Anti-Virus Comparative

Proactive/retrospective test

(on-demand detection of virus/malware)

Language: English
May 2009
Last revision: 27th May 2009

www.av-comparatives.org

Content

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.

[1] http://www.av-comparatives.org/images/stories/test/ondret/avc_report21.pdf
[2] except Sophos Anti-Virus; see comments in the February 2009 test report

3. Test results

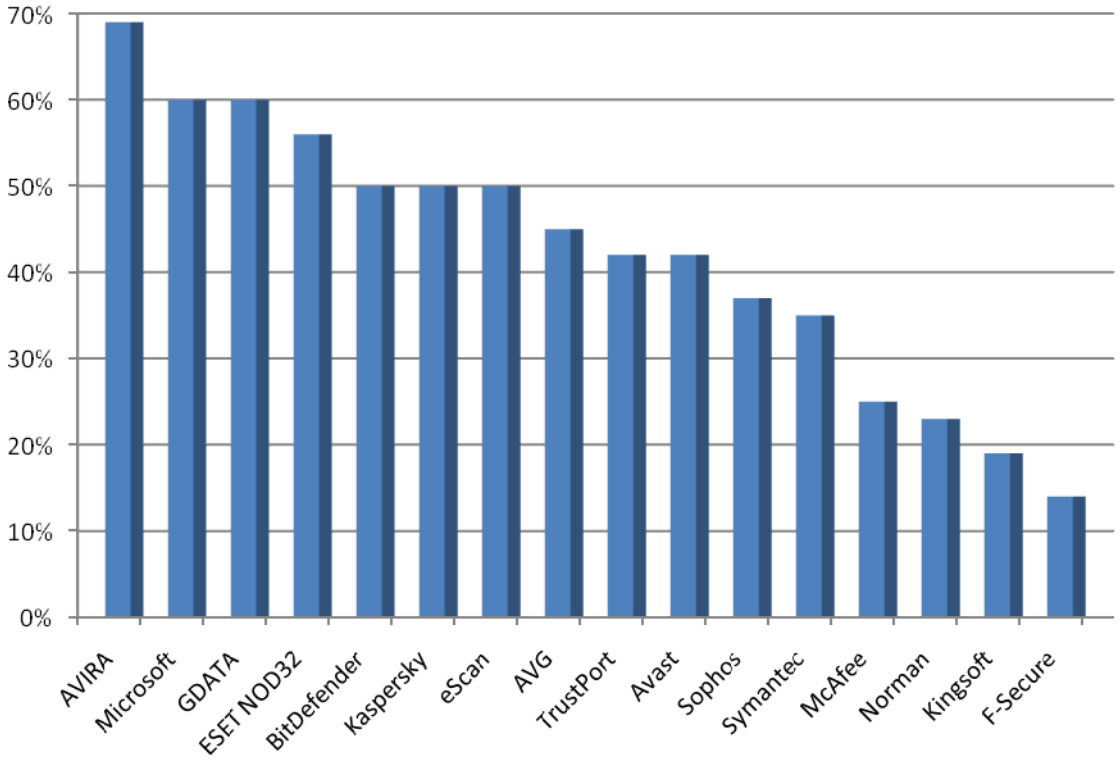
Company		AVIRA		Alwil Software		AVG Technologies		BitDefender	
Product		**AntiVir Premium**		**avast! Professional**		**AVG Anti-Virus**		**BitDefender AV**	
Program version		8.2.0.374		4.8.1335		8.0.234		12.0.11.4	
Engine / signature version		8.02.00.76/7.01.01.248		090209-0		270.10.19/1941		*N/A*	
Certification level reached		**ADVANCED**		**STANDARD**		**STANDARD**		**ADVANCED**	
Number of false positives		*many*		*many*		*many*		*many*	
ProActive detection of "NEW" samples									
Windows viruses	188	161	86%	65	35%	89	47%	87	46%
Worms	1.738	626	36%	349	20%	330	19%	562	32%
Backdoors	4.966	3.737	75%	2.677	54%	2.656	53%	3.087	62%
Trojans	13.555	9.523	70%	5.288	39%	5.823	43%	6.607	49%
other malware (incl. script+macro)	2.238	1.698	76%	1.156	52%	1.287	58%	1.105	49%
TOTAL	**22.685**	15.745	**69%**	9.535	**42%**	10.185	**45%**	11.448	**50%**

