



Anti-Virus Comparative No.1

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

Shortened version

Date of Test: 6 February 2004 (2004-02)

Author: Andreas Clementi

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

1. Conditions in order to participate

In order to participate to the comparative, products must conform at least to the following main conditions:

- a) The scanner must be able to detect 100% of ItW-samples and at least 85% of all zoo-samples.
- b) The scanner must be able to finish the scan of the full database with best possible settings within a reasonable time (time limit is 36 hours; most scanners do need about 6 hours).
- c) The product must use only (one) own scan engine(s).
- d) The scanner must be able to run without crashing or causing major problems. If it is not possible to make the scanner run, it will/can not be tested.
- e) The scanner must be able to scan files with extensions defined by the tester. Exceptions can be made if the scanner in question is of public interest.
- f) The scanner should not move or change in any way the files or system during the scan when running in report-only mode. If it does, we will run the scanner in delete mode.
- g) The scanner must be able to scan a subdirectory tree.
- h) The scanner should not issue a sound alarm on every infected file; there must be a way to turn the sound off.
- i) We keep the right to change the conditions at any time.

1.1 Tested products

The following 13 products were tested in this comparative:

Avast! 4.1.342 Professional Edition
BitDefender Anti-Virus 7.2 Professional Edition
Dr.Web Anti-Virus for Windows 95-XP 4.30a
ESET NOD32 2.000.9
F-Prot Anti-Virus for Windows 3.14b
H+B EDV AntiVir Professional Edition 6.22.00.09
Kaspersky Anti-Virus Personal 4.5.0.95
McAfee VirusScan Professional 8.0.26
Panda Platinum Internet Security 8.02.00
Symantec Norton Anti-Virus 10.0.1.13
GeCAD Reliable Anti-Virus (RAV) 8.6.105
Sophos Anti-Virus 3.78
Trend Micro Internet Security 11.10

Deadline for submitting products was the 4. February 2004. All products were updated with the last official updates that were available at 18.55 CET the 6. February 2004. The sample databases were frozen the 4. February 2004.

1.2 Creating the final summary of the results

Scans are performed up to 3 times for each product in order to get sure that all what can be detected by the scanner was detected. We process the logs and count every detected sample in each category. To be sure that the results are counted right, we finally look how many samples remained undetected. AV companies will receive their missed samples.

Note: This is a shortened version of the comparative report. It contains just the data about the results and rankings. AV companies, magazines, etc. does receive different, more detailed versions of the comparative report.

2. Test results

Developer		H+BEDV Datentechnik		Alwil Software		Softwin		DialogueScience		Frisk Software	
Product name		AntiVir Prof.		Avast! Prof.		BitDefender Prof.		Dr. Web		F-Prot	
Program version		6.22.00.09		4.1.342		7.2.0.0		4.30a		3.14b	
Engine / signature version		6.23.0.60		0401-10		N/A		4.30.0		3.14.2	
Signature date		02/06/2004		02/06/2004		02/06/2004		02/06/2004		02/05/2004	
Number of virus records		N/A		N/A		70.071		46.016		103.435	
On-demand detection of virus/malware											
DOS viruses	217.992	208.770	95,77%	210.840	96,72%	211.049	96,82%	215.419	98,82%	217.777	99,90%
Windows viruses	11.721	8.954	76,39%	10.927	93,23%	10.970	93,59%	10.952	93,44%	11.450	97,69%
Macro viruses	22.715	22.141	97,47%	22.327	98,29%	22.628	99,62%	22.698	99,93%	22.709	99,97%
Script viruses	5.107	2.736	53,57%	3.045	59,62%	3.795	74,31%	3.987	78,07%	4.172	81,69%
Worms	11.241	8.122	72,25%	8.985	79,93%	9.905	88,11%	10.220	90,92%	10.200	90,74%
Backdoors	14.739	7.673	52,06%	10.416	70,67%	13.944	94,61%	13.262	89,98%	13.982	94,86%
Trojans	12.249	6.776	55,32%	9.417	76,88%	10.503	85,75%	8.575	70,01%	11.588	94,60%
other malware	1.459	325	22,28%	1.053	72,17%	1.014	69,50%	924	63,33%	1.319	90,40%
OtherOS malware	1.070	338	31,59%	684	63,93%	368	34,39%	587	54,86%	799	74,67%
TOTAL	298.293	265.835	89,12%	277.694	93,09%	284.176	95,27%	286.624	96,09%	293.996	98,56%
<i>Total without DOS & OtherOS</i>	<i>79.231</i>	<i>56.727</i>	<i>71,60%</i>	<i>66.170</i>	<i>83,52%</i>	<i>72.759</i>	<i>91,83%</i>	<i>70.618</i>	<i>89,13%</i>	<i>75.420</i>	<i>95,19%</i>
On-demand detection of dialers											
Dialers	204.840	192.733	94,09%			82.505	40,28%				

