</td>
<td>tested</td>
<td>tested</td>
<td>STANDARD</td>
<td>ADVANCED</td>
</tr>
</tbody>
</table>
Summary results

The test-set is split in two parts. The percentages below refer to SET B, which contains only malware from the last 7 months. SET A is usually covered very well (>97%) by all the tested products and contains malware from December 2007 to December 2008.

Please consider also the false alarm rates when looking at the below detection rates!

Total detection rates:\n
1. G DATA 99.8%
2. AVIRA 99.4%
3. McAfee\(^3\) 98.7%
4. Symantec 98.4%
5. Avast 98.0%
6. F-Secure 97.9%
7. Bitdefender 97.8%
8. eScan 97.7%
9. Trustport 97.6%
10. ESET 97.2%
11. Kaspersky 94.7%
12. AVG 94.0%
13. Sophos 91.3%
14. Microsoft 90.0%
15. Kingsoft 86.4%
16. Norman 84.8%

SET B contains nearly 1.6 million malware samples. The used malware test-set consists of:

\(^2\) We estimate the remaining error margin to be around 0.2%

\(^3\) McAfee VirusScan Plus 2009 and above comes with the "in-the-cloud" Artemis technology turned on by default. For corporate users or home users using older McAfee products without “Active Protection” - as well as all other users - it may be important to know what the baseline minimum detection rate of McAfee would be, should the Internet connection be not available. **The McAfee detection rate without Internet connection was 92.6%.**
False positive/alarm test

In order to better evaluate the quality of the detection capabilities of anti-virus products, we provide also a false alarm test. False alarms can sometimes cause as much troubles as a real infection. Please consider the false alarm rate when looking at the detection rates, as a product which is prone to cause false alarms achieves higher scores easier.

**False Positive Results**

Number of false alarms found in our full set of clean files (lower is better):

1. Bitdefender, eScan, F-Secure 4
2. Microsoft, Avast 5
3. AVG, Kaspersky 8 few FP’s
4. G DATA 9
5. ESET 12
6. Symantec 13
7. AVIRA 21
8. Sophos 26
9. McAfee\(^4\) 41 many FP’s
10. Trustport, Norman 42
11. Kingsoft 47

The graph below shows the number of false alarms found in our set of clean files by the tested Anti-Virus products.


\(^4\) McAfee without in-the-cloud had 26 false alarms.
Scanning Speed Test

Anti-Virus products have different scanning speeds due to various reasons. It has to be taken in account how reliable the detection rate of an Anti-Virus is; if the Anti-Virus product uses code emulation, if it is able to detect difficult polymorphic viruses, if it does a deep heuristic scan analysis and active rootkit scan, how deep and thorough the unpacking and unarchiving support is, additional security scans, etc.

Most products have technologies to decrease scan times on subsequent scans by skipping previously scanned files. As we want to know the scan speed (when files are really scanned for malware) and not the skipping files speed, those technologies are not taken into account here. In our opinion some products should inform the users more clearly about the performance-optimized scans and then let the users decide if they prefer a short performance-optimized scan (which does not re-check all files, with potential risk of overlooking infected files) or a full-security scan.

The following graph shows the throughput rate in MB/sec (higher is faster) of the various Anti-Virus products when scanning (on-demand) with highest settings our whole set of clean files (used for the false alarm testing). The scanning throughput rate will vary based on the set of clean files, the settings and the hardware used.

The average scanning throughput rate (scanning speed) is calculated by the size of the clean-set in MB's divided by the time needed to finish the scan in seconds. The scanning throughput rate of this test cannot be compared with future tests or with other tests, as it varies from the set of files, hardware used etc.

The scanning speed tests were done under Windows XP SP3, on identical Intel Core 2 Duo E8300/2.83GHz, 2GB RAM and SATA II disks.

5 to know how fast various products would be on your PC at scanning your files, we advise you to try the products yourself
Award levels reached in this test

AV-Comparatives provides a 3-level-ranking-system (STANDARD, ADVANCED and ADVANCED+). As this report contains also the raw detection rates and not only the awards, users that do not care about false alarms can rely on that score alone if they want to.

<table>
<thead>
<tr>
<th>AWARDS</th>
<th>PRODUCTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ADVANCED+</strong></td>
<td>G DATA</td>
</tr>
<tr>
<td></td>
<td>Symantec</td>
</tr>
<tr>
<td></td>
<td>Avast</td>
</tr>
<tr>
<td></td>
<td>F-Secure</td>
</tr>
<tr>
<td></td>
<td>BitDefender</td>
</tr>
<tr>
<td></td>
<td>eScan</td>
</tr>
<tr>
<td></td>
<td>ESET</td>
</tr>
<tr>
<td></td>
<td>AVIRA*</td>
</tr>
<tr>
<td></td>
<td>McAfee*</td>
</tr>
<tr>
<td></td>
<td>TrustPort*</td>
</tr>
<tr>
<td></td>
<td>Kaspersky</td>
</tr>
<tr>
<td></td>
<td>AVG</td>
</tr>
<tr>
<td><strong>ADVANCED</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft</td>
</tr>
<tr>
<td><strong>STANDARD</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sophos*</td>
</tr>
<tr>
<td></td>
<td>Kingsoft</td>
</tr>
<tr>
<td></td>
<td>Norman</td>
</tr>
</tbody>
</table>

*: those products got lower awards due false alarms

The Awards are not only based on detection rates - also False Positives found in our set of clean files are considered. A product that is successful at detecting a high percentage of malware but suffers from false alarms may not be necessarily better than a product which detects less malware but which generates less FP’s.

---

6 We suggest to consider products with same the award to be as good as the other products with same award.
Copyright and Disclaimer

This publication is Copyright © 2009 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. 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. (September 2009)