Company		MicroWorld		F-Secure		G DATA Security		Kaspersky Labs	
Product		**eScan ISS**		**F-Secure Anti-Virus**		**G DATA AntiVirus**		**Kaspersky AV**	
Program version		10.0.946.341		9.00.149		19.1.0.0		8.0.0.506a	
Engine / signature version		*N/A*		8.10.14240		19.3715 / 19.219		*N/A*	
Certification level reached		**ADVANCED**		**STANDARD**		**ADVANCED**		**ADVANCED+**	
Number of false positives		*many*		*few*		*many*		*few*	
ProActive detection of "NEW" samples									
Windows viruses	188	87	46%	78	41%	98	52%	157	84%
Worms	1.738	561	32%	53	3%	606	35%	391	22%
Backdoors	4.966	3.080	62%	487	10%	3.573	72%	2.826	57%
Trojans	13.555	6.600	49%	1.778	13%	8.022	59%	6.353	47%
other malware (incl. script+macro)	2.238	1.101	49%	889	40%	1.322	59%	1.711	76%
TOTAL	**22.685**	11.429	**50%**	3.285	**14%**	13.621	**60%**	11.438	**50%**

Company		Kingsoft		McAfee		Microsoft		ESET	
Product		**Kingsoft AntiVirus**		**McAfee VirusScan+**		**Microsoft OneCare**		**NOD32 Antivirus**	
Program version		2008.11.6.63		13.3.117		2.5.2900.20		3.0.684.0	
Engine / signature version		*2009.2.8.1*		5300.2777 / 5521		1.51.391.0		3839.1180	
Certification level reached				**ADVANCED**		**ADVANCED+**		**ADVANCED+**	
Number of false positives		*many*		*few*		*very few*		*few*	
ProActive detection of "NEW" samples									
Windows viruses	188	43	23%	122	65%	82	44%	91	48%
Worms	1.738	190	11%	271	16%	581	33%	428	25%
Backdoors	4.966	1.230	25%	1.686	34%	3.172	64%	2.894	58%
Trojans	13.555	2.646	20%	3.242	24%	7.850	58%	7.416	55%
other malware (incl. script+macro)	2.238	112	5%	371	17%	1.981	89%	1.819	81%
TOTAL	**22.685**	4.221	**19%**	5.692	**25%**	13.666	**60%**	12.648	**56%**

Company		Norman ASA		Symantec		Sophos		Trustport	
Product		**Norman AV+AS**		**Norton Anti-Virus**		**Sophos Anti-Virus**		**TrustPort AV**	
Program version		7.10.02		16.2.0.7		7.6.4		2.8.0.3011	
Engine / signature version		6.00.06		110208v / 91468		2.83.3 / 4.38E+180		*N/A*	
Certification level reached				**ADVANCED**		**ADVANCED**		**STANDARD**	
Number of false positives		*many*		*few*		*few*		*many*	
ProActive detection of "NEW" samples									
Windows viruses	188	57	30%	60	32%	79	42%	85	45%
Worms	1.738	316	18%	315	18%	359	21%	408	23%
Backdoors	4.966	1.637	33%	1.761	35%	1.715	35%	2.588	52%
Trojans	13.555	3.028	22%	4.690	35%	5.082	37%	5.314	39%
other malware (incl. script+macro)	2.238	99	4%	1.005	45%	1.143	51%	1.210	54%
TOTAL	**22.685**	5.137	**23%**	7.831	**35%**	8.378	**37%**	9.605	**42%**

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[3] 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[4], 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 website[5].

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

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

[5] http://www.av-comparatives.org/comparativesreviews/main-tests/summary-reports

7. Copyright and Disclaimer

AV-Comparatives e.V. (May 2009)