Developer		Trend Micro		Kaspersky Labs		Network Associates		ESET	
Product name		Internet Security		KAV Personal		McAfee VirusScan		NOD32 Anti-Virus	
Program version		11.10		4.5.0.95		8.0.26		2.000.9	
Engine / signature version		6.810.1005 (757)		N/A		4.3.20 / 4322		1.617	
Signature date		02/06/2004		02/06/2004		02/04/2004		02/06/2004	
Number of virus records		N/A		84.229		85.469		N/A	
On-demand detection of virus/malware									
DOS viruses	217.992	205.840	94,43%	217.901	99,96%	217.869	99,94%	214.777	98,53%
Windows viruses	11.721	10.236	87,33%	11.705	99,86%	11.713	99,93%	11.226	95,78%
Macro viruses	22.715	22.588	99,44%	22.715	100%	22.715	100%	22.653	99,73%
Script viruses	5.107	3.515	68,83%	4.989	97,69%	5.035	98,59%	3.520	68,93%
Worms	11.241	8.758	77,91%	11.164	99,32%	11.219	99,80%	9.625	85,62%
Backdoors	14.739	8.702	59,04%	14.720	99,87%	13.813	93,72%	12.913	87,61%
Trojans	12.249	8.638	70,52%	12.187	99,49%	11.375	92,86%	8.658	70,68%
other malware	1.459	835	57,23%	1.456	99,79%	1.327	90,95%	1.022	70,05%
OtherOS malware	1.070	655	61,21%	1.035	96,73%	1.033	96,54%	519	48,50%
TOTAL	298.293	269.767	90,44%	297.872	99,86%	296.099	99,26%	284.913	95,51%
<i>Total without DOS & OtherOS</i>	<i>79.231</i>	<i>63.272</i>	<i>79,86%</i>	<i>78.936</i>	<i>99,63%</i>	<i>77.197</i>	<i>97,43%</i>	<i>69.617</i>	<i>87,87%</i>
On-demand detection of dialers									
Dialers	204.840			203.190	99,19%	204.016	99,60%		

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		8.02.00		8.6.105		3.78	
Engine / signature version		60204d		N/A		8.11		2.18	
Signature date		02/04/2004		02/06/2004		02/05/2004		02/06/2004	
Number of virus records		64.943		69.415		89.689		87.468	
On-demand detection of virus/malware									
DOS viruses	217.992	211.578	97,06%	217.494	99,77%	216.766	99,44%	212.300	97,39%
Windows viruses	11.721	11.596	98,93%	11.362	96,94%	11.419	97,42%	11.279	96,23%
Macro viruses	22.715	22.681	99,85%	22.699	99,93%	22.674	99,82%	22.613	99,55%
Script viruses	5.107	4.421	86,57%	4.800	93,99%	4.478	87,68%	3.726	72,96%
Worms	11.241	10.813	96,19%	10.861	96,62%	10.707	95,25%	9.691	86,21%
Backdoors	14.739	10.855	73,65%	14.298	97,01%	14.347	97,34%	10.763	73,02%
Trojans	12.249	9.961	81,32%	11.766	96,06%	11.150	91,03%	9.030	73,72%
other malware	1.459	1.102	75,53%	1.384	94,86%	1.180	80,88%	963	66,00%
OtherOS malware	1.070	816	76,26%	981	91,68%	888	82,99%	775	72,43%
TOTAL	298.293	283.823	95,15%	295.645	99,11%	293.609	98,43%	281.140	94,25%
<i>Total without DOS & OtherOS</i>	<i>79.231</i>	<i>71.429</i>	<i>90,15%</i>	<i>77.170</i>	<i>97,40%</i>	<i>75.955</i>	<i>95,87%</i>	<i>68.065</i>	<i>85,91%</i>
On-demand detection of dialers									
Dialers	204.840	125.950	61,49%	61.438	29,99%	202.860	99,03%	172.194	84,06%

