Anti-Virus Comparative

Proactive/retrospective test

(Static detection of new/unknown malicious software)

Language: English
August 2010
Last revision: 6th December 2010

www.av-comparatives.org

Content

1. Introduction

This test report is the second part of the August 2010 test[1]. The report is delivered begin of December 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 or while offline) 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 16th August, and the same detection settings as used in August (see page 6 of this report). This test shows the proactive detection capabilities that the products had at that time. We used new malware appeared between the 17th and 24th August 2010. The following products were tested[2]:

- avast! Free[3] Antivirus 5.0

- AVIRA AntiVir Premium 10.0

- BitDefender Anti-Virus 2011

- eScan Anti-Virus 10.0

- ESET NOD32 Antivirus 4.2

- F-Secure Anti-Virus 2011

- G DATA AntiVirus 2011

- K7 TotalSecurity 10.0

- Kaspersky Anti-Virus 2011

- Microsoft Security Essentials 1.0

- Panda Antivirus Pro 2011

- PC Tools Spyware Doctor with Antivirus 8.0

- Sophos Anti-Virus 9.5

- Symantec Norton Anti-Virus 2011

- Trustport 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 heuristic/generic detection capability was tested (offline). Some products may be had the ability to detect some samples e.g. on-execution or by other monitoring tools, like behaviour-blocker, reputation/cloud heuristics, etc. Those kinds of additional protection technologies are considered by AV-Comparatives in e.g. whole-product dynamic tests, but are outside the scope of this retrospective test.

---

[1] http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2010.pdf

[2] AVG, Kingsoft, McAfee, Norman and Trend Micro decided to not get included in this report and to renounce to get awarded

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

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 offline heuristic/generic detection of the products against unknown/new malware, without the need to execute it or to submit anything online.

Company Product Program version		AVIRA AntiVir Premium 10.0.0.603		Avast Software avast! Free Antivirus 5.0.594		BitDefender BitDefender AV 14.0.23.312		MicroWorld eScan Anti-Virus 10.0.1058.677	
Certification level reached		**ADVANCED+**		**ADVANCED**		**ADVANCED+**		**ADVANCED+**	
Number of false positives		few		few		few		few	
ProActive detection of "NEW" samples									
Worms	1.607	856	53%	639	40%	804	50%	802	50%
Backdoors	3.114	2.282	73%	1.604	52%	1.713	55%	1.704	55%
Trojans	17.440	9.965	57%	7.242	42%	9.382	54%	9.243	53%
other malware/viruses	1.076	708	66%	606	56%	764	71%	747	69%
TOTAL	**23.237**	13.811	**59%**	10.091	**43%**	12.663	**54%**	12.496	**54%**

Company Product Program version		F-Secure F-Secure Anti-Virus 10.50.197		G DATA Security G DATA AntiVirus 21.0.3.1		K7 Computing K7 TotalSecurity 10.0.0040		Kaspersky Labs Kaspersky AV 11.0.1.400 (a)	
Certification level reached		**ADVANCED+**		**ADVANCED+**		**ADVANCED**		**ADVANCED**	
Number of false positives		very few		few		many		many	
ProActive detection of "NEW" samples									
Worms	1.607	802	50%	832	52%	681	42%	961	60%
Backdoors	3.114	1.760	57%	2.316	74%	1.962	63%	1.825	59%
Trojans	17.440	9.615	55%	10.382	60%	8.519	49%	10.079	58%
other malware/viruses	1.076	764	71%	822	76%	503	47%	730	68%
TOTAL	**23.237**	12.941	**56%**	14.352	**62%**	11.665	**50%**	13.595	**59%**

Company Product Program version		ESET NOD32 Antivirus 4.2.58.3		Symantec Norton Anti-Virus 18.1.0.30		Panda Security Panda Antivirus Pro 10.00.00		Microsoft Security Essentials 1.0.1963.0	
Certification level reached		**ADVANCED+**		**ADVANCED+**		**ADVANCED**		**ADVANCED+**	
Number of false positives		few		few		many		very few	
ProActive detection of "NEW" samples									
Worms	1.607	782	49%	759	47%	788	49%	712	44%
Backdoors	3.114	1.909	61%	1.895	61%	1.942	62%	2.099	67%
Trojans	17.440	9.586	55%	8.753	50%	10.901	63%	8.653	50%
other malware/viruses	1.076	753	70%	537	50%	515	48%	523	49%
TOTAL	**23.237**	13.030	**56%**	11.944	**51%**	14.146	**61%**	11.987	**52%**

