Anti-Virus Comparative No.6

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

Date: May 2005 (2005-05)

Last revision of this report: 20th May 2005

Author: Andreas Clementi

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

1. Introduction

This test can be seen as the continuation of the February 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 6th February and 6th May 2005, which were all new to any tested product.

The following 13 products were tested in this comparative (last signature updates and versions are from 6th February 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
GeCAD Reliable Anti-Virus (RAV) 8.6.105
Sophos Anti-Virus 3.90.0
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 6th February and the 1st April.
- 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 International Wildlist[1] that appeared during the period between the 6th February 2005 and the 1st April 2005, which were new to all tested products (marked in red). The other samples were already around before (as ZOO-samples) and all were already included in the test of February 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 February 2005:

W32/Agobot!0153, **W32/Agobot!4A55**, W32/Agobot!6074, W32/Agobot!639F, W32/Agobot!87D1, **W32/Agobot!911C**, **W32/Agobot!ECE2**, W32/Bobax.N, W32/Bropia.D, W32/Bropia.G, W32/Bropia.Q, **W32/Inforyou-mm**, **W32/Mydoom.BA-mm**, **W32/Mydoom.BB-mm**, **W32/Mytob.A-mm**, W32/Rbot!1861, **W32/Rbot!226B**, W32/Rbot!BAD8, W32/Rbot!D767, W32/Rbot!E63D, W32/Sdbot!0F31, W32/Sdbot!8B15, **W32/Sober.K-mm**, W32/Wootbot!9A62.

ITW-List additions March 2005:

W32/Agobot!7F71, **W32/Agobot!C58D**, **W32/Agobot!9E9A**, W32/Bagle.AY-mm, **W32/Bagle.BN-mm**, **W32/Bagle.BO-mm**, **W32/Bagle.BP-mm**, **W32/Bropia.N**, **W32/Mydoom.BH-mm**, W32/Mydoom.BE-mm[2], **W32/Myfip.T**, **W32/Mytob.AC-mm**, **W32/Mytob.B-mm**, **W32/Mytob.C-mm**, **W32/Mytob.D-mm**, **W32/Mytob.E-mm**, **W32/Mytob.F-mm**, **W32/Mytob.G-mm**, **W32/Mytob.J-mm**, **W32/Mytob.K-mm**, **W32/Mytob.L-mm**, **W32/Mytob.M-mm**, **W32/Mytob.N-mm**, **W32/Mytob.O-mm**, **W32/Mytob.P-mm**, **W32/Mytob.Q-mm**, **W32/Mytob.R-mm**, W32/Mywife.F-mm, W32/Rbot!26F7, **W32/Rbot!683E**, **W32/Sdbot!BBB5**, W32/Sdbot!5DE5, **W32/Sdbot!5229**, W32/Sdbot!DF56, W32/Sdbot!5F74, W32/Sdbot!8A01, W32/Sdbot!6DE1, W32/Sdbot!CBDE, W32/Sdbot!D906, **W32/Sdbot!ADA4**, W32/Sdbot!D9D3, W32/Sdbot!3D3C, W32/Sdbot!35C6, W32/Sdbot!49C9, **W32/Sdbot!D3EF**, **W32/Sdbot!B386**, W32/Sdbot!443C, W32/Sdbot!521F, W32/Sdbot!9C87, W32/Sdbot!DCB6, W32/Sdbot!B66A, **W32/Sdbot!A379**, **W32/Sdbot!9679**, **W32/Sdbot!AF33**, **W32/Sdbot!D7F4**, **W32/Sdbot!6FEA**, W32/Sdbot!2859, **W32/Serflog**, **W32/Sober.L-mm**, **W32/Sober.M-mm**, W32/Spybot!56FD.

[1] The WildList Organization International www.wildlist.org

[2] This sample was not in the official WildCore collection, so we could not include it.

4. Test results

Company		H+BEDV Datentechnik		Alwil Software		GriSoft		Softwin		Doctor Web	
Product		**AntiVir Prof.**		**Avast! Prof.**		**AVG Professional**		**BitDefender Prof.+**		**Dr. Web**	
Program version		6.29.00.03		4.5.561		7.0.302		8.0.137		4.32b	
Engine / signature version		6.29.0.107		0505-2		265.8.5		7.00442		4.32b	
Signature date (mm/dd/yyyy)		02/06/2005		02/05/2005		02/03/2005		02/06/2005		02/06/2005	
Number of virus records		97.143		*unknown*		*unknown*		99.503		64.738	
ProActive detection of ITW-samples*											
In-The-Wild samples	51	0	0%	2	4%	0	0%	35	69%	18	35%
ProActive detection of "NEW" zoo-samples**											
DOS viruses	7	0	0%	0	0%	0	0%	0	0%	0	0%
Windows viruses	50	6	12%	4	8%	0	0%	6	12%	5	10%
Macro viruses	3	3	100%	0	0%	0	0%	3	100%	3	100%
Script viruses	23	0	0%	0	0%	1	4%	5	22%	3	13%
Worms	693	89	13%	57	8%	13	2%	310	45%	107	15%
Backdoors	5.416	726	13%	735	14%	293	5%	3.478	64%	2.867	53%
Trojans	1.976	172	9%	72	4%	4	0%	278	14%	74	4%
other malware	50	0	0%	2	4%	1	2%	5	10%	3	6%
OtherOS malware	41	1	2%	0	0%	0	0%	0	0%	0	0%
TOTAL	**8.259**	997	**12%**	870	**11%**	312	**4%**	4.085	**49%**	3.062	**37%**

