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

Language: English
February 2009
Last Revision: 2009-03-21

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 7
Graph of missed samples 9
Summary results 10
False positive/alarm test 11
Scanning speed test 23
Award levels reached in this test 24
Copyright and Disclaimer 25
Tested Products

- avast! Professional Edition 4.8
- AVG Anti-Virus 8.0
- AVIRA AntiVir Premium 8.2
- BitDefender Anti-Virus 2009
- Command Anti-Malware 5.0.8
- eScan Anti-Virus 10.0
- ESET NOD32 Antivirus 3.0
- F-Secure Anti-Virus 2009
- G DATA AntiVirus 2009
- Kaspersky Anti-Virus 2009
- Kingsoft AntiVirus 2009
- McAfee VirusScan Plus 2009
- Microsoft Live OneCare 2.5
- Norman Antivirus & Anti-Spyware 7.10
- Sophos Anti-Virus 7.6.4
- Symantec Norton Anti-Virus 2009
- Trustport Antivirus 2.8
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 limited to 16-18 well-known and worldwide used quality anti-virus products with high detection rates, which vendors agreed to get tested and included in this public report.

Only vendors which detected more than 97% of the Test-Set A (April 06 to April 08) have been included in this comparative. New included and qualified participants are Authentium and Kingsoft.

Tested Product Versions

The Malware sets and system Test-beds were frozen at the beginning of February 2009. All products were updated on the 9th February 2009.

The following 17 products were included in this public test:

• 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
• Command Anti-Malware 5.0.8
• 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

Some products may offer additional options/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, update frequency, 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 provide this year also a full product (proactive and normal) dynamic test report, as well as other test reports which cover different aspects/features of the products.
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). Below are some notes about the used settings (scan of all files etc. is always enabled) and some technologies which need to be explained:

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

**AVG:** runs with highest settings by default.

**AVIRA:** runs with medium heuristic by default and not all extended categories enabled. AVIRA asked already last year to get tested with all extended categories enabled and with heuristic set to high. Due to that, we recommend users to consider also setting the heuristics to high.

**BitDefender:** runs with highest settings by default.

**Command:** runs with high heuristic by default (which is also the recommended highest setting according to Authentium). Command has also maximum heuristic mode, but it is not recommended to enable it (due to too many false alarms).

**eScan:** runs with highest settings by default.

**ESET:** runs with highest settings (webfilter) by default.

**F-Secure:** runs with highest on-demand scan settings by default.

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

**Kaspersky:** runs with low heuristic setting by default. Kaspersky asked already last year to get tested with heuristics set to high. Due to that, we recommend users to consider also setting the heuristics to high.

**Kingsoft:** runs with highest settings by default.

**McAfee:** In McAfee’s Consumer product Artemis Technology is called Active Protection and it is enabled by default and only if an Internet connection is available. The Internet is the most prevalent infection vector so the test results with an Internet connection represent the capabilities to detect incoming malware more realistically. Artemis was tested at the same time as other products were updated so it did not have any time advantage over other products. The Artemis Technology sends out short fingerprints of suspicious files without any Personally Identifiable Information. Artemis currently provides almost instantaneous protection in addition to McAfee’s DAT updates for the most prevalent malware. McAfee updates how Artemis detects malware via its DAT signatures.
Microsoft: runs with highest settings by default.

Norman: runs with highest settings by default.

Sophos: runs without suspicious detection by default. Sophos (a product for enterprises) asked already months ago to get this year tested and awarded based on its default settings. For informational purposes, we noted also the results with highest settings (suspicious detection enabled etc.).

Symantec: runs with automatic heuristic by default. Symantec asked already last year to get tested with heuristic set to advanced, although it made practically no difference. Anyway, we recommend users to consider also setting the heuristic to advanced.

TrustPort: asked already last year to get tested with highest settings with two enabled engines (AVG and Norman), like used while scanning in the background (on-access).
Test Results

In this test we were more selective than during previous tests - only vendors which detected more than 97% of the Test-Set A (April 06 to April 08) have been included in this comparative.

Getting high awards is now harder, because now the Awards are based on the detection rates over Set-B only, which contains malware from the last nine months (May 08 to the beginning of February 09). In this case the detection rates (percentages) may look lower than during previous tests, where we counted the overall rating based on both Set A and Set B (where Set A is well covered by almost all vendors). Furthermore, False Alarms starting from this test will lower Award levels. Lower awards do not mean that the products are getting worse – in fact they all improved a lot, here an example: in this test Kingsoft has 85% (based on SET B only). If it were counted as in previous years (SET A + SET B), Kingsoft would have had about 92%.

