

Anti-Virus Comparative



Proactive/retrospective test

(on-demand detection of virus/malware)

Language: English

August/November 2009

Last revision: 27th November 2009

www.av-comparatives.org

Content



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

1. Introduction

This test report is the second part of the August 2009 test¹. The report is delivered late November due to the high-required work, deeper analysis and preparation of the retrospective test-set.

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, hourly or cloud 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 10th August, and the same highest² detection settings were used. This test shows the proactive detection capabilities that the products had at that time. We used new malware appeared between the 11th and 17th August 2009.

The following 16 products were tested:

- 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
- Microsoft³ Security Essentials 1.0
- Norman Antivirus & Anti-Spyware 7.10.02
- Sophos Anti-Virus 7.6.10
- Symantec Norton Anti-Virus 17.0.0.136
- Trustport Antivirus 2009 2.8.0.3017

2. Description

Anti-Virus products often claim to have high proactive detection capabilities – far higher than those reached in this test. This is not just a self-promotional statement; it is 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 should not 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 have 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 by AV-Comparatives with e.g. dynamic tests.

¹ http://www.av-comparatives.org/images/stories/test/ondret/avc_report23.pdf

² except F-Secure and Sophos; see comments in the August 2009 test report

³ scores exactly as Microsoft Live OneCare 2.5.2900.28

3. Test Results

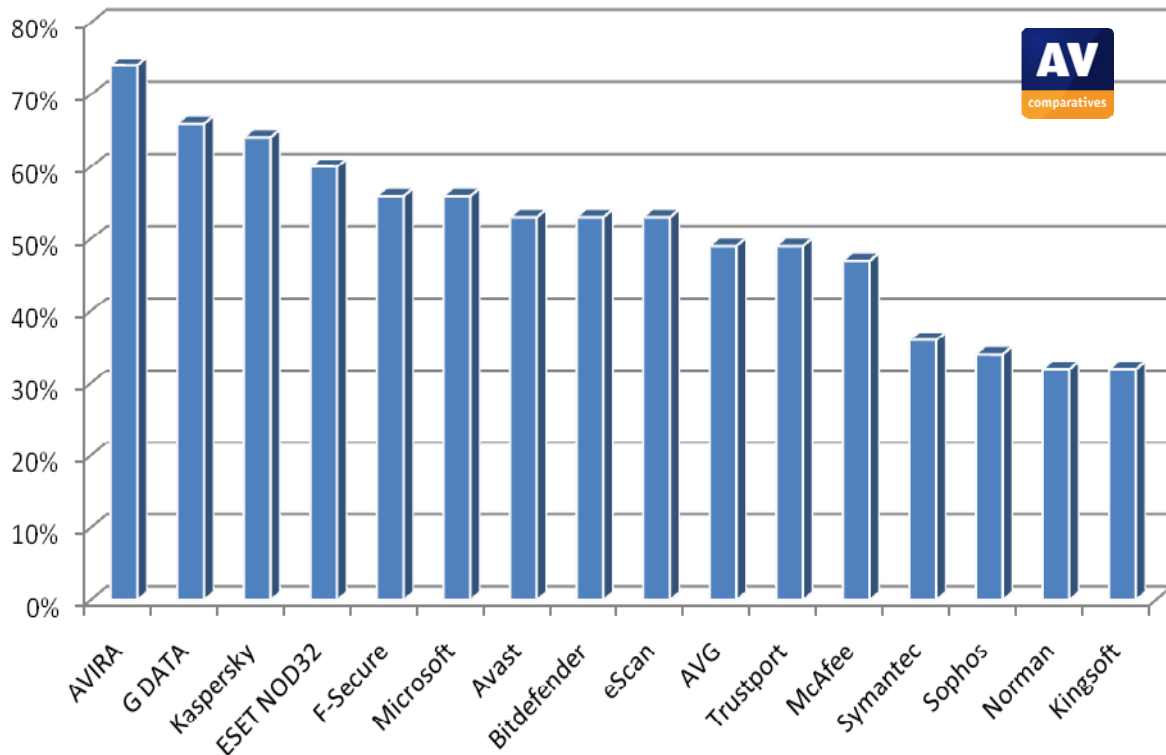
Company	AVIRA	Alwil Software	AVG Technologies	BitDefender					
Product	AntiVir Premium	avast! Professional	AVG Anti-Virus	BitDefender AV					
Program version	9.0.0.446	4.8.1348	8.5.406	13.0.13.254					
Engine / signature version	8.02.00.248/7.01.05.93	090810-0	270.13.49/2294	N/A					
Certification level reached	ADVANCED	ADVANCED+	ADVANCED	ADVANCED+					
Number of false positives	<i>many</i>	<i>few</i>	<i>few</i>	<i>few</i>					
ProActive detection of "NEW" samples									
Worms	4.903	4.328	88%	3.980	81%	2.350	48%	2.778	57%
Backdoors	2.839	2.188	77%	1.030	36%	1.866	66%	1.656	58%
Trojans	15.053	10.487	70%	7.059	47%	6.997	46%	7.684	51%
other malware/viruses	442	279	63%	272	62%	240	54%	184	42%
TOTAL	23.237	17.282	74%	12.341	53%	11.453	49%	12.302	53%

