Anti-Virus Comparative No.5

On-demand detection of malicious software

Date: February 2005 (2005-02)

Last revision of this report: 27. February 2005

Author: Andreas Clementi

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

1. Conditions in order to participate

a) The Anti-Virus scanner must detect 100% of ItW-samples and at least 85% of our zoo-samples on-demand. If a product that is actually being tested doesn't reach at least 85% of detection in the zoo-samples for on-demand test, no detection details will be provided in the results and also no samples will be supplied. If a product fails to reach 85% of detection in zoo-samples for two consecutives tests its permanence in the tests will have to be reconsidered.
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 scan files with executable 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.
e) The labels for the on-demand detection rate of dialers are: "not present" (0-5%), "low" (6-40%), "mediocre" (41-70%), "high" (71-95%) and "excellent" (96-100%). Our dialer test-set consists of ~205.000 samples.
f) 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 companies that don't send samples for the test will receive not more than 2.500 files chosen by the tester. 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 us 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 do 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) Participating companies have on our request to submit a license key and a full working product version in order that we can test it.
k) For doing the tests we accept donations for each test-series (1 year = 4 tests) on a voluntary base in order to cover expenses we have and to recompense our work and time spent. The amount of the donations is free.
l) 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.
m) Any company that wants to join tests should send all samples that being detected by their antivirus are not already in the test set collection. If the company doesn't agree about sending missed samples they can still participate in the tests but even if they send monthly collections they will not be able to get any missed sample. 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 don't accept a company, it will be not included in the tests.
n) Companies that do not answer/reply to emails for two months will be excluded from the tests at our discretion due lack of cooperation.
o) We keep the right to change the conditions at any time and to exclude products included in the test.