Tables of Results

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
<th>AVIRA AntiVirus Premium</th>
<th>Avast! Software Anti-Virus Professional</th>
<th>AVG Technologies AVG Anti-Virus</th>
<th>BitDefender BitDefender AV</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>6.2.0.374</td>
<td>4.8.1325</td>
<td>8.1.220</td>
<td>12.0.11.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>02.00.767.01.01.248</td>
<td>09208.0</td>
<td>270.10.159.941</td>
<td></td>
</tr>
<tr>
<td>Award reached in this test</td>
<td>ADVANCED</td>
<td>ADVANCED</td>
<td>STANDARD</td>
<td>ADVANCED</td>
<td></td>
</tr>
<tr>
<td>Number of false positives</td>
<td>many</td>
<td>many</td>
<td>many</td>
<td>many</td>
<td></td>
</tr>
<tr>
<td>On-demand scanning speed</td>
<td>average</td>
<td>fast</td>
<td>slow</td>
<td>slow</td>
<td></td>
</tr>
<tr>
<td>DETECTION RATES:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SET A (April - April08)</td>
<td>1.220.238</td>
<td>PASSED</td>
<td>PASSED</td>
<td>PASSED</td>
<td>PASSED</td>
</tr>
<tr>
<td>SET B (May06-Jan09)</td>
<td>1.270.065</td>
<td>97.2%</td>
<td>1.232.110</td>
<td>92.2%</td>
<td>1.100.160</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company</th>
<th>Product</th>
<th>Avira AVSS Command AM</th>
<th>Microsoft eScan ISS</th>
<th>F-Secure F-Secure AntiVirus</th>
<th>G DATA Security G DATA AntiVirus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1.220.238</td>
<td>10.0.948.341</td>
<td>19.1.0.0</td>
<td>15.371.0</td>
</tr>
<tr>
<td>Award reached in this test</td>
<td>TESTED</td>
<td>ADVANCED</td>
<td>ADVANCED</td>
<td>ADVANCED</td>
<td></td>
</tr>
<tr>
<td>Number of false positives</td>
<td>many</td>
<td>many</td>
<td>few</td>
<td>many</td>
<td></td>
</tr>
<tr>
<td>On-demand scanning speed</td>
<td>average</td>
<td>slow</td>
<td>slow</td>
<td>average</td>
<td></td>
</tr>
<tr>
<td>DETECTION RATES:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SET A (April - April08)</td>
<td>1.220.238</td>
<td>PASSED</td>
<td>PASSED</td>
<td>PASSED</td>
<td>PASSED</td>
</tr>
<tr>
<td>SET B (May06-Jan09)</td>
<td>1.270.065</td>
<td>97.1%</td>
<td>1.245.527</td>
<td>96.0%</td>
<td>1.130.730</td>
</tr>
</tbody>
</table>
### Data Analysis

#### Anti-Virus Comparative - No. 21 – February 2009

<table>
<thead>
<tr>
<th>Company</th>
<th>Kaspersky Labs</th>
<th>Kaspersoft</th>
<th>McAfee</th>
<th>Microsoft OneCare</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>Kaspersky AV</td>
<td>Kaspersoft AntiVirus</td>
<td>McAfee VirusScan+</td>
<td>Microsoft OneCare</td>
</tr>
<tr>
<td>Program version</td>
<td>8.0.0.5396</td>
<td>2008.11.83</td>
<td>13.3.117</td>
<td>2.5.2000.20</td>
</tr>
<tr>
<td>Engine / signature version</td>
<td>N4</td>
<td>2.8.1</td>
<td>5300.2777.16521</td>
<td>1.51.391.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Award reached in this test</th>
<th>ADVANCED+</th>
<th>TESTED</th>
<th>ADVANCED+</th>
<th>STANDARD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of false positives</td>
<td>few</td>
<td>many</td>
<td>few</td>
<td>very few</td>
</tr>
<tr>
<td>On-demand scanning speed</td>
<td>average</td>
<td>fast</td>
<td>average</td>
<td>average</td>
</tr>
</tbody>
</table>

#### DETECTION RATES:

**SET A (Apr’06 - Apr’09):**

<table>
<thead>
<tr>
<th></th>
<th>1,290,239</th>
<th>PASSED</th>
<th>PASSED</th>
<th>PASSED</th>
<th>PASSED</th>
</tr>
</thead>
</table>

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

**SET B (May’06 - Jun’09):**

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

**TOTAL:** 1,274,528 1,238,060 97.1% 1,002,656 84.9% 1,263,208 99.1% 1,110,456 67.1%

---

<table>
<thead>
<tr>
<th>Company</th>
<th>ESET</th>
<th>Norman ASA</th>
<th>Synantec</th>
<th>Sophos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>NOD32 Antivirus</td>
<td>Norman AV-AS</td>
<td>Norton Anti-Virus</td>
<td>Sophos Anti-Virus</td>
</tr>
<tr>
<td>Program version</td>
<td>3.0.694.0</td>
<td>7.1.0.02</td>
<td>15.2.0.7</td>
<td>7.6.4</td>
</tr>
<tr>
<td>Engine / signature version</td>
<td>3839.1160</td>
<td>6.0.0.06</td>
<td>110208f.79468</td>
<td>2.833.14.386-180</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Award reached in this test</th>
<th>ADVANCED+</th>
<th>TESTED</th>
<th>ADVANCED+</th>
<th>STANDARD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of false positives</td>
<td>few</td>
<td>many</td>
<td>few</td>
<td>few</td>
</tr>
<tr>
<td>On-demand scanning speed</td>
<td>average</td>
<td>slow</td>
<td>average</td>
<td>slow</td>
</tr>
</tbody>
</table>

