



Anti-Virus Comparative No.8

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

Date: November 2005 (2005-11)

Last revision: 28th November 2005

Author: Andreas Clementi

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

1. Introduction

This test can be seen as the continuation of the August 2005 test. The same products were used and the results show the pure proactive detection capabilities that the products had three months ago. 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. Without this ability the user has to wait for an updated release of the Anti-Virus product. 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. The same products, with the same best possible settings that the scan engines had in the last comparative, were used to make this test. For this test we used new samples received between 5th August and 5th November 2005, which were all new to any tested product.

The following 11 products were tested in this comparative (last signature updates and versions are from 5th August 2005):

Avast! 4.5.561 Professional Edition
AVG Professional 7.0.302
BitDefender Anti-Virus 8.0.137 Professional Plus
Dr.Web Anti-Virus for Windows 95-XP 4.32b
ESET NOD32 2.12.3
F-Prot Anti-Virus for Windows 3.16a
H+B EDV AntiVir Professional Edition 6.29.00.03
Kaspersky Anti-Virus Personal 5.0.227
McAfee VirusScan 9.0.10
Symantec Norton Anti-Virus 11.0.1.3b
Trend Micro Internet Security 12.1.1014

2. Description

The test-set consists of two categories:

- ITW-samples: new samples that appeared 'in-the-wild' according to the Wildlist, between the 5th August and the 1st October.
- New zoo-samples: all new zoo-samples that were classified to be new/unknown to all tested Anti-Virus products. This category is split into subcategories by virus/malware type. Results of this category show the pure proactive detection capability.

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/unknown 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 most of the 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 maybe had the ability to detect new samples, e.g. on-access or by other monitoring tools, like behaviour-blocker, etc.

3. Used ITW-samples

We used the 'In-The-Wild' samples listed on the main list of the International Wildlist (www.wildlist.org) that appeared during the period between the 5th August 2005 and the 1st October 2005, which were new to all tested products (marked in red). Because this year no ITW list was delivered for the month of August and because at the time of testing there was still no October Wildlist available¹, we had to use only the ITW-list additions of the month of September. The other samples were already around before (as Zoo-samples) and all were already included in the test of August 2005. This is a simple example to also show that the detection of so called Zoo-Samples is important. It is probably true that part of all zoo-samples exists only in anti-virus labs, as they were submitted directly from the virus authors to them. However it is also true that samples which were submitted from users that were actually infected by virus/malware that was not so wide-spread, are not on the official International Wildlist - They are also called Zoo-samples. Detection rates of 100% of samples that are on the official Wildlist, is a must and every Anti-Virus should be able to detect them. Detection of non-ITW-samples (Zoo-samples) is also important to users (as it is also possible to get infected by such threats) that Anti-Virus software detects them. Of course, detection rates of 100% of Zoo-samples are not really possible. In the case of ITW-samples, it is possible, as the Anti-Virus companies know those samples on the Wildlist already and usually have enough time to detect them before tests are done using them.

ITW-List additions September 2005:

W32/Agobot!ITW#347,	W32/Bagle.BW-mm,	W32/Bagle.DM-mm,
W32/Bagle.DN-mm,	W32/Bagle.DQ-mm,	W32/Bobax.AH,
W32/Cissi.B-mm,	W32/Eyevog.J,	W32/Mytob!ITW#117,
W32/Mytob!ITW#133,	W32/Mytob!ITW#140,	W32/Mytob!ITW#152,
W32/Mytob!ITW#175,	W32/Mytob!ITW#178,	W32/Mytob!ITW#183,
W32/Mytob!ITW#233,	W32/Mytob!ITW#234,	W32/Mytob!ITW#236,
W32/Mytob!ITW#237,	W32/Mytob!ITW#238,	W32/Mytob!ITW#239,
W32/Mytob!ITW#240,	W32/Mytob!ITW#241,	W32/Mytob!ITW#242,
W32/Mytob!ITW#244,	W32/Mytob!ITW#246,	W32/Mytob!ITW#248,
W32/Mytob!ITW#251,	W32/Mytob!ITW#252,	W32/Mytob!ITW#253,
W32/Mytob!ITW#254,	W32/Mytob!ITW#255,	W32/Mytob!ITW#256,
W32/Mytob!ITW#257,	W32/Mytob!ITW#261,	W32/Mytob!ITW#265,
W32/Mytob!ITW#267,	W32/Mytob!ITW#268,	W32/Mytob!ITW#273,
W32/Mytob!ITW#281,	W32/Mytob!ITW#282,	W32/Mytob!ITW#284,
W32/Mytob!ITW#285,	W32/Mytob!ITW#287,	W32/Mytob!ITW#288,
W32/Mytob!ITW#292,	W32/Poebot!1B31,	W32/Rants.B,
W32/Rbot!ITW#1191,	W32/Reatle.A-mm,	W32/Reatle.B-mm,
W32/Reatle.F,	W32/Sdbot!ITW#1253,	W32/Sober.Q-mm,
W32/Yaha.Q-mm.		

