



## Anti-Virus Comparative No.20

Proactive/retrospective test  
(on-demand detection of virus/malware)

Date: November 2008 (2008-11)

Last revision: 29<sup>th</sup> November 2008

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

## **1. Introduction**

This test report is the second part of the August 2008 test<sup>1</sup>. 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 same products, with the same updates and signatures they had the 4<sup>th</sup> August, as well as the same highest detection settings were used for this test, which shows the proactive detection capabilities that the products had at that time. For this test we used all new and unique samples received between 4<sup>th</sup> and 31<sup>st</sup> August 2008, split in one and four weeks periods. The following 16 products were tested:

- ❖ avast! Professional Edition 4.8.1229
- ❖ AVG Anti-Virus 8.0.156
- ❖ AVIRA AntiVir Premium 8.1.0.362
- ❖ BitDefender Anti-Virus 11.0.17
- ❖ eScan Anti-Virus 9.0.824.217
- ❖ ESET NOD32 Antivirus 3.0.669.0
- ❖ F-Secure Anti-Virus 9.00.148
- ❖ G DATA AntiVirusKit (AVK) 19.0.0.49
- ❖ Kaspersky Anti-Virus 8.0.0.454
- ❖ McAfee VirusScan Plus 12.1.110 (5300)
- ❖ Microsoft Live OneCare 2.5.2900.03
- ❖ Norman Antivirus & Anti-Spyware 7.10
- ❖ Sophos Endpoint Protection 7.5.1
- ❖ Symantec Norton Anti-Virus 16.0.0.125
- ❖ Trustport<sup>2</sup> Antivirus 2.8.0.3006
- ❖ VBA32 Scanner for Windows 3.12.8.2

## **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 will be evaluated by AV-Comparatives with dynamic tests in 2009.

---

<sup>1</sup> <http://www.av-comparatives.org/seiten/ergebnisse/report19.pdf>

<sup>2</sup> TrustPort was tested with only two engines (AVG, Norman)