#### DETECTION RATES:

**SET A (Apr’06 - Apr’09):**

<table>
<thead>
<tr>
<th></th>
<th>1,290,239</th>
<th>PASSED</th>
<th>PASSED</th>
<th>PASSED</th>
<th>PASSED</th>
</tr>
</thead>
</table>

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

**SET B (May’06 - Jun’09):**

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

**TOTAL:** 1,274,528 1,244,754 97.0% 1,113,469 87.0% 1,256,448 96.7% 1,142,707 89.0%

---

<table>
<thead>
<tr>
<th>Company</th>
<th>TrustPort</th>
<th>TrustPort AV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td></td>
<td>2.9.0.3011</td>
</tr>
<tr>
<td>Program version</td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Award reached in this test</th>
<th>ADVANCED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of false positives</td>
<td>many</td>
</tr>
<tr>
<td>On-demand scanning speed</td>
<td>slow</td>
</tr>
</tbody>
</table>

#### DETECTION RATES:

**SET A (Apr’06 - Apr’09):**

<table>
<thead>
<tr>
<th></th>
<th>1,290,239</th>
<th>PASSED</th>
</tr>
</thead>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

**SET B (May’06 - Jun’09):**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>

**TOTAL:** 1,274,328 1,237,704 97.1%
Graph of missed samples (lower is better)

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 covering other aspects of the various products will be released from time to time during the year on our website.

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. Those special protection features will be evaluated by us later this year.

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 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.
Summary results

The test-set has been split in two parts. The percentages below refer to SET B, which contains only malware from the last 9 months. As a result, percentages may look lower than in previous tests. SET A is covered very well (>97%) by all the tested products and contains malware from April 2006 to April 2008. Please consider also the false alarm rates (listed on next page) when looking at the below detection rates!

Total detection rates¹:

<table>
<thead>
<tr>
<th>Product</th>
<th>Detection Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. G DATA</td>
<td>99.8%</td>
</tr>
<tr>
<td>2. AVIRA</td>
<td>99.7%</td>
</tr>
<tr>
<td>3. McAfee²</td>
<td>99.1%</td>
</tr>
<tr>
<td>4. Symantec</td>
<td>98.7%</td>
</tr>
<tr>
<td>5. Avast</td>
<td>98.2%</td>
</tr>
<tr>
<td>6. BitDefender, eScan</td>
<td>98.0%</td>
</tr>
<tr>
<td>7. ESET</td>
<td>97.6%</td>
</tr>
<tr>
<td>8. Kaspersky, TrustPort</td>
<td>97.1%</td>
</tr>
<tr>
<td>9. F-Secure</td>
<td>93.4%</td>
</tr>
<tr>
<td>10. AVG</td>
<td>93.0%</td>
</tr>
<tr>
<td>11. Sophos</td>
<td>89.6%</td>
</tr>
<tr>
<td>12. Command</td>
<td>88.9%</td>
</tr>
<tr>
<td>13. Norman</td>
<td>87.8%</td>
</tr>
<tr>
<td>14. Microsoft</td>
<td>87.1%</td>
</tr>
<tr>
<td>15. Kingsoft</td>
<td>84.9%</td>
</tr>
</tbody>
</table>

SET B contains nearly 1.3 million malware samples. The used malware test-set consists of:

![Pie chart showing malware distribution](image)

¹ We estimate the remaining error margin for those detection rates to be around 0.4%
² McAfee VirusScan Plus 13.3 comes with the "in-the-cloud" Artemis technology turned on by default. For some users it may be important to know what the baseline minimum detection rate of McAfee would be, should the Internet connection be not available. So we measured also the detection rate of McAfee with no Internet connection. The McAfee detection rate without Internet connection was 95.2%.
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. Microsoft 2 very few FP’s
2. Sophos 5
3. Symantec, F-Secure 7 few FP’s
4. ESET, McAfee 13
5. Kaspersky 14
6. AVG, eScan 17
7. Norman 23
8. AVIRA 24
9. BitDefender 25
10. Trustport 27 many FP’s
11. Avast 28
12. G DATA 44
13. Authentium 55
14. Kingsoft 66

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

With AV testing it is important to measure not only detection capabilities but also reliability - one of reliability aspects is certainly product's tendency to flag clean files as infected. No product is immune from false positives (FP's) but there are differences among them and the goal is to measure them. Nobody has all legitimate files that exist and so no "ultimate" test of FP's can be done. What can be done and is reasonable, is to create and use a set of clean files which is independent. If on such set one product has e.g. 100 FP's and another only 50, it is likely that the first product is more prone to FP's than the other. It doesn't mean the product with 50 FP's doesn't have more than 50 FP's globally, but important is the relative number.