3. 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	99.80%
2.	Kaspersky	99.58%
3.	Panda	97.91%
4.	Symantec	97.49%
5.	RAV	97.03%
6.	F-Prot	95.56%
7.	Dr.Web	94.24%
8.	Sophos	93.16%
9.	BitDefender	93.14%
10.	NOD32	92.60%
11.	Avast	89.17%
12.	TrendMicro	88.80%
13.	H+BEDV	82.61%

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

1.	Kaspersky	99.70%
2.	Panda	96.49%
3.	RAV	93.78%
4.	F-Prot	94.52%
5.	McAfee	93.21%
6.	BitDefender	89.50%
7.	Dr.Web	80.01%
8.	NOD32	79.42%
9.	Symantec	77.05%
10.	Avast	73.42%
11.	Sophos	72.79%
12.	TrendMicro	63.89%
13.	H+BEDV	51.94%

(c) Results over DOS virus detection:

1.	Kaspersky	99.96%
2.	McAfee	99.94%
3.	F-Prot	99.90%
4.	Panda	99.77%
5.	RAV	99.44%
6.	Dr.Web	98.82%
7.	NOD32	98.53%
8.	Sophos	97.39%
9.	Symantec	97.06%
10.	BitDefender	96.82%
11.	Avast	96.72%
12.	H+BEDV	95.77%
13.	TrendMicro	94.43%

(d) Results over Dialer detection:

1.	McAfee	99.60%
2.	Kaspersky	99.19%
3.	RAV	99.03%
4.	H+BEDV	94.09%
5.	Sophos	84.06%
6.	Symantec	61.49%
7.	BitDefender	40.28%
8.	Panda	29.99%
9.	all the others	< 1 %

(e) Results over 'OtherOS malware' detection:

1.	Kaspersky	96.73%
2.	McAfee	96.54%
3.	Panda	91.68%
4.	RAV	82.99%
5.	Symantec	76.26%
6.	F-Prot	74.67%
7.	Sophos	72.43%
8.	Avast	63.93%
9.	TrendMicro	61.21%
10.	Dr.Web	54.86%
11.	NOD32	48.50%
12.	BitDefender	34.39%
13.	H+BEDV	31.59%

4. Credits

After each comparative, products will receive "credits" based on the rankings reached in each single category:

	a	b	c	d	e	$\Sigma^1/5$
Avast	11	10	11	9	8	9.80
BitDefender	9	6	10	7	12	8.80
Dr.Web	7	7	6	9	10	7.80
F-Prot	6	4	3	9	6	5.60
H+BEDV	13	13	12	4	13	11.00
Kaspersky	2	1	1	2	1	1.40
McAfee	1	5	2	1	2	2.20
NOD32	10	8	7	9	11	9.00
Panda	3	2	4	8	3	4.00
RAV	5	3	5	3	4	4.00
Sophos	8	11	8	5	7	8.00
Symantec	4	9	9	6	5	6.60
TrendMicro	12	12	13	9	9	11.00

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:

1 st	place: Kaspersky	(1.40)
2 nd	place: McAfee	(2.20)
3 rd	place: Panda	(4.00)
3 rd	place: RAV	(4.00)
4 th	place: F-Prot	(5.60)
5 th	place: Symantec	(6.60)
6 th	place: Dr.Web	(7.80)
6 th	place: Sophos	(7.80)
7 th	place: BitDefender	(8.80)
8 th	place: NOD32	(9.00)
9 th	place: Avast	(9.80)
10 th	place: TrendMicro	(11.0)
10 th	place: H+BEDV	(11.0)

¹ Lower numbers means „better“.

5. 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 (February 2004)