### 3. Test results

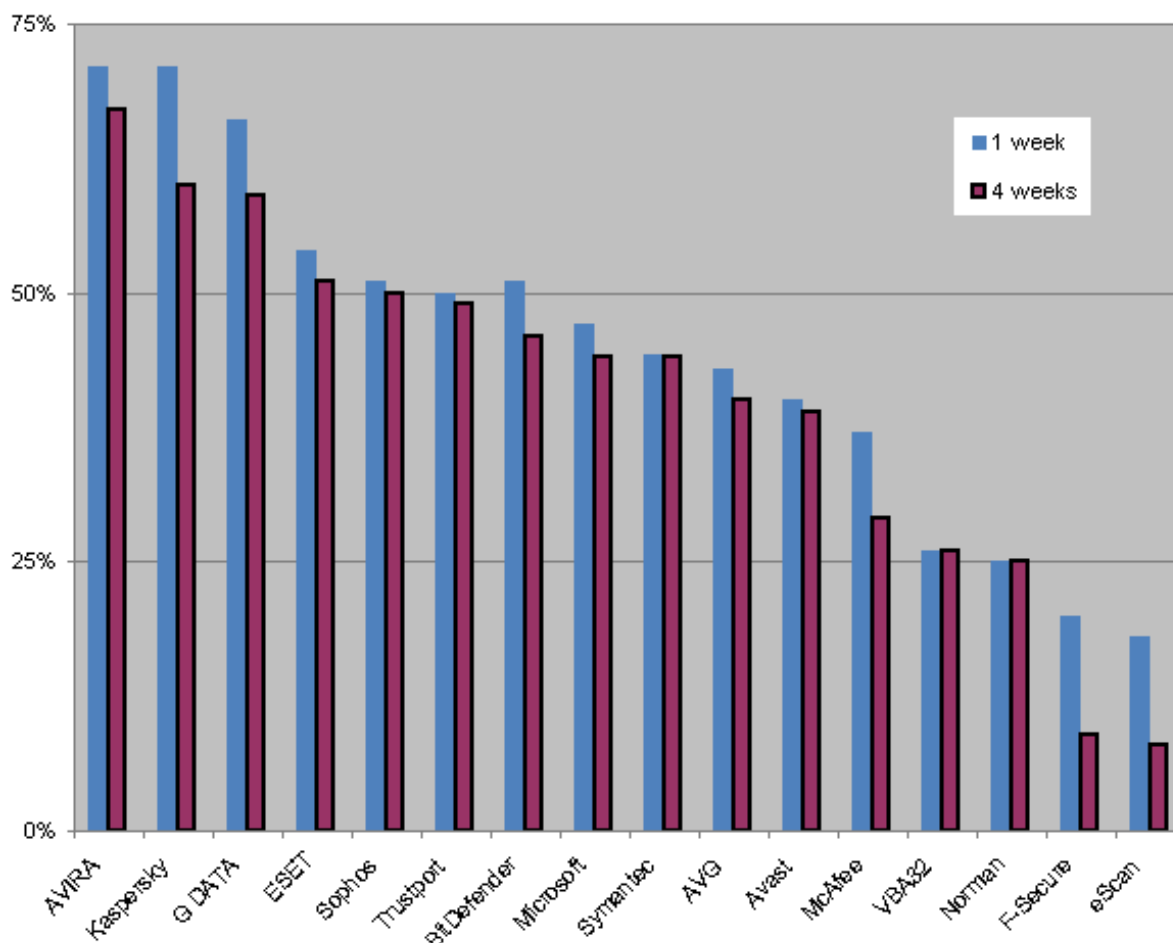
<i>Company</i>		AVIRA		G DATA Security		Alwil Software		AVG Technologies	
<i>Product</i>		<b>AntiVir Premium</b>		<b>AntiVirusKit (AVK)</b>		<b>avast! Professional</b>		<b>AVG Anti-Virus</b>	
<i>Program version</i>		8.1.0.362		19.0.0.49		4.8.1229		8.0.156	
<i>Engine / signature version</i>		8.01.01.15 / 7.00.05.212		N/A		080804-0		270.5.12/1590	
<i>Number of virus records</i>		1.533.821		unknown		unknown		unknown	
<b>Certification level reached</b>		<b>ADVANCED</b>		<b>ADVANCED</b>		<b>STANDARD</b>		<b>STANDARD</b>	
<b>Number of false positives<sup>1</sup></b>		<b>many</b>		<b>many</b>		<b>many</b>		<b>many</b>	
<b>ProActive detection of "NEW" samples<sup>11</sup></b>									
Windows viruses	540	494	91%	332	61%	298	55%	303	56%
Script malware	187	45	24%	91	49%	79	42%	24	13%
Worms	1.390	1.020	73%	935	67%	503	36%	735	53%
Backdoors	10.120	8.114	80%	7.853	78%	6.052	60%	5.524	55%
Trojans	33.165	20.815	63%	17.483	53%	11.016	33%	11.507	35%
other malware	429	302	70%	220	51%	140	33%	169	39%
<b>TOTAL</b>	<b>45.831</b>	<b>30.790</b>	<b>67%</b>	<b>26.914</b>	<b>59%</b>	<b>18.088</b>	<b>39%</b>	<b>18.262</b>	<b>40%</b>
<b>Results over first week only</b>	<b>11.295</b>		<b>71%</b>		<b>66%</b>		<b>40%</b>		<b>43%</b>