All listed false alarms were reported and sent to the Anti-Virus vendors for verification and are now already fixed. False alarms caused by unencrypted data blocks in Anti-Virus related files were not counted. If a product had several false alarms belonging to the same software, it is counted here as only one false alarm (that's why we label all software in general as “package”). Cracks, keygens, etc. or other questionable applications and tools, as well as FP's distributed by vendors or other non independent sources are not counted here as False Positives.

Below you will find the false alarms we observed in our independent set of clean files. In future we may provide this list as a separate document and not include it in the test report.

Microsoft

False alarm found in some parts of	Detected as
BackProtection package	Trojan:Win32/Vhorse.EY
InkScapePortable package	VirTool:Win32/Obfuscator.C

Microsoft OneCare had 2 false alarms.

Sophos

False alarm found in some parts of	Detected as
eScan package	Istbar
PhotoMatix package	Mal/Generic-A
RegistryHealer package	Mal/HckPk-A
SpyCop package	Mal/VB-A
TorChat package	Mal/HckPk-E

Sophos had 5 false alarms with default settings. With enabled suspicious detection there were about 68 FP's; around 20000 additional malware samples would be detected with enabled “Suspicious” detections. As Sophos is a product for corporate users, which computers are managed by an administrator, the discovered FP's are not a big issue. These files are technically FP's, but the administrators most likely would like to know about the presence of those applications.
Symantec

**False alarm found in some parts of**
- 0190warner package
- Burn4Free package
- CLO8 package
- CSFireMonitor package
- NiriCmd package
- OpenOffice package
- RegCool package

**Detected as**
- Suspicious.MH690
- SecurityRisk.NavHelper
- Trojan Horse
- Downloader
- Backdoor.Trojan
- Suspicious.MH690
- Backdoor.Bifrose

Symantec Norton Anti-Virus had 7 false alarms.

F-Secure

**False alarm found in some parts of**
- CSFireMonitor package
- eScan package
- GoogleTool package
- Lektora package
- NetMeter package
- Photomatix package
- SweetDream package

**Detected as**
- Trojan-Downloader.Win32.Small.afxn
- Trojan.Win32.Genome.erg
- SMS-Flooder.Win32.Delf.l
- Email-Worm.Win32.Skybag.c
- Backdoor.Win32.Delf.kxp
- Net-Worm.Win32.Kolabc.dtf
- Trojan.Win32.Agent.bkjm

F-Secure had 7 false alarms.

ESET

**False alarm found in some parts of**
- 6-Zip package
- BattlestationsMidway package
- dotWidglet package
- F1Challenge package
- FineReaderPro package
- InkScapePortable package
- IZArc package
- JkDefrag package
- KnightsOfHonor package
- Musketeers package
- PunkWar package
- T-Online package
- WinDVD package

**Detected as**
- Win32/Agent
- Win32/Statik
- Win32/Statik
- Win32/Genetik
- Win32/Statik
- Win32/Statik
- Win32/Statik
- Win32/Statik
- Win32/Statik
- NewHeur_PE
- Win32/Genetik

ESET NOD32 had 13 false alarms.

McAfee

**False alarm found in some parts of**
- 6-Zip package
- AutoStartAdmin package

**Detected as**
- Generic.dx
- Generic!Artemis
CDDVDBurner package
FileFolderUnlocker package
GoogleDesktop package
GoogleTool package
MultiInstall package
Noctramic package
RegRun package
RootkitUnhooker package
Soldner package
TaskManager package
XPTweaker package

McAfee with Artemis had 13 false alarms.

Kaspersky

False alarm found in some parts of
CleanCenter package
CSFireMonitor package
Downutube package
DVDIdentifier package
eScan package
GoogleTool package
Lektora package
NetMeter package
PAR package
Photomatix package
PicSize package
SweetDream package
WinMerge package
WinPlosion package

Detected as
Backdoor.Win32.5dBot.it
Trojan-Downloader.Win32.SdBot.itt
Trojan-Downloader.Win32.Small.afxn
Trojan.Win32.Generic
Trojan.Win32.Generic
SMS-Flooder.Win32.Delf.l
Email-Worm.Win32.Delf.kxp
Trojan-Dropper.Script.Generic
Net-Worm.Win32.Kolabc.dtf
Trojan-Dropper.Script.Generic
Trojan.Win32.Agent.bkjm
Email-Worm.Script.Generic
Trojan.Win32.Hooker.t

Kaspersky had 14 false alarms.

