Content

1. Introduction 3
2. Description 3
3. Test results 4
4. Summary results 7
5. False positive/alarm test 7
6. Certification levels reached in this test 8
7. Copyright and Disclaimer 9
1. Introduction

This test report is the second part of the February 2009 test\(^1\). Many new viruses and other types of malware appear every day, this is why it’s important that Anti-Virus products not only provide new updates, as often and as fast as possible, in order to identify those new threats, but also that they are able to detect such threats in advance with generic and/or heuristic techniques. Even if nowadays most anti-virus products provide daily or hourly updates, without heuristic/generic methods there is always a time-frame where the user is not protected, and much more important than time to release an update, is the time it takes to get that update deployed. The products used the same updates and signatures they had the 9th February, and the same highest\(^2\) detection settings were used. This test shows the proactive detection capabilities that the products had at that time. We used new samples appeared and received between the 9th and 16th February 2009. The following 16 products were tested:

- avast! Professional Edition 4.8.1335
- AVG Anti-Virus 8.0.234
- AVIRA AntiVir Premium 8.2.0.374
- BitDefender Anti-Virus 12.0.11.4
- eScan Anti-Virus 10.0.946.341
- ESET NOD32 Antivirus 3.0.684.0
- F-Secure Anti-Virus 9.00.149
- G DATA AntiVirus 19.1.0.0
- Kaspersky Anti-Virus 8.0.0.506a
- Kingsoft AntiVirus 2008.11.6.63
- McAfee VirusScan Plus 13.3.117
- Microsoft Live OneCare 2.5.2900.20
- Norman Antivirus & Anti-Spyware 7.10.02
- Sophos Anti-Virus 7.6.4
- Symantec Norton Anti-Virus 16.2.0.7
- Trustport Antivirus 2.8.0.3011

2. Description

Anti-Virus products often claim to have high proactive detection capabilities – far higher than those reached in this test. This isn’t just a self-promotional statement; it’s possible that products reach the stated percentages, but this depends on the duration of the test-period, the size of the sample set and the used samples. The data shows how good the proactive detection capabilities of the scanners were in detecting actual new threats. Users shouldn’t be afraid if products have, in a retrospective test, low percentages. If the anti-virus software is always kept up-to-date, it will be able to detect more samples. For understanding how the detection rates of the Anti-Virus products look with updated signatures and programs, have a look at our regular on-demand detection tests. Only the on-demand detection capability was tested. Some products may be had the ability to detect some samples e.g. on-execution or by other monitoring tools, like behaviour-blocker, etc. Those kinds of additional protection technologies are evaluated with dynamic tests by AV-Comparatives and will be published later this year.

---


\(^2\) except Sophos Anti-Virus; see comments in the February 2009 test report
### 3. Test results

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
<th>Program version</th>
<th>Engine signature version</th>
<th>Certification level reached</th>
<th>Number of false positives</th>
<th>Proactive detection of &quot;NEW&quot; samples</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>many</td>
<td>many</td>
</tr>
<tr>
<td>AVG AntiVirus</td>
<td>ProPlus</td>
<td>5.2.0.374</td>
<td>02.03.2009</td>
<td>ADVANCED</td>
<td>188</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>many</td>
<td>many</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>many</td>
<td>many</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>many</td>
<td>many</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>many</td>
<td>many</td>
</tr>
</tbody>
</table>

#### Windows viruses
- AVG AntiVirus: 66%
- F-Secure: 83%
- McAfee: 83%
- Microsoft: 83%
- ESET: 83%
- McAfee Antivirus: 83%
- Microsoft: 83%
- ESET HU32 Antivirus: 83%

#### Viruses
- AVG AntiVirus: 36%
- F-Secure: 36%
- McAfee: 36%
- Microsoft: 36%
- ESET: 36%
- McAfee Antivirus: 36%
- Microsoft: 36%
- ESET HU32 Antivirus: 36%

#### Backdoor
- AVG AntiVirus: 26%
- F-Secure: 26%
- McAfee: 26%
- Microsoft: 26%
- ESET: 26%
- McAfee Antivirus: 26%
- Microsoft: 26%
- ESET HU32 Antivirus: 26%

#### Trojan
- AVG AntiVirus: 13%
- F-Secure: 13%
- McAfee: 13%
- Microsoft: 13%
- ESET: 13%
- McAfee Antivirus: 13%
- Microsoft: 13%
- ESET HU32 Antivirus: 13%

#### Other malware (incl. script/macro)
- AVG AntiVirus: 40%
- F-Secure: 40%
- McAfee: 40%
- Microsoft: 40%
- ESET: 40%
- McAfee Antivirus: 40%
- Microsoft: 40%
- ESET HU32 Antivirus: 40%

#### TOTAL
- AVG AntiVirus: 114.92%
- F-Secure: 114.92%
- McAfee: 114.92%
- Microsoft: 114.92%
- ESET: 114.92%
- McAfee Antivirus: 114.92%
- Microsoft: 114.92%
- ESET HU32 Antivirus: 114.92%

---

**AV Comparatives**

- [www.av-comparatives.org](http://www.av-comparatives.org)
The below table shows the proactive on-demand detection capabilities of the various products, sorted by detection rate. The given awards (see page 8 of this report) are based not only on the detection rates over the new malware, but also considering the false alarm rates.