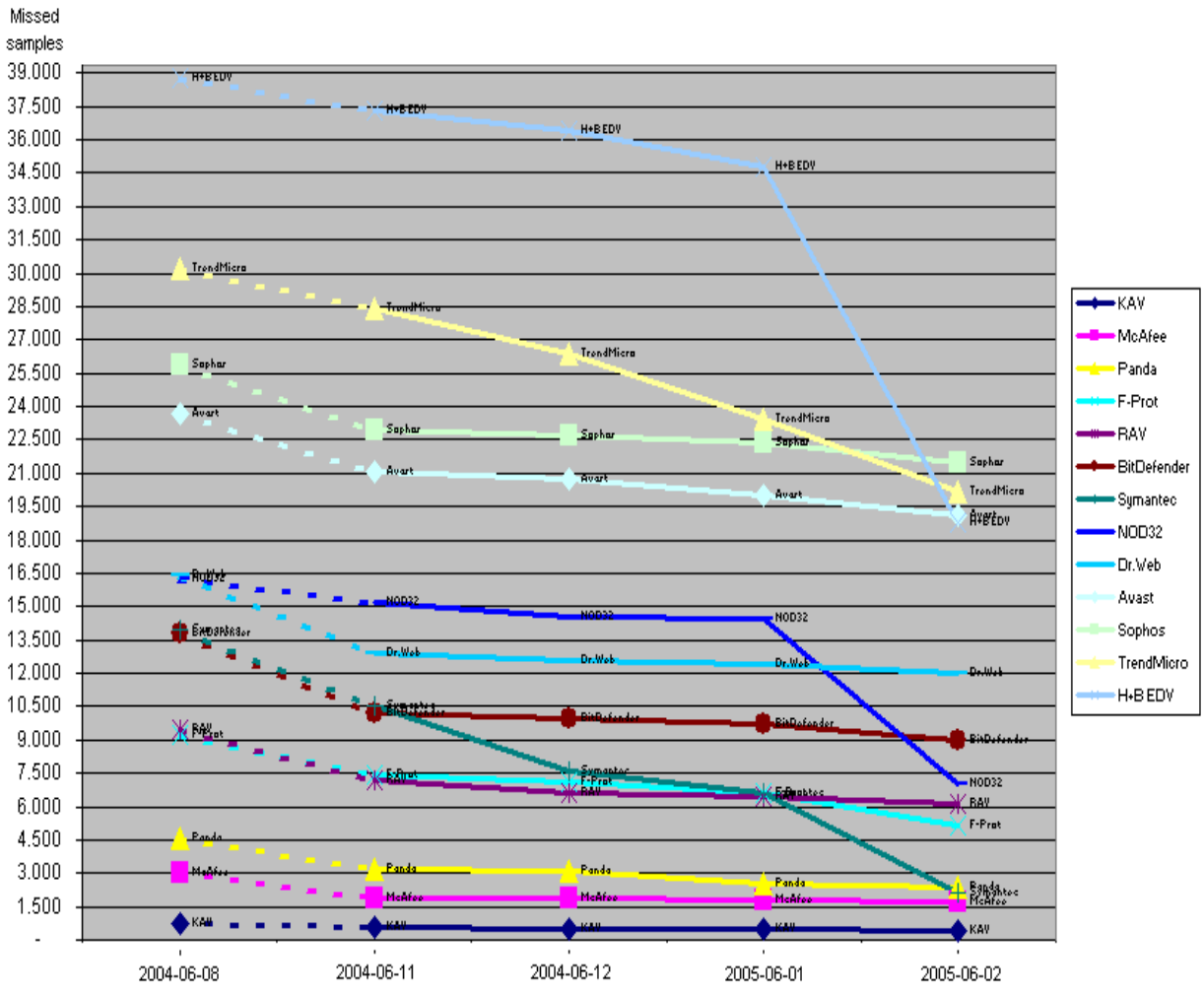
2. Tested products

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

All products were updated the 6th February 2005 and set to use the best possible settings. Test-beds were frozen the 4th February 2005.

3. Progresses made since last comparative

Below you see how many of the missed samples in the August 2004 comparative were detected/added after 3, 4, 5 and 6 months by the respective companies.



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	
On-demand detection rate of dialers (*)		*excellent*		*mediocre*		*high*		*mediocre*		*low*	
On-demand detection of virus/malware											
DOS viruses	233.929	221.124	94,53%	225.891	96,56%	214.482	91,69%	229.529	98,12%	225.771	96,51%
Windows viruses	17.411	13.339	76,61%	15.779	90,63%	14.195	81,53%	16.565	95,14%	15.732	90,36%
Macro viruses	32.649	32.502	99,55%	32.107	98,34%	32.376	99,16%	32.212	98,66%	32.615	99,90%
Script viruses	7.956	3.875	48,71%	4.527	56,90%	2.494	31,35%	6.078	76,40%	6.066	76,24%
Worms	18.153	16.391	90,29%	14.918	82,18%	16.382	90,24%	16.429	90,50%	17.000	93,65%
Backdoors	39.467	37.002	93,75%	31.693	80,30%	37.135	94,09%	35.760	90,61%	36.990	93,72%
Trojans	29.618	23.666	79,90%	20.889	70,53%	13.468	45,47%	22.464	75,85%	24.229	81,80%
other malware	5.085	3.181	62,56%	3.939	77,46%	1.353	26,61%	3.220	63,32%	3.357	66,02%
OtherOS malware	1.836	614	33,44%	890	48,47%	281	15,31%	767	41,78%	829	45,15%
TOTAL	**386.104**	351.694	**91,09%**	350.633	**90,81%**	332.166	**86,03%**	363.024	**94,02%**	362.589	**93,91%**
Total without DOS & OtherOS	*150.339*	*129.956*	*86,4%*	*123.852*	*82,4%*	*117.403*	*78,1%*	*132.728*	*88,3%*	*135.989*	*90,5%*