AVG

False alarm found in some parts of
AVIRA package
BattleMaps package
BlackMirror package
BlazeMediapro package
CDDVDBurner package
CreateMovie package
Cubes package
FreeMSNWrapper package
HotLaunch package
InkScapePortable package
Linkman package
PCodeGuard package
SmartMorph package
Soldner package

Detected as
Generic11.BJHA
Win32/Heur
Downloader.Swizzor
Generic12.BLDZ
Generic10.VAH
BackDoor.Hupigon4.AEWM
Win32/Heur
Generic6.IYW
Generic12.BLDZ
Obfustat.NPF
SHeur.ERY
BackDoor.Generic10.LFG
Generic12.BLDZ
PSW.Generic6.FR
Sophos package
StartKiller package
SummerBound package

AVG had 17 false alarms.

eScan

False alarm found in some parts of
ApplicationAccessServer package
BitTorrent package
CDDVDBurner package
CFOS package
CityGuide package
cLO8 package
GoogleTool package
HPRestore package
InkScapePortable package
LogMeIn package
MediaConverter package
PCSecurityTest package
PowerTools package
Putty package
SmartNIC package
Word2Web package
Zattoo package

Detected as
Trojan.Spy.Sigatar.5041.B
Trojan.Generic.376185
Trojan.Generic.97211
Trojan.Heur.GM.0440616120
Trojan.AgentMB.Delf.HZGAB0939497
Trojan.Generic.430620
Trojan.Generic.1267563
BAT.KILIAV.Gen
Trojan.Generic.103962
Virtool.903
Backdoor.Generic.148978
Trojan.Generic.1397003
Macro.VBA
Worm.Generic.15375
Trojan.Downloader.JLPF
Macro.VBA
Trojan.Generic.1372495

eScan had 17 false alarms.

Norman

False alarm found in some parts of
AudioVideo2Exe package
Azureus package
BookmarkBuddy package
dBPower package
Firefox package
GPSphoto package
IconHider package
Insaniquarium package
JSplit package
Kazaa package
MaulwurfsMover package
Nero package
NirCmd package
PocketChess package
RadLight package
PDPSoftware package
RivaTuner package
StreamRipper package
TaskManager package

Detected as
W32/Packed_Upack.A
dL0ader.LOXQ
Ircbot.YJP
W32/Malware.ERCK
HTML/Iframe.gen.A
W32/Joiner.BRV.dropper
W32/Webmoner.ABJ
W32/Smalltroj.IBLY
W32/Crypto
W32/Packed_PeX.B
Suspicious_F.gen
W32/OnLineGames.HUPN
Smalldoor.CGNH
W32/Agent.GZWS.dropper
Malware.DNHL
Malware.FNSF
W32/Agent.IQHH
NetworkWorm.EMS
W32/LdPinch.SFX
TyperShark package  W32/Smalltroj.IBLY
Vitascene package  W32/EMailWorm.BES
XP-AS package      Antivirus2008.PU
Zuma package       W32/Smalltroj.IBLU

Norman had 23 false alarms.

**AVIRA**

**False alarm found in some parts of**
- 3DScreensaver package
- 6-Zip package
- AdKiller package
- BOM package
- CDSearch package
- ClipboardRecorder package
- CSFireMonitor package
- Dashboard package
- DrWeb package
- Edimax driver package
- Ekalkulator package
- EUprice package
- GoogleTool package
- HP scanner package
- InternetDownloadManager package
- iRejectTrash package
- LaunchExpress package
- MSi WLAN package
- NeighborsFromHell package
- Paraworld package
- PCDoorGuard package
- SmartProtector package
- StickSecurity package
- TrendMicro package

**Detected as**
- TR/Spy.8369026.A
- TR/Agent.239371.A
- HEUR/Malware
- HEUR/HTML.Malware
- HEUR/HTML.Malware
- HEUR/Malware
- Dr/Oldr.Small.Lafxn
- HEUR/Malware
- TR/QQShou.E0.1
- SPR/Hacktool.57344
- TR/Crypt.ULPM.Gen
- HEUR/Macro.Word95
- DR/Flood.Delf.L
- HEUR/Malware
- TR/Crypt.XPACK.Gen
- HEUR/Malware
- HEUR/Malware
- ADSPY/Agent.emg
- TR/Dropper.Gen
- TR/Downloader.Gen
- BDS/Beasty.A
- TR/Agent.593920.A
- HEUR/Malware
- TR/Hijacker.Gen

AVIRA had 24 false alarms.

**BitDefender**

**False alarm found in some parts of**
- ApplicationAccessServer package
- BitTorrent package
- Browster package
- CDVDBurner package
- CFOS package
- CityGuide package
- Clo8 package
- DiaShowPro package
- FotoWorks package
- GoogleTool package
- Haushaltsbuch package

**Detected as**
- Trojan.Spy.Sigatar.5041.B
- Trojan.Generic.376185
- Win32.ExplorerHijack
- Trojan.Generic.97211
- Trojan.Heur.GM.0440616120
- Trojan.AgentMB.Delf.HZGAB0939497
- Trojan.Generic.430620
- Packer.Morphine
- Packer.Morphine
- Trojan.Generic.1267563
- Generic.PWS.Games.4.4E81B454
Bitdefender had 25 false alarms.

