AV
comparatives

Anti-Virus Comparative No.3

a) On-demand detection of virus/malware
b) On-demand detection of dialers

Date: August 2004 (2004-08)

Last revision of this report: 25. October 2004

Author: Andreas Clementi

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

1. Conditions in order to participate

a) The scanner must detect 100% of ItW-samples and at least 85% of all zoo-samples.
b) The product must use only (one) own scan engine(s).
c) The scanner must be able to finish the scan of the full database with best possible settings within a reasonable time, without crashing or causing major problems. It must be able to scan a subdirectory tree and it should be able to scan files with extensions defined by the tester.
d) The scanner should not move or change in any way the files or system during the scan when running in report-only mode. The scanner should create a report file on the fly. If no report file is created, the scanner will be run in delete-mode and no report file will be delivered for that product.
e) In order to be tested over dialers, the scanner must detect on-demand at least 10% of Dialers.
f) For the tests we use the best possible settings in accordance with the producers. If a switch produces too many false alarms so that it would be senseless to use it, a lower switch will be used.
g) Participating Antivirus companies sending samples for the test are allowed to receive all missed samples in the case they agree to send their samples to other submitting companies also. Participating Antivirus companies that do not send samples for the test will receive not more than 2.500 new samples. This is done under request of the companies submitting samples. Companies that will from now on submit their collections will have to agree to allow me to send the missed samples to the other companies that share their samples too.
h) Participating companies have to agree to participate without any complaint about the results or the used test methods.
i) Participating companies that does any kind of fooling (e.g. md5-signatures on replicating malware) or illegal/unethical practices will be excluded from future tests. On purpose and/or human errors that may lead to wrong test results will be considered fooling.
j) Any company being tested in the comparatives that is found sending samples to persons not working for an antivirus company (magazine reporters, virus collectors, ...) will be excluded from tests forever. Any company that is not being tested but that is found in the same situation will not be included in the comparatives ever.
k) We keep the right to change the conditions at any time and to add new products to the test or exclude products included in the test. New candidates for the test must additionally be accepted by the already participating companies before they can be included in our tests. If the majority (half antivirus companies + 1) don’t accept a company, it will be not included in the tests.