As the Wildlist additions of the September Wildlist contained only some few new samples that appeared after the 5th August, the results of the ITW category is this time not so meaningful like it was in the previous retrospective test of May 2005.

¹ We would like to put the attention of the readers to this paper about the Wildlist: <http://www.people.frisk-software.com/~bontchev/papers/wildlist.html>

4. Test results

Company	H+BEDV Datentechnik		Alwil Software		GriSoft		Softwin		
Product	AntiVir Workstation		Avast! Prof.		AVG Professional		BitDefender Prof.+		
Program version	6.31.00.03		4.6.691		7.0.338		8.0.200		
Engine / signature version	6.31.1.0 / 6.31.1.62		0531-4		267.10.1.64		7.02560		
Signature date (mm/dd/yyyy)	08/05/2005		08/05/2005		08/04/2005		08/05/2005		
Number of virus records	202.710		unknown		unknown		198.395		
Certification level reached in this test:	STANDARD		STANDARD				ADVANCED+		
<i>ProActive detection of ITW-samples*</i>									
<i>In-The-Wild samples</i>	8	1	13%	0	0%	0	0%	2	25%
ProActive detection of "NEW" zoo-samples**									
DOS viruses	10	1	10%	1	10%	3	30%	4	40%
Windows viruses	34	1	3%	1	3%	3	9%	10	29%
Macro viruses	8	8	100%	1	13%	1	13%	6	75%
Script viruses	44	6	14%	1	2%	0	0%	17	39%
Worms	590	107	18%	63	11%	29	5%	244	41%
Backdoors	3.921	649	17%	888	23%	260	7%	2.429	62%
Trojans	3.179	356	11%	180	6%	48	2%	1.116	35%
other malware	66	4	6%	5	8%	3	5%	14	21%
OtherOS malware	28	2	7%	0	0%	0	0%	1	4%
TOTAL	7.880	1.134	14%	1.140	14%	347	4%	3.841	49%

Company	Doctor Web		Frisk Software		Trend Micro		Kaspersky Labs		
Product	Dr. Web		F-Prot Anti-Virus		Internet Security		KAV Personal Pro		
Program version	4.32b		3.16c		12.1.1034		5.0.372		
Engine / signature version	4.32b		3.16.6		7.510.1002 / 2.761.00		N/A		
Signature date (mm/dd/yyyy)	08/05/2005		08/05/2005		08/04/2005		08/05/2005		
Number of virus records	82.894		191.534		unknown		142.285		
Certification level reached in this test:	ADVANCED		STANDARD		STANDARD		ADVANCED		
<i>ProActive detection of ITW-samples*</i>									
<i>In-The-Wild samples</i>	8	1	13%	0	0%	0	0%	0	0%
ProActive detection of "NEW" zoo-samples**									
DOS viruses	10	0	0%	3	30%	0	0%	0	0%
Windows viruses	34	8	24%	10	29%	0	0%	4	12%
Macro viruses	8	5	63%	7	88%	0	0%	0	0%
Script viruses	44	21	48%	0	0%	0	0%	6	14%
Worms	590	111	19%	124	21%	62	11%	95	16%
Backdoors	3.921	1.277	33%	878	22%	1.346	34%	2.111	54%
Trojans	3.179	514	16%	318	10%	69	2%	291	9%
other malware	66	5	8%	3	5%	1	2%	1	2%
OtherOS malware	28	0	0%	0	0%	0	0%	0	0%
TOTAL	7.880	1.941	25%	1.343	17%	1.478	19%	2.508	32%