**TrustPort**

**False alarm found in some parts of**
- Audio2Exe package
- AVIRA package
- Azureus package
- BookmarkBuddy package
- CDDVDBurner package
- CreateMovie package
- dBPower package
- Firefox package
- GPSphoto package
- IconHider package
- Insaniquarium package
- JSplit package
- Kazaa package
- MaulwurfsMover package
- NirCmd package
- PCDoorGuard package
- PocketChess package
- RadLight package
- RivaTuner package
- Soldner package
- Sophos package
- StreamRipper package
- TaskManager package
- TyperShark package
- Vitascene package
- XP-AS package
- Zuma package

**Detected as**
- W32/Packed_Upack.A
- Generic11.BJHA
- DLoader.LOXQ
- Ircbot.YJP
- Generic10.VAH
- BackDoor,Hupigon4.AEWMD
- W32/Malware.ERCK
- HTML/Iframe.gen.A
- W32/Joiner.BRV.dropper
- W32/Webmoner.AB3
- W32/Smalltroj.IBLY
- W32/Crypto
- W32/Packed_PeX.B
- Suspicious_F.gen
- Smalldoor.CGNH
- BackDoor.Generic10.LFG
- W32/Agent.GZWS.dropper
- Malware.DNHL
- W32/Agent.IOHH
- PSW.Generic6.FR
- Agent.AOUE
- NetworkWorm.EMS
- W32/LdPinch.SFX
- W32/Smalltroj.IBLY
- W32/EMailWorm.BES
- Antivirus2008.PU
- W32/Smalltroj.IBLU

TrustPort had 27 false alarms.
Avast

False alarm found in some parts of
3DScreensaver package
0190warner package
Burn4Free package
CDDVDBurner package
CheckMail package
CL08 package
CreateMovie package
CSFireMonitor package
CTManager package
Dirwat package
edVARdo package
ExelockExpress package
FolderPatrol package
FTFP4Pro package
GoogleTool package
iNetQuery package
iPodAccess package
LockFolderXP package
MDAddressbuch package
NetMeter package
Noctramic package
PDFExplorer package
PhotoMatrix package
SharpEye package
SKs package
StartpageSave package
Suse package
Winter package

Detected as
Win32:Trojan-gen {Other}
Win32:Rootkit-gen [Rtk]
Win32:Naveexcel-H [Tr]
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Delf-GJF [Tr]
Win32:Trojan-gen {Other}
Win32:Hgweb-B [Trj]
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:SkiMorph [Cryp]
Win32:Trojan-gen {Other}
Win32:Trojan-gen {Other}
Win32:Race-D [Expl]
Win32:Trojan-gen {Other}

Avast had 28 false alarms.

G DATA

False alarm found in some parts of
0190warner package
3DScreensaver package
ApplicationAccessServer package
BitTorrent package
Burn4Free package
CDDVDBurner package
CFOS package
CheckMail package
CityGuide package
CL08 package
CreateMovie package
CSFireMonitor package
CTManager package
Dirwat package

Detected as
Win32:Badya
Win32:Badya
Trojan.Spy.Sigatar.5041.B
Trojan.Generic.376185
Win32:Badya
Win32:Badya
Trojan.Heur.GM.0440616120
Win32:Badya
Trojan.AgentMB.Delf.HZGAB0939497
Trojan.Generic.430620
Win32:Badya
Win32:Badya
Win32:Badya
Win32:Badya
Win32:Badya
Win32:Daum.A
edVARdo package
ExelockExpress package
FolderPatrol package
FTP4Pro package
GoogleTool package
HPRestore package
iNetQuery package
iPodAccess package
LockFolderXP package
LogMeIn package
MDAddressbuch package
MediaConverter package
NetMeter package
Noctramic package
PCSecurityTest package
PDFExplorer package
PhotoMatix package
PowerTools package
Putty package
SharpEye package
SKS package
SmartNIC package
StartpageSave package
Suse package
Winter package
Word2Web package
Zattoo package

Win32:Badya
Win32:Badya
Win32:Badya
Win32:Badya
Win32:Badya
BAT.KillAV.Gen
Win32:Badya
Win32:Badya
Win32:Badya
Win32:Badya
Backdoor.Generic.148978
Win32:Trojan-gen {Other}
Win32:Badya
Win32:Trojan-gen {Other}
Macro.VBA
Worm.Generic.15375
Win32:SkiMorph [Cryp]
Win32:Trojan-gen {Other}
Trojan.Downloader.JLPF
Win32:Trojan-gen {Other}
ELF:Race-D [Expl]
Win32:Trojan-gen {Other}
Macro.VBA
Trojan.Generic.1372495

G DATA had 44 false alarms.

Command

False alarm found in some parts of
3DScreensaver package
320mph package
Air2Mp3 package
AnimateDesktop package
AVIRA package
Blitzkrieg package
Budgeter package
Burn4Free package
CD/DVD Burning package
ClonyXXL package
CookieCooker package
CPUZ package
DM package
DriveImage package
DriveIndexTool package
DvWeb package
Enfish package

Detected as
W32/Malware!b74
W32/Backdoor2.YMQ
W32/Banload.E.gen!Eldorado
W32/Heuristic-187!Eldorado
W32/Agent.K.gen!Eldorado
W32/IRCbot-based!Maximus
W32/Backdoor2.RWA
W32/Malware6e64
W32/Heuristic-210!Eldorado
W32/Heuristic-210!Eldorado
Security_Risk
W32/Downldr2.OYOA
W32/OnlineGames.F.gen!Eldorado
W32/Downloader!GSA
W32/Autoit.B
W32/Downloader.N.gen!Eldorado
W32/Threat-SysAdderSml!Eldorado
Command had 55 false alarms. Please note that Command is a new entry in our tests. We expect that in the next test the number of false alarms will be much lower.