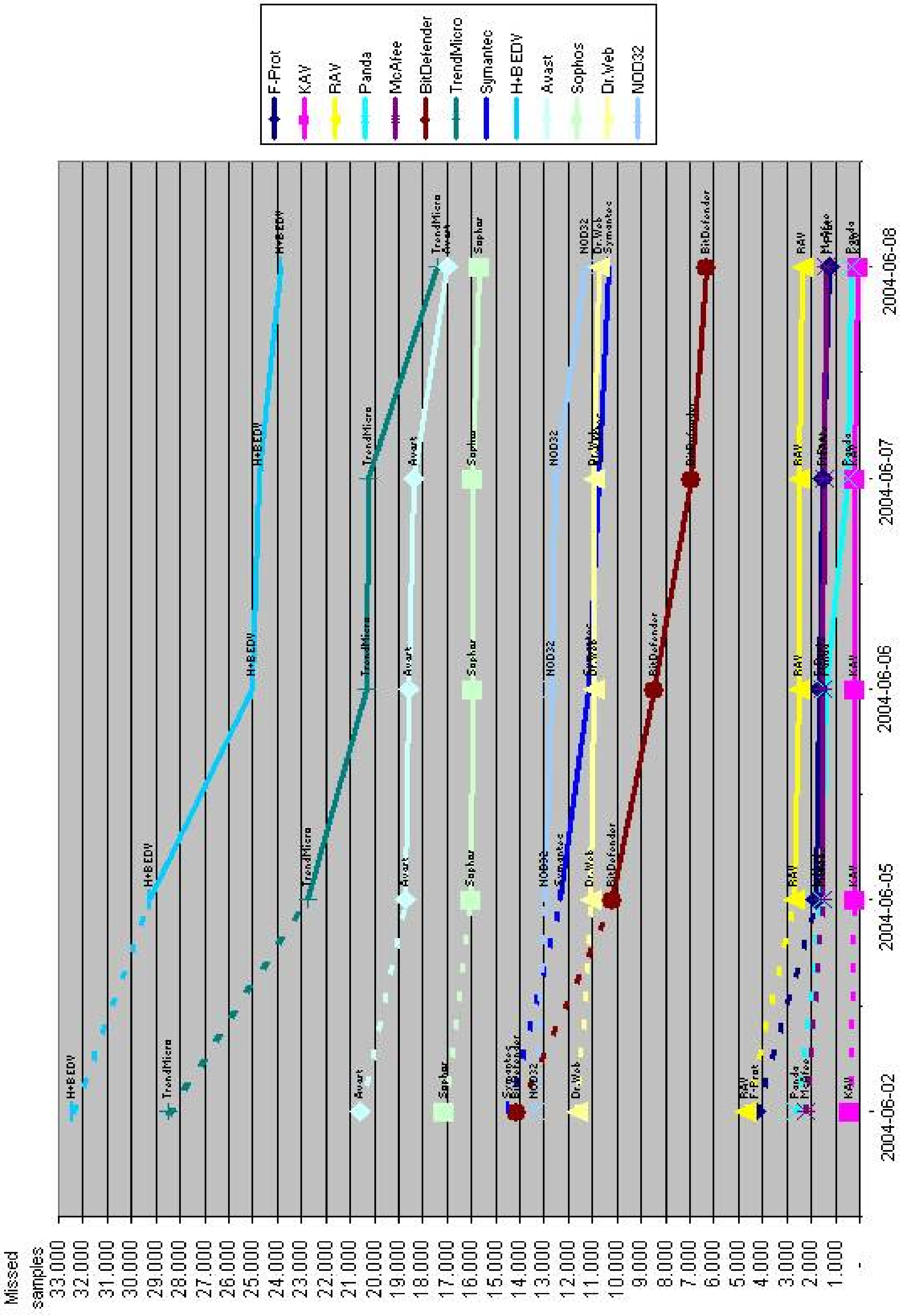
2. Tested products

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

Product submission deadline was 1st August 2004. All products were updated with the last official updates that were available the 6th August 2004. Test-beds were frozen the 4th August 2004.

3. **Progresses made since last comparative**

All participating companies received the samples that their product did not detect in the comparative of February 2004 (Dialers and unwanted samples excluded). Below you see how many of their missed samples were detected/added after 3, 4, 5 and 6 months by the respective companies.



4. Test results

Company		H+BEDV Datentechnik		Alwil Software		Softwin		DialogueScience		Frisk Software	
Product		**AntiVir Prof.**		**Avast! Prof.**		**BitDefender Prof.**		**Dr. Web**		**F-Prot**	
Program version		6.26.01.01		4.1.418		7.2.0.0		4.31b		3.15	
Engine / signature version		6.26.0.10		0432-2		N/A		N/A		3.15.1	
Signature date		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	
On-demand detection of virus/malware											
DOS viruses	218.208	208.854	95,71%	210.884	96,64%	214.207	98,17%	215.532	98,77%	217.830	99,83%
Windows viruses	13.291	10.481	78,86%	12.157	91,47%	12.821	96,46%	12.274	92,35%	12.760	96,00%
Macro viruses	23.198	23.060	99,41%	22.771	98,16%	23.141	99,75%	23.182	99,93%	23.198	100%
Script viruses	6.638	3.300	49,71%	4.160	62,67%	5.246	79,03%	4.958	74,69%	5.596	84,30%
Worms	14.204	11.368	80,03%	11.840	83,36%	13.111	92,30%	12.984	91,41%	13.109	92,29%
Backdoors	24.094	15.160	62,92%	19.826	82,29%	22.467	93,25%	21.944	91,08%	21.703	90,08%
Trojans	18.527	10.521	56,79%	14.549	78,53%	15.413	83,19%	13.207	71,29%	16.144	87,14%
other malware	3.580	1.124	31,40%	2.390	66,76%	2.241	62,60%	1.921	53,66%	2.623	73,27%
OtherOS malware	1.287	374	29,06%	753	58,51%	561	43,59%	588	45,69%	855	66,43%
TOTAL	**323.027**	284.242	**87,99%**	299.330	**92,66%**	309.208	**95,72%**	306.590	**94,91%**	313.818	**97,15%**
Total without DOS & OtherOS	*103.532*	*75.014*	*72,45%*	*87.693*	*84,70%*	*94.440*	*91,22%*	*90.470*	*87,38%*	*95.133*	*91,89%*
On-demand detection of dialers											
Dialers	205.016	204.320	~100%			84.147	41%				