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	
On-demand detection rate of dialers (*)		*not present*		*not present*		*excellent*		*excellent*	
On-demand detection of virus/malware									
DOS viruses	233.929	233.427	99,79%	222.444	95,09%	233.813	99,95%	233.802	99,95%
Windows viruses	17.411	16.370	94,02%	15.029	86,32%	17.353	99,67%	17.337	99,57%
Macro viruses	32.649	32.649	100%	32.549	99,69%	32.649	100%	32.648	~100%
Script viruses	7.956	6.956	87,43%	5.218	65,59%	7.789	97,90%	7.843	98,58%
Worms	18.153	16.945	93,35%	16.026	88,28%	18.086	99,63%	18.083	99,61%
Backdoors	39.467	34.337	87,00%	33.782	85,60%	39.323	99,64%	37.123	94,06%
Trojans	29.618	22.456	75,82%	23.237	78,46%	29.208	98,62%	25.316	85,48%
other malware	5.085	3.552	69,85%	3.383	66,53%	5.035	99,02%	4.661	91,66%
OtherOS malware	1.836	1.202	65,47%	876	47,71%	1.487	80,99%	1.735	94,50%
TOTAL	**386.104**	367.894	**95,28%**	352.544	**91,31%**	384.743	**99,65%**	378.548	**98,04%**
Total without DOS & OtherOS	*150.339*	*133.265*	*88,6%*	*129.224*	*86,0%*	*149.443*	*99,4%*	*143.011*	*95,1%*

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	
On-demand detection rate of dialers (*)		*not present*		*excellent*		*excellent*		*high*	
On-demand detection of virus/malware									
DOS viruses	233.929	229.788	98,23%	232.193	99,26%	232.971	99,59%	227.818	97,39%
Windows viruses	17.411	16.659	95,68%	17.356	99,68%	16.553	95,07%	15.886	91,24%
Macro viruses	32.649	32.641	99,98%	32.639	99,97%	32.542	99,67%	32.536	99,65%
Script viruses	7.956	5.364	67,42%	7.576	95,22%	7.074	88,91%	5.315	66,80%
Worms	18.153	16.737	92,20%	17.965	98,96%	17.003	93,66%	15.029	82,79%
Backdoors	39.467	37.785	95,74%	38.168	96,71%	30.338	76,87%	29.943	75,87%
Trojans	29.618	25.115	84,80%	27.104	91,51%	21.799	73,60%	17.045	57,55%
other malware	5.085	3.883	76,36%	4.829	94,97%	3.626	71,31%	3.003	59,06%
OtherOS malware	1.836	774	42,16%	1.732	94,34%	1.228	66,88%	1.304	71,02%
TOTAL	**386.104**	368.746	**95,50%**	379.562	**98,31%**	363.134	**94,05%**	347.879	**90,10%**
Total without DOS & OtherOS	*150.339*	*138.184*	*91,9%*	*145.637*	*96,9%*	*128.935*	*85,8%*	*118.757*	*79,0%*

If you have any questions about the tests or the results, please read the document with the FAQ's that can be found on the website or ask us directly by visiting http://www.av-comparatives.org/forum

5. Summary results

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

1.	McAfee	99.7%
2.	Kaspersky	99.6%
3.	Symantec	99.2%
4.	RAV	96.1%
5.	F-Prot	95.7%
6.	Dr.Web	93.8%
7.	NOD32	93.7%
8.	BitDefender	93.6%
9.	TrendMicro	90.4%
10.	Sophos	90.3%
11.	Avast	88.4%
12.	H+BEDV	86.8%
13.	AVG	85.9%

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

1.	Kaspersky	99.2%
2.	Symantec	94.5%
3.	McAfee	90.5%
4.	NOD32	90.0%
5.	Dr.Web	87.1%
6.	H+BEDV	86.1%
7.	BitDefender	82.8%
8.	TrendMicro, F-Prot	81.4%
9.	Avast	76.2%
10.	RAV	75.2%
11.	AVG	70.0%
12.	Sophos	67.4%

(c) Total detection rates without ‘DOS’ and ‘OtherOS malware’:

1.	Kaspersky	99.4%
2.	Symantec	96.9%
3.	McAfee	95.1%
4.	NOD32	91.9%
5.	Dr.Web	90.5%
6.	F-Prot	88.6%
7.	BitDefender	88.3%
8.	H+BEDV	86.4%
9.	TrendMicro	86.0%
10.	RAV	85.8%
11.	Avast	82.4%
12.	Sophos	79.0%
13.	AVG	78.1%