**Kingsoft**

**False alarm found in some parts of**
- ACER driver package
- AlbumCoverArt package
- Animation package
- Astra package
- Autoruns package
- BaldursGate package

**Detected as**
- Win32.Troj.Monder.475648
- Win32.Troj.StartPage.a.1585049
- Win32.Hack.HacDef.1245184
- Win32.Troj.Chuzy.352256
- Win32.Hack.Kelebek.1120149
<table>
<thead>
<tr>
<th>Package Name</th>
<th>Malware Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCleaner</td>
<td>Win32.Troj.Selfish.1497584</td>
</tr>
<tr>
<td>ClonyXXL</td>
<td>Worm.Roron.136332</td>
</tr>
<tr>
<td>ColoringBook</td>
<td>Win32.Troj.Unknown.az.186112</td>
</tr>
<tr>
<td>CounterStrike</td>
<td>Worm.Roron.136332</td>
</tr>
<tr>
<td>CPUZ</td>
<td>Win32.TrojDownloader.Small.624231</td>
</tr>
<tr>
<td>Creative driver</td>
<td>Win32.Troj.Obfuscated.40960</td>
</tr>
<tr>
<td>DarkHorizons</td>
<td>Win32.Troj.Unknown.az.186112</td>
</tr>
<tr>
<td>eMule</td>
<td>Win32.Troj.Agent.3534076</td>
</tr>
<tr>
<td>FAR</td>
<td>Win32.Troj.Taris.1418369</td>
</tr>
<tr>
<td>Ffia</td>
<td>Win32.Hack.Beastdoor.1154875</td>
</tr>
<tr>
<td>Folder2ISO</td>
<td>Win32.TrojDownloader.Delf.us.3174400</td>
</tr>
<tr>
<td>Gothic2c</td>
<td>Win32.PSWTroj.Nilage.42496</td>
</tr>
<tr>
<td>Grep</td>
<td>Win32.Troj.VB.96768</td>
</tr>
<tr>
<td>HotSpotShield</td>
<td>Win32.Troj.Agent oe.1035231</td>
</tr>
<tr>
<td>HoverWheel</td>
<td>Win32.Hack.IRCBot.1444845</td>
</tr>
<tr>
<td>IceAge2</td>
<td>Win32.Hack.ThinPacker.T.a.378833</td>
</tr>
<tr>
<td>LoginControl</td>
<td>Win32.WinInstaller.Agent.508937</td>
</tr>
<tr>
<td>MapInfo</td>
<td>Win32.Troj.Varvar.292864</td>
</tr>
<tr>
<td>MapleXP</td>
<td>Win32.WinInstaller.Agent.842830</td>
</tr>
<tr>
<td>Medion driver</td>
<td>Win32.Troj.Hidrag.110592</td>
</tr>
<tr>
<td>MIRC</td>
<td>Win32.Troj.Plutor.1007616</td>
</tr>
<tr>
<td>MS Links</td>
<td>Win32.Troj.SysJunkT.hh</td>
</tr>
<tr>
<td>MS Office97</td>
<td>Win32.Troj.Undercover___5B.318976</td>
</tr>
<tr>
<td>MS Windows95</td>
<td>Worm.Ganda___3E514.70199</td>
</tr>
<tr>
<td>MS Windows95 SP1</td>
<td>Win32.Troj.Pres___13089A.66672</td>
</tr>
<tr>
<td>MS Windows98</td>
<td>Worm.Ganda___6A7DE.70199</td>
</tr>
<tr>
<td>MS Windows2000</td>
<td>Worm.Ridnu.4880</td>
</tr>
<tr>
<td>MS WindowsXP</td>
<td>Win32.Troj.Patched.14336</td>
</tr>
<tr>
<td>MS WindowsXP SP1</td>
<td>Worm.Polip.274432</td>
</tr>
<tr>
<td>MS WindowsXP SP2</td>
<td>Worm.Polip.388608</td>
</tr>
<tr>
<td>MS WindowsXP SP3</td>
<td>Worm.Wast___66F897.156550</td>
</tr>
<tr>
<td>MS WindowsME</td>
<td>Win32.Troj.Pres___CAA2FB.81920</td>
</tr>
<tr>
<td>NortonSystemWorks</td>
<td>Worm.Brontok.176911</td>
</tr>
<tr>
<td>PCW</td>
<td>2S.Agent.deg.4982</td>
</tr>
<tr>
<td>PEID</td>
<td>Win32.Troj.Sality.158720</td>
</tr>
<tr>
<td>Perl</td>
<td>VBS.DNAOrder.aa.35780</td>
</tr>
<tr>
<td>PowerStrip</td>
<td>Win32.Hack.Huigezi.1012719</td>
</tr>
<tr>
<td>ProcessExplorer</td>
<td>Win32.Troj.Stagol.192512</td>
</tr>
<tr>
<td>RegistryMonitor</td>
<td>Win32.Troj.Taris.98304</td>
</tr>
<tr>
<td>RegistryOptimierer</td>
<td>Worm.Beagle.102400</td>
</tr>
<tr>
<td>Resistance</td>
<td>Win32.Troj.JunkDLLao.147559</td>
</tr>
<tr>
<td>SataRaid</td>
<td>Win32.Troj.Virut.905216</td>
</tr>
<tr>
<td>Scanner</td>
<td>Win32.Troj.Sality.160256</td>
</tr>
<tr>
<td>ShellOut</td>
<td>Win32.Joke.MovingMouse.k.20480</td>
</tr>
<tr>
<td>SQLW</td>
<td>Win32.Troj.Tvido.1598976</td>
</tr>
<tr>
<td>SpaceShooter</td>
<td>Win32.Hack.Kelebek.1120149</td>
</tr>
<tr>
<td>SQL</td>
<td>Win32.Troj.Selfish.90166</td>
</tr>
</tbody>
</table>
TCPview package       Win32.PSWTroj.LdPinch.94208
WinRAR package        Win32.Troj.Selfish.1004712
WinRoll package       Win32.Troj.OnLineGames.of.15360
Zzzap package         Win32.IRC.Flood.n.2103523

