Anti-Virus Comparative No.4

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

Date: November 2004 (2004-11)

Last revision of this report: 1st December 2004

Author: Andreas Clementi

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

1. Introduction

This test can be seen as the continuation of the last test (August 2004). 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 or heuristic techniques. Without this ability the user has to wait for an updated release of the Anti-Virus product. 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 August and 6th November 2004, 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 August 2004):
Avast! 4.1.418 Professional Edition
BitDefender Anti-Virus 7.2 Professional Edition
Dr.Web Anti-Virus for Windows 95-XP 4.31b
ESET NOD32 2.000.9
F-Prot Anti-Virus for Windows 3.15
H+B EDV AntiVir Professional Edition 6.26.01.01
Kaspersky Anti-Virus Personal 5.0.142
McAfee VirusScan Professional 8.0.41
Panda Platinum Internet Security 8.05.00
Symantec Norton Anti-Virus 10.0.1.13
GeCAD Reliable Anti-Virus (RAV) 8.6.105
Sophos Anti-Virus 3.84
Trend Micro Internet Security 11.31

2. Description

In this test, only two main categories were included, as too many old samples were received, which wouldn't deliver reliable results.
The two categories were:

- ITW-samples: new, ITW-samples that appeared 'in-the-wild' according to the Wildlist, between the 6th August and the 6th 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. 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 August 2004 and the 6th October[2] 2004, which were new to all tested products (marked in red). The other samples were already around before (as ZOO-samples) and nearly all were already included in the test of August 2004. 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 (usually some months before, as the WildCore collection is delivered with some delay).

ITW-List additions August 2004:
W32/Agobot!6928, W32/Atak.A-mm, **W32/Bagle.AQ-mm**, W32/Evaman.C-mm, W32/Korgo.AB, W32/Korgo.AC, W32/Korgo.Z, W32/Lovgate.AI-mm, W32/Mydoom.R-mm, **W32/Mydoom.S-mm**, **W32/Mywife.C-mm**, W32/Rbot!0628, W32/Rbot!8B6C, **W32/Sasser.G**, W32/Sdbot!0976, W32/Sdbot!63ED, W32/Sdbot!B507, W32/Sdbot!FFC4, W32/Zindos.

ITW-List additions September 2004:
W32/Bagle.AZ-mm, W32/Korgo.T, W32/Korgo.V, **W32/Mydoom.T-mm**, **W32/Neveg.C-mm**, W32/Rbot!CCC2, W32/Sdbot!6067, **W32/Spybot!E11E**.

ITW-List additions October 2004:
As noted above, the International Wildlist Organization does deliver the Wildlist with some delay. Today is December 1st 2004 and on the Wildlist website there is still only the Wildlist of September 2004. Also, the so called "Real-Time Wildlist" is just a copy of the September Wildlist. For this reason, we will no longer wait for the release of the October 2004 Wildlist, as we want to deliver this test report within our predefined time lines. We hope that in the future the Wildlist Organization will put even more efforts to deliver the monthly Wildlist in a more timely manner.

[1] The WildList Organization International www.wildlist.org
[2] Due to the delay of the official October Wildlist, we had to use a 2 month period for the ITW-samples instead of the planned 3 month period.

4. Test results

Developer		H+BEDV Datentechnik			Alwil Software			Softwin			DialogueScience			Frisk Software		
Product name		**AntiVir Professional**			**Avast! Professional**			**BitDefender Prof.**			**Dr. Web**			**F-Prot**		
Program version		6.26.01.01			4.1.418			7.2.0.0			4.31b			3.15		
Version of engine / signature		6.26.0.10			0432-2			*N/A*			4.30.0			3.15.1		
Date of signature		08/06/2004			08/04/2004			08/06/2004			08/06/2004			08/06/2004		
Number of virus records		88.519			*N/A*			88.298			52.998			122.919		
ProActive detection of ITW-samples*																
In-The-Wild samples	8	1	13%		0	0%		2	25%		1	13%		0	0%	
ProActive detection of "NEW" zoo-samples**																
DOS viruses	18	0	0%		0	0%		14	78%		17	94%		3	17%	
Windows viruses	152	22	14%		5	3%		15	10%		28	18%		41	27%	
Macro viruses	8	1	13%		0	0%		1	13%		2	25%		1	13%	
Script viruses	152	6	4%		6	4%		20	13%		91	60%		1	1%	
Worms	381	114	30%		17	4%		140	37%		94	25%		28	7%	
Backdoors	3.704	445	12%		454	12%		1.874	51%		1.677	45%		413	11%	
Trojans	1.514	146	10%		16	1%		97	6%		36	2%		64	4%	
other malware	88	0	0%		1	1%		5	6%		0	0%		0	0%	
OtherOS malware	128	0	0%		0	0%		0	0%		0	0%		0	0%	
TOTAL	6.145	734	12%		499	8%		2.166	35%		1.945	32%		551	9%	