Company	McAfee		ESET		Symantec		
Product	McAfee VirusScan		NOD32 Anti-Virus		Horton Anti-Virus		
Program version	10.0.21		2.51.8		11.0.11.4		
Engine / signature version	4.4.00 / 4551		1.1187		70805q		
Signature date (mm/dd/yyyy)	08/05/2005		08/05/2005		08/05/2005		
Number of virus records	141.156		unknown		70.431		
Certification level reached in this test:	ADVANCED		ADVANCED+		STANDARD		
<i>ProActive detection of ITW-samples*</i>							
<i>In-The-Wild samples</i>	8	1	13%	4	50%	0	0%
ProActive detection of "NEW" zoo-samples**							
DOS viruses	10	1	10%	3	30%	3	30%
Windows viruses	34	11	32%	13	38%	9	26%
Macro viruses	8	5	63%	4	50%	1	13%
Script viruses	44	16	36%	0	0%	4	9%
Worms	590	189	32%	382	65%	78	13%
Backdoors	3.921	1.712	44%	2.835	72%	531	14%
Trojans	3.179	770	24%	1.628	51%	208	7%
other malware	66	26	39%	8	12%	2	3%
OtherOS malware	28	4	14%	0	0%	1	4%
TOTAL	7.880	2.734	35%	4.873	62%	837	11%

Please also have a look at the overviews that can be found on the website, to see how the scanners scored in this, and in past, tests. Note: Always check for the latest data available on our website - the previous data of e.g. 6 months ago can now be considered outdated.

5. Summary results

Below are the results obtained by each scanner in the various categories, sorted by detection rate:

(a) ProActive detection of new ITW-samples:

1.	NOD32	50%
2.	BitDefender	25%
3.	McAfee, Dr.Web, H+BEDV	13%
4.	all the others	0%

(b) ProActive detection of new Backdoors, Trojans and other malware:

1.	NOD32	62%
2.	BitDefender	50%
3.	McAfee	35%
4.	Kaspersky	34%
5.	Dr.Web	25%
6.	TrendMicro	20%
7.	F-Prot	17%
8.	Avast	15%
9.	H+BEDV	14%
10.	Symantec	10%
11.	AVG	4%

(c) ProActive detection of new DOS, Windows and OtherOS viruses/malware, Worms, Macro and Script viruses/malware:

1.	NOD32	56%
2.	BitDefender	39%
3.	McAfee	31%
4.	Dr.Web, F-Prot	20%
5.	H+BEDV	17%
6.	Kaspersky	15%
7.	Symantec	13%
8.	Avast, TrendMicro	9%
9.	AVG	5%

(d) ProActive detection of all new samples used in the test:

1.	NOD32	62%	ADVANCED+
2.	BitDefender	49%	ADVANCED+
3.	McAfee	35%	ADVANCED
4.	Kaspersky	32%	ADVANCED
5.	Dr.Web	25%	ADVANCED
6.	TrendMicro	19%	STANDARD
7.	F-Prot	17%	STANDARD
8.	Avast, H+BEDV	14%	STANDARD
9.	Symantec	11%	STANDARD
10.	AVG	4%	-----

The results show the pure proactive detection capabilities of the scan engines. The Percentages are rounded to the nearest whole number. Do not take the results as absolute - they just give an idea of who detected more, and who less, in this specific test. To know how the anti-virus performs 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 a selection of very good scanners and if any of them are used and kept up-to-date, users can feel safe with any of them. Read more in the previous August 2005 comparative.

6. Copyright and Disclaimer

This publication is Copyright (c) 2005 by Andreas Clementi, Austria. Any use of the results, etc. in whole or in parts, is ONLY permitted after explicit written agreement of Andreas Clementi, prior to any publication. We can not be held liable for any damage or loss which might occur as a 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 a liability for the correctness of the test results can not be taken by Andreas Clementi. We do not give any guarantee for the correctness, completeness, etc. 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 site and co-related data.

Andreas Clementi, Austria (November 2005)