Kingsoft had 66 false alarms, and some of them were on operating system files. Please note that
Kingsoft is a new entry in our tests. We expect that in the next test the number of false alarms will be
much lower.

Kingsoft is the first vendor from China, which is brave enough to face the challenge of
our international test. Before a product can take part in our public main tests, it first has to pass our
minimum requirements. Not many Chinese vendors are eligible to participate in our international
tests.

**Influence of false alarms on the awards**

Please note that - as we announced already last year - false alarms lead now to lower Awards in our
test. The labels for false alarms found in our set of clean files are unchanged, as well as the detection
rate ranges. The awards are given according to the table below:

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

By having fixed ranges (esp. for FP’s) it may be sometimes a bit hard for vendors to accept that they fall
down to the next award due to only a few more FP’s in our set of clean files. But in our opinion the
ranges are already quite generous (esp. considering that all vendors always get the false alarm samples
after the test and can fix them, while our clean set does not grow that much over time).

We will not change ranges just to make some vendors happy. We suggest vendors to continue improving
their products and they will then get higher Awards when according to our test results they deserve it.
Those new rules were announced already last year. Some vendors which would reach higher awards by
looking at detection rates only, may be a bit unhappy that those higher requirements for the awards
have now been implemented.
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.

Some 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\(^3\), the settings and the hardware used.

![Graph showing scanning speed test results](image)

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.

\(^3\) 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 (see page 10) and not only the awards, users that do not care about false alarms can rely on that score alone if they want to.

Getting high awards is now harder, because now the Awards are based on detection rates over Set B, which contains malware from the last nine months (May 08 to the beginning of February 09). In this case the detection rates (percentages) are lower than at the last tests, were we counted the overall rating based on Set A and Set B (where Set A is well covered by almost all vendors). Furthermore, False Alarms now reduce the Awards level.

<table>
<thead>
<tr>
<th>AWARDS (based on detection rates and false alarms)</th>
<th>PRODUCTS (in no specific order)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="AV comparatives FEB 09" /></td>
<td>✓ Symantec</td>
</tr>
<tr>
<td></td>
<td>✓ ESET</td>
</tr>
<tr>
<td></td>
<td>✓ Kaspersky</td>
</tr>
<tr>
<td></td>
<td>✓ McAfee*</td>
</tr>
<tr>
<td><img src="image2" alt="AV comparatives FEB 09" /></td>
<td>✓ G DATA*</td>
</tr>
<tr>
<td></td>
<td>✓ AVIRA*</td>
</tr>
<tr>
<td></td>
<td>✓ Avast*</td>
</tr>
<tr>
<td></td>
<td>✓ BitDefender*</td>
</tr>
<tr>
<td></td>
<td>✓ eScan*</td>
</tr>
<tr>
<td></td>
<td>✓ TrustPort*</td>
</tr>
<tr>
<td></td>
<td>✓ F-Secure</td>
</tr>
<tr>
<td><img src="image3" alt="AV comparatives FEB 09" /></td>
<td>✓ AVG*</td>
</tr>
<tr>
<td></td>
<td>✓ Sophos</td>
</tr>
<tr>
<td></td>
<td>✓ Microsoft</td>
</tr>
<tr>
<td><img src="image4" alt="AV comparatives FEB 09" /></td>
<td>✓ Authentium*</td>
</tr>
<tr>
<td></td>
<td>✓ Norman*</td>
</tr>
<tr>
<td></td>
<td>✓ Kingsoft</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.

---

4 We suggest to consider products with same the award to be as good as the other products with same award.

5 McAfee without Artemis would have earned ADVANCED, please see comments on pages 5 and 10.
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. (March 2009)