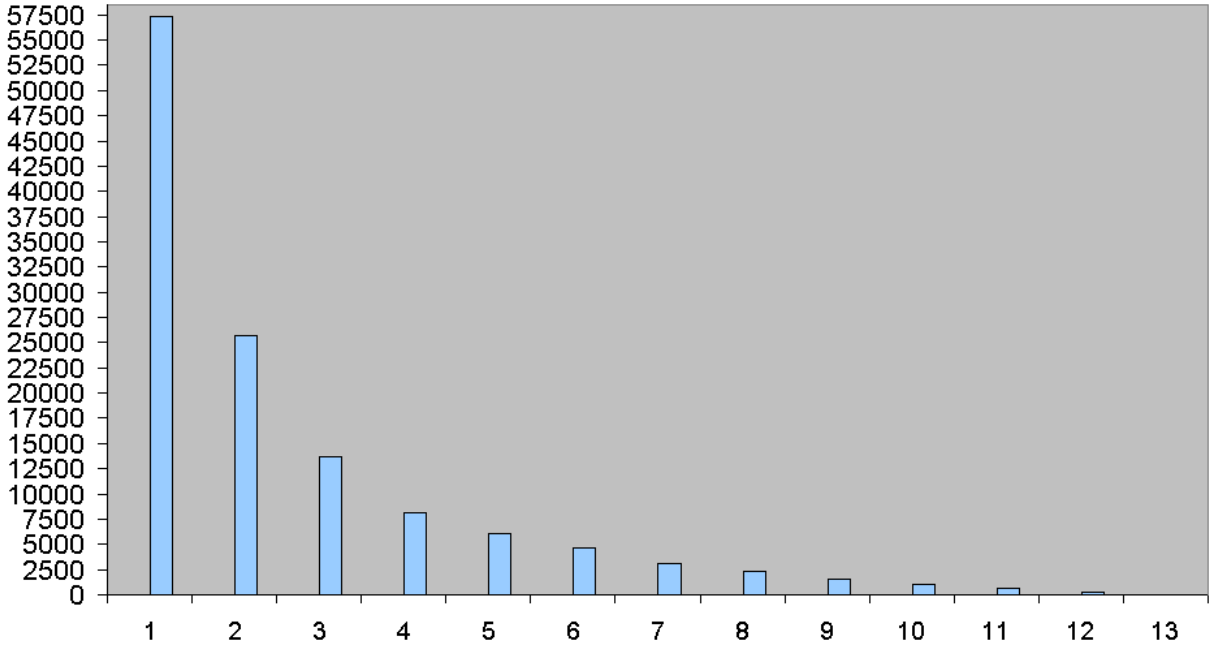
(d) Total detection rates (including DOS and OtherOS):

1.	Kaspersky	99.65%	ADVANCED+
2.	Symantec	98.31%	ADVANCED+
3.	McAfee	98.04%	ADVANCED+
4.	NOD32	95.50%	ADVANCED
5.	F-Prot	95.28%	ADVANCED
6.	RAV	94.05%	ADVANCED
7.	BitDefender	94.02%	ADVANCED
8.	Dr.Web	93.91%	ADVANCED
9.	TrendMicro	91.31%	STANDARD
10.	H+BEDV	91.09%	STANDARD
11.	Avast	90.81%	STANDARD
12.	Sophos	90.10%	STANDARD
13.	AVG	86.03%	--------

We replaced the ranking-system with a 3-level-system (standard, advanced and advanced+). The levels are set for each test by the tester. All the overviews can be found on our website.

6. Non-detected samples in the test-bed of February 2005

About 68% of the test-set is detected by all 13 scanners. The non-detected samples consist as follow:



This figure shows how many samples were not detected by how many scanners in the used test-set. All samples were detected by at least one scanner. Examples: around 270 samples were not detected by 12 scanners; one (NOT a single scanner!) of the 13 scanners detected them. Around 57.270 samples were detected by 12 scanners and not by one scanner (NOT a single scanner!).

7. Copyright and Disclaimer

Andreas Clementi, Austria (February 2005)