Company Product Program version		Sophos Sophos Anti-Virus 9.5.1		PC Tools SpywareDoctor+AV 8.0.0.594		Trustport TrustPort AV 5.0.0.4134	
Certification level reached		**ADVANCED+**		**ADVANCED**		**ADVANCED**	
Number of false positives		few		few		many	
ProActive detection of "NEW" samples							
Worms	1.607	844	53%	651	41%	815	51%
Backdoors	3.114	1.632	52%	1.139	37%	1.724	55%
Trojans	17.440	10.360	59%	6.165	35%	10.231	59%
other malware/viruses	1.076	630	59%	533	50%	773	72%
TOTAL	**23.237**	13.466	**58%**	8.488	**37%**	13.543	**58%**

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.
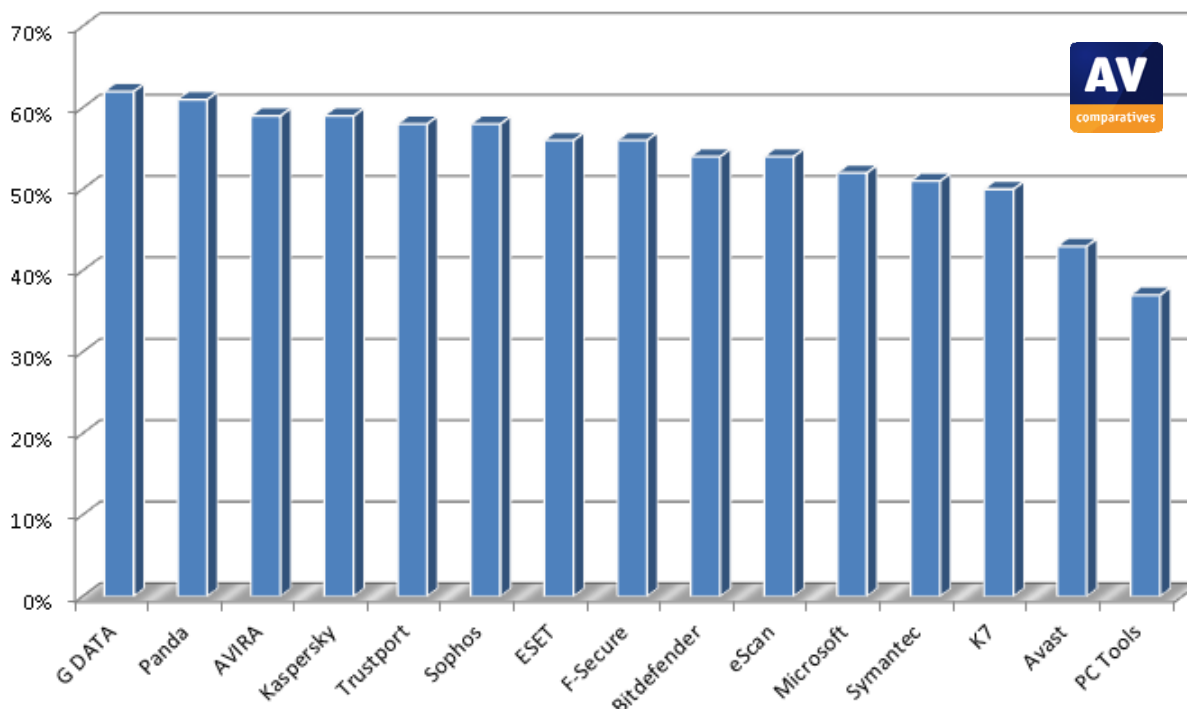
As it can be seen above, most of the tested products are able to detect a quantity of completely new/unknown malware proactively even without executing the malware, using passive heuristics, while other protective mechanisms like HIPS, behavior analysis and behavior-blockers, reputation/cloud heuristics, 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" features 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.

