Anti-Virus Comparative

Proactive/retrospective test

(on-demand detection of virus/malware)

Language: English
February/May 2010
Last revision: 5th June 2010

www.av-comparatives.org

Content

1. Introduction

This test report is the second part of the February 2010 test[1]. The report is delivered begin of June due 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, but also that they are able to detect such threats in advance (also without executing them) 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 reliably protected.

The products used the same updates and signatures they had the 10th February, and the same highest[2] detection settings were used as in February. This test shows the proactive detection capabilities that the products had at that time. We used new malware appeared between the 11th and 18th February 2010. The following 20 products were tested:

- avast! Free[3] Antivirus 5.0
- AVG Anti-Virus 9.0
- AVIRA AntiVir Premium 9.0
- BitDefender Anti-Virus 2010
- eScan Anti-Virus 10.0
- ESET NOD32 Antivirus 4.0
- F-Secure Anti-Virus 2010
- G DATA AntiVirus 2010
- K7 TotalSecurity 10.0
- Kaspersky Anti-Virus 2010
- Kingsoft AntiVirus 2010
- McAfee AntiVirus Plus 2010
- Microsoft Security Essentials 1.0
- Norman Antivirus & Anti-Spyware 7.30
- Panda Antivirus Pro 2010
- PC Tools Spyware Doctor with Antivirus 7.0
- Sophos Anti-Virus 9.0
- Symantec Norton Anti-Virus 2010
- Trend Micro AntiVirus plus AntiSpyware 2010
- Trustport[4] Antivirus 2010

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 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 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 considered by AV-Comparatives in e.g. dynamic tests.

[1] http://www.av-comparatives.org/images/stories/test/ondret/avc_report25.pdf

[2] except AVG, AVIRA, F-Secure and Sophos; see comments in the February 2010 test report or on page 6

[3] Avast Software decided to participate in the tests with their free product version

[4] Based on two engines (AVG and Bitdefender)

3. Test Results

Note: If you are going to republish those results, it is compulsory to include a comment that products use also additional protection features (like behavior-blockers, etc.) to protect against completely new/unknown malware. As described on previous and next pages, this test evaluates only the heuristic/generic detection of the products against unknown/new malware, without the need to execute it.

Company		AVIRA		Avast Software		AVG Technologies		BitDefender	
Product		**AntiVir Premium**		**avast! Free Antivirus**		**AVG Anti-Virus**		**BitDefender AV**	
Program version		9.0.0.457		5.0.396		9.0.733		13.0.19.347	
Engine / signature version		8.02.01.160/7.10.04.23		100210-0		271.1.1/2679		N/A	
Certification level reached		**ADVANCED+**		**ADVANCED**		**ADVANCED**		**ADVANCED+**	
Number of false positives		**few**		**few**		**few**		**very few**	
ProActive detection of "NEW" samples									
Worms	6.541	1.841	28%	353	5%	970	15%	5.133	78%
Backdoors	3.342	2.681	80%	1.787	53%	1.810	54%	1.836	55%
Trojans	17.046	9.833	58%	5.523	32%	6.215	36%	6.574	39%
other malware/viruses	342	178	52%	182	53%	142	42%	149	44%
TOTAL	**27.271**	14.533	**53%**	7.845	**29%**	9.137	**34%**	13.692	**50%**