<i>Company</i>		BitDefender		MicroWorld		ESET		F-Secure	
<i>Product</i>		<b>BitDefender AV</b>		<b>eScan Anti-Virus</b>		<b>ESET NOD32 Antivirus</b>		<b>F-Secure Anti-Virus</b>	
<i>Program version</i>		11.0.17		9.0.824.217		3.0.669.0		9.00.148	
<i>Engine / signature version</i>		N/A		N/A		3325		8.10.14240	
<i>Number of virus records</i>		1.414.639		unknown		unknown		unknown	
<b>Certification level reached</b>		<b>STANDARD</b>				<b>ADVANCED+</b>			
<b>Number of false positives<sup>1</sup></b>		<b>many</b>		<b>few</b>		<b>few</b>		<b>few</b>	
<b>ProActive detection of "NEW" samples<sup>11</sup></b>									
Windows viruses	540	324	60%	276	51%	306	57%	365	68%
Script malware	187	36	19%	50	27%	20	11%	52	28%
Worms	1.390	801	58%	166	12%	840	60%	167	12%
Backdoors	10.120	5.908	58%	791	8%	5.838	58%	1.187	12%
Trojans	33.165	14.046	42%	2.285	7%	15.979	48%	2.546	8%
other malware	429	172	40%	32	7%	217	51%	36	8%
<b>TOTAL</b>	<b>45.831</b>	<b>21.287</b>	<b>46%</b>	<b>3.600</b>	<b>8%</b>	<b>23.200</b>	<b>51%</b>	<b>4.353</b>	<b>9%</b>
<b>Results over first week only</b>	<b>11.295</b>		<b>51%</b>		<b>18%</b>		<b>54%</b>		<b>20%</b>

<i>Company</i>		Kaspersky Labs		McAfee		Microsoft		Norman ASA	
<i>Product</i>		<b>Kaspersky AV</b>		<b>McAfee VirusScan+</b>		<b>Microsoft OneCare</b>		<b>Norman AV+AS</b>	
<i>Program version</i>		8.0.0.454		12.1.110		2.5.2900.03		7.10	
<i>Engine / signature version</i>		N/A		5300.2777 / 5352		1.3807 / 1.41.18.0		5.93.01	
<i>Number of virus records</i>		1.045.550		437.316		753.216		1.979.741	
<b>Certification level reached</b>		<b>ADVANCED</b>		<b>ADVANCED</b>		<b>ADVANCED</b>		<b>STANDARD</b>	
<b>Number of false positives<sup>1</sup></b>		<b>many</b>		<b>very few</b>		<b>very few</b>		<b>many</b>	
<b>ProActive detection of "NEW" samples<sup>11</sup></b>									
Windows viruses	540	498	92%	484	90%	451	84%	46	9%
Script malware	187	53	28%	37	20%	82	44%	13	7%
Worms	1.390	826	59%	315	23%	592	43%	406	29%
Backdoors	10.120	6.677	66%	4.206	42%	5.151	51%	3.412	34%
Trojans	33.165	19.251	58%	8.262	25%	13.777	42%	7.632	23%
other malware	429	178	41%	182	42%	244	57%	103	24%
<b>TOTAL</b>	<b>45.831</b>	<b>27.483</b>	<b>60%</b>	<b>13.486</b>	<b>29%</b>	<b>20.297</b>	<b>44%</b>	<b>11.612</b>	<b>25%</b>
<b>Results over first week only</b>	<b>11.295</b>		<b>71%</b>		<b>37%</b>		<b>47%</b>		<b>25%</b>