Company		Trend Micro		Kaspersky Labs		Network Associates		ESET	
Product		**Internet Security**		**KAV Personal**		**McAfee VirusScan**		**NOD32 Anti-Virus**	
Program version		11.31		5.0.142		8.0.41		2.000.9	
Engine / signature version		7.100 (951)		N/A		4.3.20 / 4383		1.835	
Signature date		08/04/2004		08/06/2004		08/04/2004		08/06/2004	
Number of virus records		N/A		98.958		95.980		N/A	
On-demand detection of virus/malware									
DOS viruses	218.208	207.570	95,12%	218.139	99,97%	218.180	99,99%	214.955	98,51%
Windows viruses	13.291	11.588	87,19%	13.268	99,83%	13.274	99,87%	12.798	96,29%
Macro viruses	23.198	23.136	99,73%	23.198	100%	23.198	100%	23.138	99,74%
Script viruses	6.638	4.315	65,00%	6.535	98,45%	6.619	99,71%	4.691	70,67%
Worms	14.204	11.679	82,22%	14.178	99,82%	14.182	99,85%	12.984	91,41%
Backdoors	24.094	19.031	78,99%	23.970	99,49%	23.095	95,85%	21.984	91,24%
Trojans	18.527	12.715	68,63%	18.390	99,26%	16.825	90,81%	13.358	72,10%
other malware	3.580	2.137	59,69%	3.580	100%	3.330	93,02%	2.279	63,66%
OtherOS malware	1.287	679	52,76%	1.038	80,65%	1.270	98,68%	571	44,37%
TOTAL	**323.027**	292.850	**90,66%**	322.296	**99,77%**	319.973	**99,05%**	306.758	**94,96%**
Total without DOS & OtherOS	*103.532*	*84.601*	*81,71%*	*103.119*	*99,60%*	*100.523*	*97,09%*	*91.232*	*88,12%*
On-demand detection of dialers									
Dialers	205.016			205.010	~100%	204.984	~100%		

Company		Symantec		Panda Software		GeCAD Software		Sophos	
Product		**Norton Anti-Virus**		**Panda Platinum IS**		**RAV Desktop**		**Sophos Anti-Virus**	
Program version		10.0.1.13		8.05.00		8.6.105		3.84	
Engine / signature version		60804ah		N/A		8.11		2.20	
Signature date		08/04/2004		08/06/2004		08/05/2004		08/06/2004	
Number of virus records		67.916		81.569		103.044		92.776	
On-demand detection of virus/malware									
DOS viruses	218.208	212.966	97,60%	217.608	99,73%	216.924	99,41%	211.881	97,10%
Windows viruses	13.291	13.175	99,13%	12.925	97,25%	12.826	96,50%	12.484	93,93%
Macro viruses	23.198	23.110	99,62%	23.188	99,96%	23.128	99,70%	23.051	99,37%
Script viruses	6.638	5.641	84,98%	6.216	93,64%	5.751	86,64%	4.762	71,74%
Worms	14.204	13.920	98,00%	13.831	97,37%	13.513	95,14%	11.905	83,81%
Backdoors	24.094	22.072	91,61%	23.420	97,20%	21.328	88,52%	17.633	73,18%
Trojans	18.527	14.402	77,74%	17.138	92,50%	16.065	86,71%	12.322	66,51%
other malware	3.580	2.941	82,15%	3.139	87,68%	2.932	81,90%	2.227	62,21%
OtherOS malware	1.287	870	67,60%	997	77,47%	1.064	82,67%	861	66,90%
TOTAL	**323.027**	309.097	**95,69%**	318.462	**98,59%**	313.531	**97,06%**	297.126	**91,98%**
Total without DOS & OtherOS	*103.532*	*95.261*	*92,01%*	*99.857*	*96,45%*	*95.543*	*92,28%*	*84.384*	*81,51%*
On-demand detection of dialers									
Dialers	205.016	141.070	69%	204.876	~100%	204.612	~100%	153.964	75%

Tests were done on a Windows XP Professional SP1 system with this Hardware: 1*Pentium 4 HT 2,8 GHz, 512 MB RAM, 1*40 GB hard disks + 2*120 GB hard disks, DVD-ReWriter.