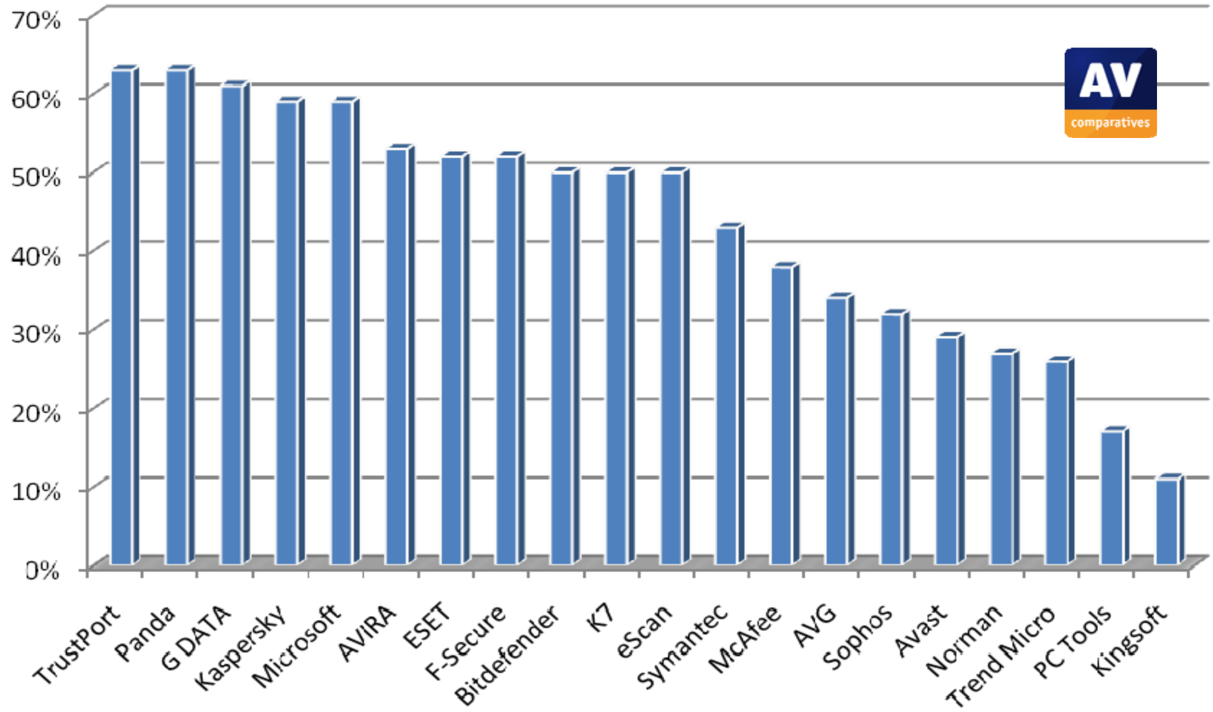
Company		MicroWorld		F-Secure		G DATA Security		K7 Computing	
Product		**eScan Anti-Virus**		**F-Secure Anti-Virus**		**G DATA AntiVirus**		**K7 TotalSecurity**	
Program version		10.0.1058.644		10.12.108		20.2.4.1		10.0.0025	
Engine / signature version		N/A		9.20.15437		N/A		9.38.0891	
Certification level reached		**ADVANCED+**		**ADVANCED+**		**ADVANCED+**		**ADVANCED**	
Number of false positives		**very few**		**very few**		**few**		**very many**	
ProActive detection of "NEW" samples									
Worms	6.541	5.130	78%	5.135	79%	5.253	80%	2.021	31%
Backdoors	3.342	1.799	54%	1.894	57%	2.409	72%	2.585	77%
Trojans	17.046	6.574	39%	7.016	41%	8.648	51%	8.906	52%
other malware/viruses	342	149	44%	151	44%	226	66%	146	43%
TOTAL	**27.271**	13.652	**50%**	14.196	**52%**	16.536	**61%**	13.658	**50%**

Company		Kaspersky Labs		Kingsoft		McAfee		ESET	
Product		**Kaspersky AV**		**Kingsoft AntiVirus**		**McAfee AntiVirus +**		**NOD32 Antivirus**	
Program version		9.0.0.736 (a.b)		2010.02.10.01		14.0.306		4.0.474.0	
Engine / signature version		N/A		N/A		5400.1158 / 5888		4854.1261	
Certification level reached		**ADVANCED+**				**STANDARD**		**ADVANCED+**	
Number of false positives		**few**		**many**		**many**		**very few**	
ProActive detection of "NEW" samples									
Worms	6.541	5.336	82%	140	2%	2.997	46%	2.007	31%
Backdoors	3.342	1.748	52%	673	20%	1.841	55%	2.464	74%
Trojans	17.046	8.898	52%	2.190	13%	5.331	31%	9.553	56%
other malware/viruses	342	105	31%	87	25%	97	28%	183	54%
TOTAL	**27.271**	16.087	**59%**	3.090	**11%**	10.266	**38%**	14.207	**52%**

Company		Norman ASA		Symantec		Panda Security		Microsoft	
Product		**Norman AV+AS**		**Norton Anti-Virus**		**Panda Antivirus Pro**		**Security Essentials**	
Program version		7.30		17.5.0.127		9.01.00		1.0.1611.0	
Engine / signature version		6.04.03		120210d		N/A		1.75.617.0	
Certification level reached		**STANDARD**		**ADVANCED**		**ADVANCED**		**ADVANCED+**	
Number of false positives		**many**		**few**		**many**		**very few**	
ProActive detection of "NEW" samples									
Worms	6.541	188	3%	5.208	80%	5.900	90%	5.170	79%
Backdoors	3.342	1.676	50%	1.838	55%	2.129	64%	2.327	70%
Trojans	17.046	5.518	32%	4.583	27%	9.059	53%	8.366	49%
other malware/viruses	342	93	27%	165	48%	110	32%	129	38%
TOTAL	**27.271**	7.475	**27%**	11.794	**43%**	17.198	**63%**	15.992	**59%**