Company	Symantec	Sophos	Trustport	VirusBlokAda					
Product	<b>Horton Anti-Virus</b>	<b>Sophos E S&amp;C</b>	<b>TrustPort Antivirus</b>	<b>VBA32 Anti-Virus</b>					
Program version	16.0.0.125	7.5.1	2.8.0.3006	3.12.8.2					
Engine / signature version	100804c / 84315	2.75.4 / 4.31E+305	N/A	N/A					
Number of virus records	2.043.091	447.478	unknown	unknown					
<b>Certification level reached</b>	<b>ADVANCED</b>		<b>STANDARD</b>	<b>STANDARD</b>					
<b>Number of false positives*</b>	<b>few</b>	<b>(very many)*</b>	<b>many</b>	<b>many</b>					
<b>ProActive detection of "NEW" samples**</b>									
Windows viruses	540	309	57%	324	60%	312	58%	195	36%
Script malware	187	50	27%	35	19%	30	16%	18	10%
Worms	1.390	734	53%	783	56%	827	59%	282	20%
Backdoors	10.120	5.064	50%	6.863	68%	6.495	64%	3.649	36%
Trojans	33.165	13.876	42%	14.847	45%	14.460	44%	7.871	24%
other malware	429	200	47%	178	41%	179	42%	54	13%
<b>TOTAL</b>	<b>45.831</b>	<b>20.233</b>	<b>44%</b>	<b>23.030</b>	<b>50%</b>	<b>22.303</b>	<b>49%</b>	<b>12.069</b>	<b>26%</b>
<b>Results over first week only</b>	<b>11.295</b>	<b>44%</b>	<b>51%</b>	<b>50%</b>	<b>26%</b>				

The below table shows the proactive on-demand detection capabilities of the various products, sorted by detection rate. The given awards (see page 7 of this report) are based not only on the detection rates over the new malware appeared during the four weeks, but also considering the false alarm rates.



#### **4. Summary results**

The results show the proactive on-demand<sup>3</sup> 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 our methodology document for further details (<http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf>).

Below you can see the test results over the two time periods:

(a) ProActive detection of new samples (1<sup>st</sup> week only):

1. AVIRA, Kaspersky	71%
2. GDATA	66%
3. NOD32	54%
4. Sophos, BitDefender	51%
5. TrustPort	50%
6. Microsoft	47%
7. Symantec	44%
8. AVG	43%
9. Avast	40%
10. McAfee	37%
11. VBA32	26%
12. Norman	25%
13. F-Secure	20%
14. eScan	18%

(b) ProActive detection of new samples (all 4-weeks):

1. AVIRA	67%
2. Kaspersky	60%
3. GDATA	59%
4. NOD32	51%
5. Sophos	50%
6. TrustPort	49%
7. BitDefender	46%
8. Microsoft, Symantec	44%
9. AVG	40%
10. Avast	39%
11. McAfee	29%
12. VBA32	26%
13. Norman	25%
14. F-Secure <sup>4</sup>	9%
15. eScan	8%

As the four weeks period contains a broader variety and amount of samples, it reflects in our opinion better the overall proactive/generic/heuristic detection capabilities against new malware of the various Anti-Virus products.

<sup>3</sup> this test is performed on-demand – it is **NOT** an on-execution/behavioral test.

<sup>4</sup> with an engine which works only in real-time, F-Secure would detect 33% (4 weeks) and 41% (1st week), but it would also have „very many“ false alarms. In addition to this engine, F-Secure and also some other Anti-Virus products contain various proactive protection technologies that were not tested in this retrospective test.