5. Summary results

Here are the results reached by each scanner on each category, sorted by detection rate.

(a) Results over Windows viruses, Macros, Worms and Scripts detection:

1.	McAfee	99.90%
2.	Kaspersky	99.73%
3.	Panda	97.96%
4.	Symantec	97.41%
5.	RAV	96.31%
6.	F-Prot	95.35%
7.	BitDefender	94.75%
8.	NOD32	93.51%
9.	Dr.Web	93.14%
10.	Sophos	91.05%
11.	Avast	88.83%
12.	TrendMicro	88.47%
13.	H+BEDV	84.09%

(b) Results over Backdoors, Trojans and other malware detection:

1.	Kaspersky	99.44%
2.	Panda	94.58%
3.	McAfee	93.61%
4.	F-Prot	87.60%
5.	RAV	87.28%
6.	BitDefender	86.84%
7.	Symantec	85.31%
8.	NOD32	81.43%
9.	Dr.Web	80.24%
10.	Avast	79.58%
11.	TrendMicro	73.34%
12.	Sophos	69.66%
13.	H+BEDV	58.02%

(c) Results over DOS virus detection:

1.	McAfee	99.99%
2.	Kaspersky	99.97%
3.	F-Prot	99.83%
4.	Panda	99.73%
5.	RAV	99.41%
6.	Dr.Web	98.77%
7.	NOD32	98.51%
8.	BitDefender	98.17%
9.	Symantec	97.60%
10.	Sophos	97.10%
11.	Avast	96.64%
12.	H+BEDV	95.71%
13.	TrendMicro	95.12%

(d) Results over Dialer detection:

1.	McAfee, Kaspersky, Panda, H+BEDV, RAV	~100%
2.	Sophos	75%
3.	Symantec	69%
4.	BitDefender	41%
5.	all the others	< 10%

(e) Results over ‘OtherOS malware’ detection:

1.	McAfee	98.68%
2.	RAV	82.67%
3.	Kaspersky	80.65%
4.	Panda	77.47%
5.	Symantec	67.60%
6.	Sophos	66.90%
7.	F-Prot	66.43%
8.	Avast	58.51%
9.	TrendMicro	52.76%
10.	Dr.Web	45.69%
11.	NOD32	44.37%
12.	BitDefender	43.59%
13.	H+BEDV	29.06%

6. Credits

After each comparative products will receive “credits” based on the rankings reached in each single category (This is mainly just for my curiosity):

	a	b	c	d	e	∑/5
Avast	11	10	11	5	8	9.00
BitDefender	7	6	8	4	8	6.60
Dr.Web	9	9	6	5	10	7.80
F-Prot	6	4	3	5	7	5.00
H+BEDV	13	13	12	1	13	10.40
Kaspersky	2	1	2	1	3	1.80
McAfee	1	3	1	1	1	1.40
NOD32	8	8	7	5	11	7.80
Panda	3	2	4	1	4	2.80
RAV	5	5	5	1	2	3.60
Sophos	10	12	10	2	6	8.00
Symantec	4	7	9	3	5	5.60
TrendMicro	12	11	13	5	9	10.00

All the tested products are already a selection of very good Anti-Virus scan engines. Anyway, based on this test, I would rank the products as follow:

1st place:	McAfee	(1.40)
2nd place:	Kaspersky	(1.80)
3rd place:	Panda	(2.80)
4th place:	RAV	(3.60)
5th place:	F-Prot	(5.00)
6th place:	Symantec	(5.60)
7th place:	BitDefender	(6.60)
8th place:	NOD32	(7.80)
8th place:	Dr.Web	(7.80)
9th place:	Sophos	(8.00)
10th place:	Avast	(9.00)
11th place:	TrendMicro	(10.0)
12th place:	H+BEDV	(10.4)