Company	MicroWorld	F-Secure	G DATA Security	Kaspersky Labs					
Product	eScan Anti-Virus	F-Secure Anti-Virus	G DATA AntiVirus	Kaspersky AV					
Program version	10.0.997.491	10.00.246	20.0.4.9	9.0.0.463					
Engine / signature version	N/A	9.10.15261	N/A	N/A					
Certification level reached	ADVANCED+	ADVANCED+	ADVANCED+	ADVANCED+					
Number of false positives	<i>few</i>	<i>few</i>	<i>few</i>	<i>few</i>					
ProActive detection of "NEW" samples									
Worms	4.903	2.778	57%	3.107	63%	4.118	84%	2.753	56%
Backdoors	2.839	1.656	58%	1.688	59%	1.687	59%	2.035	72%
Trojans	15.053	7.684	51%	8.105	54%	9.300	62%	9.782	65%
other malware/viruses	442	184	42%	184	42%	303	69%	213	48%
TOTAL	23.237	12.302	53%	13.084	56%	15.408	66%	14.783	64%

Company	Kingsoft	McAfee	ESET	Norman ASA					
Product	Kingsoft AntiVirus	McAfee VirusScan+	IID32 Antivirus	Norman AV+AS					
Program version	2009.11.6.63	13.11.102	4.0.437.0	7.10.02					
Engine / signature version	2009.8.10.12	5400.1158 / 5705	4323.1230	6.01.09					
Certification level reached	STANDARD	STANDARD	ADVANCED+	STANDARD					
Number of false positives	<i>many</i>	<i>many</i>	<i>few</i>	<i>many</i>					
ProActive detection of "NEW" samples									
Worms	4.903	2.223	45%	3.762	77%	4.166	85%	493	10%
Backdoors	2.839	1.176	41%	1.049	37%	1.441	51%	1.532	54%
Trojans	15.053	3.895	26%	6.013	40%	8.148	54%	5.353	36%
other malware/viruses	442	118	27%	152	34%	250	57%	128	29%
TOTAL	23.237	7.412	32%	10.976	47%	14.005	60%	7.506	32%

Company	Symantec	Microsoft	Sophos	Trustport					
Product	Horton Anti-Virus	Security Essentials	Sophos Anti-Virus	TrustPort AV					
Program version	17.0.0.136	1.0	7.6.10	2.8.0.3017					
Engine / signature version	N/A	N/A	2.89.1 / 4.44E+183	N/A					
Certification level reached	ADVANCED	ADVANCED+	STANDARD	STANDARD					
Number of false positives	<i>few</i>	<i>few</i>	<i>many</i>	<i>many</i>					
ProActive detection of "NEW" samples									
Worms	4.903	755	15%	3.115	64%	1.323	27%	2.341	48%
Backdoors	2.839	1.254	44%	1.648	58%	1.054	37%	1.851	65%
Trojans	15.053	6.281	42%	8.043	53%	5.307	35%	6.935	46%
other malware/viruses	442	175	40%	220	50%	133	30%	232	52%
TOTAL	23.237	8.465	36%	13.026	56%	7.817	34%	11.359	49%

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, but also considering the false alarm rates.



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.

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. In retrospective tests „in-the-cloud“ technologies are not considered⁴, as well it was not considered how often or how fast new updates are delivered to the user, as that it not the scope of the test. Nowadays, hardly any Anti-Virus products rely purely on “simple” signatures anymore. They all use complex generic signatures, heuristics etc. in order to catch new malware, without needing to download signatures or initiate manual analysis of new threats.

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 good protection.

⁴ All products, including McAfee, were tested without Internet connection.

4. Summary results

The results show the proactive on-demand⁵ 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 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, using a one-week period reflects well the varying 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 our set of new malware appeared within one week:

ProActive detection of new malware:

1.	AVIRA	74%
2.	G DATA	66%
3.	Kaspersky	64%
4.	ESET NOD32	60%
5.	F-Secure, Microsoft⁶	56%
6.	Avast, BitDefender, eScan	53%
7.	AVG, TrustPort	49%
8.	McAfee	47%
9.	Symantec	36%
10.	Sophos	34%
11.	Norman, Kingsoft	32%

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. The false alarm test results were already included in the test report Nr. 23. For details, please read the report available at http://www.av-comparatives.org/images/stories/test/fp/avc_report23_fp.pdf

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




⁵ this test is performed on-demand – it is **NOT** an on-execution/behavioral test.

⁶ Microsoft Security Essentials scores the same as OneCare.

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 website⁷.

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

CERTIFICATION LEVELS	PRODUCTS
	G DATA Kaspersky ESET NOD32 F-Secure Microsoft Avast BitDefender eScan
	AVIRA* AVG Symantec
	McAfee* TrustPort* Sophos* Norman* Kingsoft*

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

	Proactive Detection Rates			
	0-10%	10-25%	25-50%	50-100%
None - Few FP	tested	STANDARD	ADVANCED	ADVANCED+
Many FP	tested	tested	STANDARD	ADVANCED

Due to structural changes/enhancements of the test-set, we will set up new marks for the awards next year.

⁷ <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 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 an Austrian Non-Profit Organization.

AV-Comparatives e.V. (November 2009)