Company		Sophos		PC Tools		Trend Micro		Trustport	
Product		**Sophos Anti-Virus**		**SpywareDoctor+AV**		**Trend Micro AV+AS**		**TrustPort AV**	
Program version		9.0.3		7.0.0.514		17.50.1366.0000		5.0.0.4087	
Engine / signature version		3.4.2 / 4.50G+204		N/A		6.837.50		N/A	
Certification level reached		**ADVANCED**		**STANDARD**		**STANDARD**		**ADVANCED+**	
Number of false positives		**few**		**few**		**many**		**few**	
ProActive detection of "NEW" samples									
Worms	6.541	327	5%	677	10%	1.681	26%	5.234	80%
Backdoors	3.342	2.044	61%	893	27%	1.195	36%	2.389	71%
Trojans	17.046	6.310	37%	2.809	16%	4.083	24%	9.412	55%
other malware/viruses	342	88	26%	142	42%	79	23%	191	56%
TOTAL	**27.271**	8.769	**32%**	4.521	**17%**	7.038	**26%**	17.226	**63%**

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.



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" signatures are not considered, as well it was not considered how often or how fast new updates are delivered to the user, as that is not the scope of the test.

As it can be seen above, most products are able to detect a quantity of completely new/unknown malware proactively 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.

We tried to include in the test-set only prevalent real-world malware that has not been seen before the 10th February 2010 by consulting telemetry / cloud data collected and shared within the AV industry. Consulting that data was quite interesting for us, as it showed that, while some vendors had seen some malware already many months or even years ago, the same malware hashes appeared in some other vendors clouds only recently.

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.

To avoid some frequent questions, below are some notes about the used settings (scan of all files etc. is always enabled) of some products, whereas highest settings were not used on vendors request:

F-Secure, Sophos: asked to get tested and awarded based on their default settings (i.e. without using their advanced heuristics / suspicious detections setting).

AVG, AVIRA: asked to do not enable/consider the informational warnings of packers as detections.

4. Summary results

The results show the proactive (generic/heuristic) on-demand[5] detection capabilities of the scan engines against new malware. 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. Below you can see the proactive on-demand detection results over our set of new malware appeared within about one week:

ProActive detection of new malware:

1.	**Trustport, Panda**	**63%**
2.	**G DATA**	**61%**
3.	**Kaspersky, Microsoft**	**59%**
4.	**AVIRA**	**53%**
5.	**ESET NOD32, F-Secure**	**52%**
6.	**BitDefender, K7, eScan**	**50%**
7.	**Symantec**	**43%**
8.	**McAfee**	**38%**
9.	**AVG**	**34%**
10.	**Sophos**	**32%**
11.	**Avast**	**29%**
12.	**Norman**	**27%**
13.	**Trend Micro**	**26%**
14.	**PC Tools**	**17%**
15.	**Kingsoft**	**11%**

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)[6] 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. 25. For details, please read the report available at http://www.av-comparatives.org/images/stories/test/fp/avc_report25_fp.pdf

Very few false alarms (0-3):	eScan, F-Secure, Bitdefender, Microsoft, ESET
Few false alarms (4-15):	Sophos, Kaspersky, G DATA, PC Tools, Trustport, AVG, Avast, Symantec, AVIRA
Many false alarms (over 15):	Trend Micro, Panda, McAfee, Norman, Kingsoft, K7

[5] this test is performed on-demand – it is NOT an on-execution/behavioral test.
[6] All discovered false alarms were already reported to the vendors in February and are now already fixed.

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[7].
The following certification levels are for the results reached in the retrospective test:

CERTIFICATION LEVELS	PRODUCTS
AV comparatives ADVANCED+ ★★★ RETROSPECTIVE / PROACTIVE TEST MAY 2010	TrustPort G DATA Kaspersky Microsoft AVIRA ESET NOD32 F-Secure BitDefender eScan
AV comparatives ADVANCED ★★ RETROSPECTIVE / PROACTIVE TEST MAY 2010	Panda* K7* Symantec AVG Sophos Avast
AV comparatives STANDARD ★ RETROSPECTIVE / PROACTIVE TEST MAY 2010	McAfee* Norman* Trend Micro* PC Tools
AV comparatives TESTED RETROSPECTIVE / PROACTIVE TEST MAY 2010	Kingsoft*

*: Products with "many" false alarms were rated 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

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

7. Copyright and Disclaimer

This publication is Copyright © 2010 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. (June 2010)