Developer		Trend Micro			Kaspersky Labs			McAfee			ESET		
Product name		**Internet Security**			**KAV Personal**			**McAfee VirusScan**			**NOD32 Anti-Virus**		
Program version		11.31			5.0.142			8.0.41			2.000.9		
Version of engine / signature		7.100 (951)			*N/A*			4.3.20 / 4383			1.835		
Date of signature		08/04/2004			08/06/2004			08/04/2004			08/06/2004		
Number of virus records		*N/A*			98.958			95.958			*N/A*		
ProActive detection of ITW-samples*													
In-The-Wild samples	8	0	0%		2	25%		0	0%		8	100%	
ProActive detection of "NEW" zoo-samples**													
DOS viruses	18	0	0%		14	78%		0	0%		8	44%	
Windows viruses	152	3	2%		30	20%		45	30%		75	49%	
Macro viruses	8	0	0%		1	13%		0	0%		0	0%	
Script viruses	152	3	2%		22	14%		38	25%		7	5%	
Worms	381	16	4%		91	24%		113	30%		237	62%	
Backdoors	3.704	236	6%		2.373	64%		1.335	36%		2.492	67%	
Trojans	1.514	0	0%		94	6%		211	14%		156	10%	
other malware	88	0	0%		1	1%		8	9%		7	8%	
OtherOS malware	128	0	0%		0	0%		9	7%		0	0%	
TOTAL	6.145	258	4%		2.626	43%		1.759	29%		2.982	49%	

Developer		Symantec			Panda Software			GeCAD Software			Sophos		
Product name		**Norton Anti-Virus**			**Panda Platinum IS**			**RAV Desktop**			**Sophos Anti-Virus**		
Program version		10.0.1.13			8.05.00			8.6.105			3.78		
Version of engine / signature		60804ah			*N/A*			8.11			2.20		
Date of signature		08/04/2004			08/06/2004			08/05/2004			08/06/2004		
Number of virus records		67.916			81.569			103.044			92.776		
ProActive detection of ITW-samples*													
In-The-Wild samples	8	0	0%		0	0%		0	0%		0	0%	
ProActive detection of "NEW" zoo-samples**													
DOS viruses	18	5	28%		5	28%		0	0%		0	0%	
Windows viruses	152	35	23%		47	31%		21	14%		0	0%	
Macro viruses	8	0	0%		0	0%		0	0%		0	0%	
Script viruses	152	13	9%		22	14%		14	9%		3	2%	
Worms	381	71	19%		60	16%		37	10%		28	7%	
Backdoors	3.704	961	26%		1.105	30%		422	11%		735	20%	
Trojans	1.514	88	6%		74	5%		11	1%		9	1%	
other malware	88	2	2%		2	2%		3	3%		1	1%	
OtherOS malware	128	1	1%		0	0%		0	0%		0	0%	
TOTAL	6.145	1.176	19%		1.315	21%		508	8%		776	13%	

Based on the numbers we see in the tables, we can see that nowadays the main threats are not coming from worms, as in recent years, but that there is a bigger danger coming from Backdoors and Botgens, like RBots, Agobots, SdBots, etc.

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.

5. Summary results

Below are the results reached by each scanner on various categories, sorted by detection rate over the samples that appeared in a 3-month time period and were new/unknown to any of the tested products:

(a) ProActive detection of new ITW-samples:

1.	NOD32	100%
2.	BitDefender, Kaspersky	25%
3.	Dr.Web, H+BEDV	13%
4.	all the others	0%

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

1.	NOD32	50%
2.	Kaspersky	47%
3.	BitDefender	37%
4.	Dr.Web	32%
5.	McAfee	30%
6.	Panda	22%
7.	Symantec	20%
8.	Sophos	14%
9.	H+BEDV	11%
10.	F-Prot, Avast	9%
11.	RAV	8%
12.	TrendMicro	4%

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

1.	NOD32	39%
2.	Dr.Web	28%
3.	McAfee	24%
4.	BitDefender	23%
5.	Kaspersky	19%
6.	H+BEDV	17%
7.	Panda	16%
8.	Symantec	15%
9.	F-Prot, RAV	9%
10.	Sophos	4%
11.	Avast, TrendMicro	3%

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

1.	NOD32	49%	ADVANCED+
2.	Kaspersky	43%	ADVANCED+
3.	BitDefender	35%	ADVANCED+
4.	Dr.Web	32%	ADVANCED+
5.	McAfee	29%	ADVANCED+
6.	Panda	21%	ADVANCED
7.	Symantec	19%	ADVANCED
8.	Sophos	13%	STANDARD
9.	H+BEDV	12%	STANDARD
10.	F-Prot	9%	STANDARD
11.	RAV, Avast	8%	STANDARD
12.	TrendMicro	4%	--------

The categories (a), (b), (c) and (d) show the detection rates over samples that were unknown to ANY tested product. The results show the pure proactive detection capabilities of the scan engines.

Do not take the results as absolute - they just give an idea of who detected more, and who less, in this specific test. Percentages in our retrospective tests will always contain only rough numbers. We will no longer provide a ranking system. 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 (November 2004)