Company		Frisk Software		Trend Micro		Kaspersky Labs		McAfee	
Product		**F-Prot Anti-Virus**		**Internet Security**		**KAV Personal**		**McAfee VirusScan**	
Program version		3.16a		12.1.1014		5.0.227		9.0.10	
Engine / signature version		3.16.2		7.500.1001 / 2.394.00		*N/A*		4.4.00 / 4426	
Signature date (mm/dd/yyyy)		02/05/2005		02/05/2005		02/06/2005		02/03/2005	
Number of virus records		148.895		*unknown*		117.316		115.035	
ProActive detection of ITW-samples*									
In-The-Wild samples	51	10	20%	6	12%	18	35%	11	22%
ProActive detection of "NEW" zoo-samples**									
DOS viruses	7	0	0%	0	0%	6	86%	0	0%
Windows viruses	50	10	20%	4	8%	6	12%	4	8%
Macro viruses	3	3	100%	3	100%	0	0%	3	100%
Script viruses	23	0	0%	0	0%	4	17%	9	39%
Worms	693	141	20%	56	8%	86	12%	202	29%
Backdoors	5.416	1.216	22%	1.074	20%	3.791	70%	1.874	35%
Trojans	1.976	170	9%	63	3%	107	5%	377	19%
other malware	50	1	2%	0	0%	0	0%	4	8%
OtherOS malware	41	0	0%	0	0%	0	0%	8	20%
TOTAL	**8.259**	1.541	**19%**	1.200	**15%**	4.000	**48%**	2.481	**30%**

Company		ESET		Symantec		GeCAD Software		Sophos	
Product		**NOD32 Anti-Virus**		**Norton Anti-Virus**		**RAV Desktop**		**Sophos Anti-Virus**	
Program version		2.12.3		11.0.1.3b		8.6.105		3.90.0	
Engine / signature version		1.992		70206d		8.11		2.28.3	
Signature date (mm/dd/yyyy)		02/05/2005		02/06/2005		02/02/2005		02/05/2005	
Number of virus records		*unknown*		69.976		111.964		100.050	
ProActive detection of ITW-samples*									
In-The-Wild samples	51	46	90%	4	8%	1	2%	19	37%
ProActive detection of "NEW" zoo-samples**									
DOS viruses	7	0	0%	0	0%	0	0%	0	0%
Windows viruses	50	16	32%	9	18%	0	0%	0	0%
Macro viruses	3	3	100%	0	0%	0	0%	0	0%
Script viruses	23	0	0%	2	9%	0	0%	0	0%
Worms	693	484	70%	71	10%	71	10%	61	9%
Backdoors	5.416	4.726	87%	1.033	19%	600	11%	2.729	50%
Trojans	1.976	550	28%	55	3%	17	1%	21	1%
other malware	50	5	10%	2	4%	2	4%	0	0%
OtherOS malware	41	0	0%	1	2%	0	0%	0	0%
TOTAL	**8.259**	5.784	**70%**	1.173	**14%**	690	**8%**	2.811	**34%**

Based on the numbers in the tables, we see that nowadays the main threats are Backdoors and the various Botgens, followed by Trojans and worms. The Spyware/adware problem is also growing, but this was not included in this test-set. The proactive security provided by most of the scanners improved significantly since last year.

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 rely to the latest available data on our website – the previous data of e.g. last year can now be considered as outdated.

5. Summary results

Below are the results reached by each scanner on various categories, sorted by detection rate:

(a) ProActive detection of new ITW-samples:

1.	NOD32	90%
2.	BitDefender	69%
3.	Sophos	37%
4.	Kaspersky, Dr.Web	35%
5.	McAfee	22%
6.	F-Prot	20%
7.	TrendMicro	12%
8.	Symantec	8%
9.	Avast	4%
10.	RAV	2%
11.	H+BEDV, AVG	0%

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

1.	NOD32	71%
2.	Kaspersky	52%
3.	BitDefender	51%
4.	Dr.Web	40%
5.	Sophos	37%
6.	McAfee	30%
7.	F-Prot	19%
8.	TrendMicro, Symantec	15%
9.	H+BEDV	12%
10.	Avast	11%
11.	RAV	8%
12.	AVG	4%

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

1.	NOD32	62%
2.	BitDefender	40%
3.	McAfee	28%
4.	F-Prot	19%
5.	Dr.Web	14%
6.	Kaspersky, H+BEDV	12%
7.	Symantec	10%
8.	RAV	9%
9.	TrendMicro	8%
10.	Sophos, Avast	7%
11.	AVG	2%

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

1.	NOD32	70%	ADVANCED+
2.	BitDefender	49%	ADVANCED+
3.	Kaspersky	48%	ADVANCED+
4.	Dr.Web	37%	ADVANCED
5.	Sophos	34%	ADVANCED
6.	McAfee	30%	ADVANCED
7.	F-Prot	19%	STANDARD
8.	TrendMicro	15%	STANDARD
9.	Symantec	14%	STANDARD
10.	H+BEDV	12%	STANDARD
11.	Avast	11%	STANDARD
12.	RAV	8%	STANDARD
13.	AVG	4%	--------

The results show the pure proactive detection capabilities of the scan engines. The percentages are rounded to rough numbers. 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 to our on-demand tests of February and August. Readers should take a look to 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.

6. Copyright and Disclaimer

Andreas Clementi, Austria (May 2005)