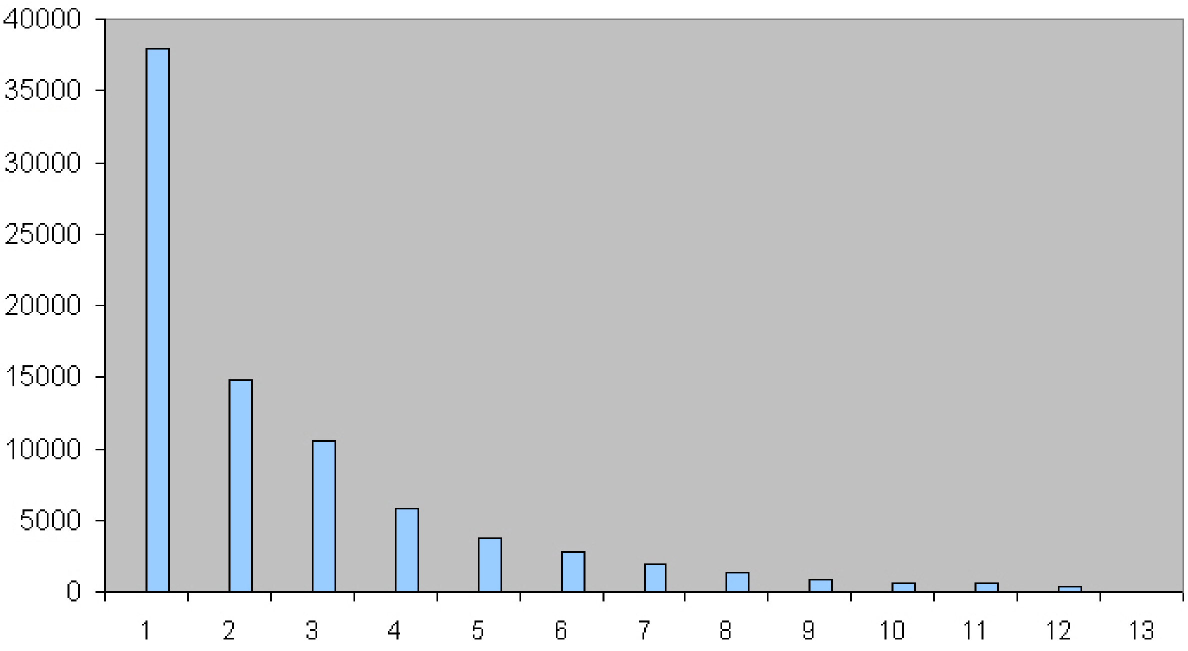
7. Overview / certification

Below you will find an overview of all tests in order to see better the reached levels and to give to the companies one more reason to continue to improve their products (and collaterally reach better results in next tests); it can be understood as some kind of certification.

	February 2004 On-demand test	May 2004 *Retrospective test*	August 2004 On-demand test
Avast!	ADVANCED		STANDARD
BitDefender	ADVANCED	*ADVANCED*	ADVANCED
Dr.Web	ADVANCED	*ADVANCED+*	ADVANCED
F-Prot	ADVANCED+	*STANDARD*	ADVANCED+
H+BEDV	STANDARD		STANDARD
Kaspersky	ADVANCED+	*ADVANCED+*	ADVANCED+
McAfee	ADVANCED+	*ADVANCED+*	ADVANCED+
NOD32	ADVANCED	*ADVANCED+*	ADVANCED
Panda	ADVANCED+	*STANDARD*	ADVANCED+
RAV	ADVANCED+	*STANDARD*	ADVANCED+
Sophos	ADVANCED		STANDARD
Symantec	ADVANCED	*STANDARD*	ADVANCED
TrendMicro	STANDARD	*STANDARD*	STANDARD

8. Non-detected samples in the test-bed of August 2004

About 75% of the test-set is detected by all 13 scanners. At least one scanner does not detect around 25% (~81.300 samples) of the samples. The non-detected samples consist as follow:



This figure shows how many samples are not detected by how many scanners. All samples are detected by at least one scanner.
Examples: around 400 samples are not detected by 12 scanners; one (NOT a single scanner!) of the 13 scanners does detect them.
Around 38.000 samples are detected by 12 scanners and not by one scanner (NOT a single scanner!).

9. Copyright and Disclaimer

This publication is Copyright (c) 2004 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. A liability for the correctness of the results given on the comparatives cannot be taken by the authors. We do not give any guaranty of any kind. We are under no circumstances liable for any consequential damage including but not limited to capital/profit loss or other direct or indirect damage that could arise.

Andreas Clementi, Austria (August 2004)