In this retrospective test any „in-the-cloud“ technologies that were implemented in the products under test were, of course, disabled. The retrospective test is performed using passive scanning and demonstrates the ability of the products under test to detect new malware proactively, without being executed. Even if “in-the-cloud” technologies provide very fast updates, they are still using an essentially reactive detection method based on signature detection.

If a malicious program is already detected “in-the-cloud” (that is, it’s already in the database), it isn’t unknown/”new” malware. To leave “in-the-cloud” signature detection enabled would be unfair to other products under test that are being prevented from receiving signature updates.

Nowadays, hardly any Anti-Virus products rely purely on “simple” signatures anymore. They all use complex generic signatures and heuristics etc. in order to catch new malware, without needing to download signatures or initiate manual analysis of new threats.

As it can be seen above, most products are already able to detect much completely new/unknown malware proactively. Such products can do this even without executing the malware, using passive heuristics, while other protective mechanisms like HIPS, behavior analysis and behavior-blockers, etc. add an extra layer of protection.
In addition, Anti-Virus vendors continue to deliver signatures and updates to fill the gaps where proactive mechanisms initially fail to detect some threats. Anti-Virus software uses various technologies to protect a PC. The combination of such multi-layered protection usually provides fairly good protection. Anti-Virus products are not dying; they have evolved as the threat landscape has changed and will continue to evolve and adapt, incorporating new defensive techniques. In our opinion, security products which rely on a single protection layer will not work effectively in the long term except by:

- requiring the user to take “difficult” decisions where automated software cannot determine whether software is or is not malicious

  or

- requiring the user to accept that a high volume of false positives is an acceptable trade-off against a low volume of false negatives (failed detections).
4. Summary results

The results show the proactive on-demand detection capabilities of the scan engines. The percentages are rounded to the nearest whole number. Do not take the results as an absolute assessment of quality - they just give an idea of who detected more, and who less, in this specific test. To know how these anti-virus products perform with updated signatures, please have a look at our on-demand tests of February and August. Readers should take a look at the results and build an opinion based on their needs. All the tested products are already selected from a group of very good scanners and if used correctly and kept up-to-date, users can feel safe with any of them. Please also have a look on the methodology document on our website for further details. Due the broad variety and high amount of malware appearing already within one week, we think that using this time only a one-week period reflects good the overall proactive/generic/heuristic detection capabilities against new malware of the various Anti-Virus products.

Below you can see the proactive on-demand detection results over new malware appeared within one week without signature updates:

ProActive detection of new malware:
1. AVIRA 69%
2. Microsoft, G DATA 60%
3. ESET NOD32 56%
4. BitDefender, Kaspersky, eScan 50%
5. AVG 45%
6. TrustPort, Avast 42%
7. Sophos 37%
8. Symantec 35%
9. McAfee 25%
10. Norman 23%
11. Kingsoft 19%
12. F-Secure 14%

5. False positive/alarm test

To better evaluate the quality of the detection capabilities, the false alarm rate has to be taken into account too. A false alarm (or false positive) is when an Anti-Virus product flags an innocent file to be infected when it is not. False alarms can sometimes cause as much troubles like a real infection. We included a false alarm test already in the test report Nr. 21. For details, please read the report available at http://www.av-comparatives.org/images/stories/test/ondret/avc_report21.pdf

| Very few false alarms (0-2): | Microsoft |
| Few false alarms (3-15): | Sophos, Symantec, F-Secure, ESET, McAfee, Kaspersky |
| Many false alarms (over 15): | AVG, eScan, Norman, AVIRA, BitDefender, TrustPort, Avast, G DATA, Kingsoft |

3 this test is performed on-demand – it is NOT an on-execution/behavioral test.
4 some products, like e.g. BitDefender, may had over 15 FP’s also due the fact that they support some few additional file/installer formats.
6. Certification levels reached in this test

We provide a 3-level-ranking-system (STANDARD, ADVANCED and ADVANCED+). Overviews of levels reached in previous main tests can be found on our website5.

The following certification levels are for the results reached in the retrospective test:

<table>
<thead>
<tr>
<th>CERTIFICATION LEVELS</th>
<th>PRODUCTS</th>
</tr>
</thead>
</table>
| ![AV comparatives](MAY_09) ADVANCED+ | Microsoft  
ESET NOD32  
Kaspersky |
| ![AV comparatives](MAY_09) ADVANCED | AVIRA*  
G DATA*  
BitDefender*  
eScan*  
Sophos  
Symantec  
McAfee |
| ![AV comparatives](MAY_09) STANDARD | AVG*  
TrustPort*  
Avast*  
F-Secure |
| ![AV comparatives](MAY_09) TESTED | Norman*  
Kingsoft* |

*: Products with “many” false alarms were penalized according to the below award system:

<table>
<thead>
<tr>
<th>Proactive Detection Rates</th>
<th>0-10%</th>
<th>10-25%</th>
<th>25-50%</th>
<th>50-100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>None - Few FP</td>
<td>tested</td>
<td>STANDARD</td>
<td>ADVANCED</td>
<td>ADVANCED+</td>
</tr>
<tr>
<td>Many FP</td>
<td>tested</td>
<td>tested</td>
<td>STANDARD</td>
<td>ADVANCED</td>
</tr>
</tbody>
</table>

5 http://www.av-comparatives.org/comparativesreviews/main-tests/summary-reports
7. 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 no representative of AV-Comparatives e.V. can he held liable for the accuracy of the test results. 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 an Austrian Non-Profit Organization.

AV-Comparatives e.V. (May 2009)