## 5. False positive/alarm test

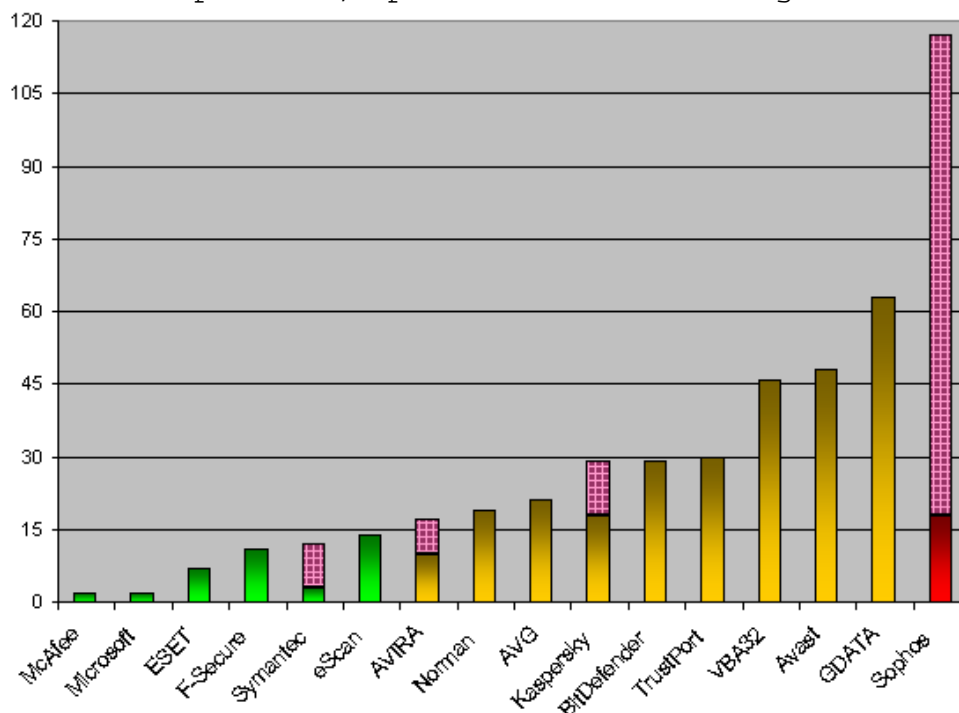
To better evaluate the quality of the detection capabilities, the false alarm rate has to be taken into account too. A false alarm (or false positive) is when an Anti-Virus product flags an innocent file to be infected when it is not. False alarms can sometimes cause as much troubles like a real infection.

**We included this false alarm test already in the test report Nr. 19. For details, please download and read the report available at <http://www.av-comparatives.org/seiten/ergebnisse/report19.pdf>**

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

1. McAfee, Microsoft	1	very few FP's
2. ESET	7	
3. F-Secure	11	
4. Symantec	12	few FP's
5. eScan	14	
6. AVIRA	17	
7. Norman	19	
8. AVG	21	
9. BitDefender	27	
10. Kaspersky	28	many FP's
11. Trustport	30	
12. VBA32	46	
13. Avast	47	
14. GDATA	62	
15. Sophos <sup>5</sup>	117	very many FP's

The graph below shows the number of false alarms by the various Anti-Virus products, split in default and highest settings:






<sup>5</sup> Sophos is an exception in our tests, because while the other products are targeted for the home user and corporate market, Sophos products are designed exclusively the corporate market, where Administrators would in fact like to get informed about the misdetections<sup>5</sup> (<http://www.sophos.com/security/blog/2008/06/1485.html>).

## 6. Certification levels reached in this test

We provide a 3-level-ranking-system (STANDARD, ADVANCED and ADVANCED+). Overviews of levels reached in past can be found on our website (<http://www.av-comparatives.org/seiten/overview.html>).

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

<u>CERTIFICATION LEVELS</u>	<u>PRODUCTS</u>
	NOD32
	AVIRA* Kaspersky* Microsoft Symantec McAfee GDATA*
	TrustPort* BitDefender* AVG* Avast* Norman* VBA32*
no certification	Sophos* F-Secure eScan

\*: Products with "many" false alarms (Avast, AVG, AVIRA, BitDefender, GDATA, Kaspersky, Norman, Sophos, Trustport and VBA32) were penalized according to the below award system:

	0-10%	10-25%	25-50%	50-100%
none - few	NO AWARD	STANDARD	ADVANCED	ADVANCED+
many	NO AWARD	NO AWARD	STANDARD	ADVANCED
very many	NO AWARD	NO AWARD	NO AWARD	NO AWARD

Note: With default settings, AVIRA would have less false alarms than with highest settings, but still detect over 50% of the test-set.

To join our newsletter, please visit [www.av-comparatives.org](http://www.av-comparatives.org)

## **7. Copyright and Disclaimer**

This publication is Copyright © 2008 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 be 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 a Non-Profit Organization.

AV-Comparatives e.V. (November 2008)