This test does not include some vendor's products who decided to do not be included in this "proactive/retrospective" test, e.g. because in their opinion their product's real-life capabilities are not adequately represented in the retrospective test due to the absence of a live Internet connection. The methodology of our "proactive/retrospective" testing indeed does not allow cloud-based products to connect to their remote knowledge bases, as this is not what we want to measure/compare in this type of test. Several other included products also have cloud-based technologies (and some don't), but at the same time they still provide good offline generic/heuristic detections, without having to rely on / sent data to their clouds and without having many false alarms. Cloud technologies should be seen as an additional protection enhancement, but not as a replacement of basic technologies.

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.

Almost all products run nowadays by default with highest protection settings (at least either at the entry points, during whole computer on-demand scans or scheduled scans) or switch automatically to highest settings in case of a detected infection. Due that, in order to get comparable results, we tested all products with highest settings, if not explicitly advised otherwise by the vendors (as we will use same settings over all tests, the reason is usually that their highest settings either cause too many false alarms, have a too high impact on system performance, or the settings are planned to be changed/removed by the vendor in near future). To avoid some frequent questions, below are some notes about the used settings (scan of all files etc. is always enabled) of some products:

AVIRA, Kaspersky, Symantec, TrustPort: asked to get tested with heuristic set to high/advanced. Due to that, we recommend users to consider also setting the heuristics to high/advanced.

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

AVIRA: asked to do not enable/consider the informational warnings of packers as detections. Due that, we did not count them as detections (neither on the malware set, nor on the clean set).

AV-Comparatives prefer to test with default settings. As most products run with highest settings by default (or switch to highest automatically when malware is found, making it impossible to test against various malware with "default" settings), in order to get comparable results we set also the few remaining products to highest settings (or leave them to lower settings) in accordance with the respective vendors. We hope that all vendors will find the appropriate balance of detection/false alarms/system impact and will provide highest security already by default and remove paranoid settings inside the user interface which are too high to be ever of any benefit for normal users.

4. Summary results

The results show the proactive (generic/heuristic) detection[4] 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.	**G DATA**	**62%**
2.	**Panda**	**61%**
3.	**AVIRA, Kaspersky**	**59%**
4.	**Trustport, Sophos**	**58%**
5.	**ESET, F-Secure**	**56%**
6.	**BitDefender, eScan**	**54%**
7.	**Microsoft**	**52%**
8.	**Symantec**	**51%**
9.	**K7**	**50%**
10.	**Avast**	**43%**
11.	**PC Tools**	**37%**

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)[5] 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 of August. For details, please read the report available at http://www.av-comparatives.org/images/stories/test/fp/avc_fp_aug2010.pdf

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

---

[4] this test is performed offline and on-demand – it is NOT an on-execution/behavioral/cloud test.
[5] All discovered false alarms were already reported to the vendors in August 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[6].

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

CERTIFICATION LEVELS	PRODUCTS
ADVANCED+ ★★★ RETROSPECTIVE / PROACTIVE TEST NOV 2010	G DATA AVIRA Sophos ESET F-Secure BitDefender eScan Microsoft Symantec
ADVANCED ★★ RETROSPECTIVE / PROACTIVE TEST NOV 2010	Panda* Kaspersky* TrustPort* K7* Avast PC Tools
STANDARD ★ RETROSPECTIVE / PROACTIVE TEST NOV 2010	-
TESTED RETROSPECTIVE / PROACTIVE TEST NOV 2010	-
NOT INCLUDED[7]	*AVG** *Kingsoft** *McAfee** *Norman** *Trend Micro**

*: 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

---

[6] http://www.av-comparatives.org/comparativesreviews/main-tests/summary-reports
[7] As those products are included in our yearly public test-series, they are listed even if those vendors decided to do not get included (read more on page 5 of this report).

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. (December 2010)

**Every second counts.
Who is attacking you? And how?**

**Even the best AV solution leaves you exposed
to zero-day and custom malware attacks.**

**Get real-time analysis.
No waiting for signature updates.**

validEDGE
www.validedge.com

*ValidEdge Malware Analysis Appliances
Free 30-day evaluation.*

DETECT   ANALYZE   HEAL