Anti-Virus Comparative No.7

On-demand detection of malicious software

Date: August 2005 (2005-08)

Last revision of this report: 26th August 2005

Author: Andreas Clementi

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

1. Conditions in order to participate

a) The Anti-Virus scanner should 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 after the test if they send me their samples with permission to share them with other submitting companies. 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.
h) Participating companies have to agree not to take any legal action against those involved in the testing and agree not to try to discredit the tests or those performing the tests due the results of their tests or the test methodology (or due any other reason).
i) Participating companies that use inappropriate detection methods (e.g. md5-signatures on missed samples of replicating malware) or engage in illegal practices or practices that are generally considered harmful to the AV industry will be excluded from future tests. Deliberate practices that may lead to wrong test results will be considered inappropriate.
j) Participating companies will on our request provide a license key and a full working product version in order that we can test it.
k) For doing the tests we accept donations on a voluntary base in order to cover expenses we have and to recompense our work and time spent. The donations are always done after the test and not in advance. The appropriate amount of any donation is up to the donor.
l) Any company being tested in the comparatives that provide samples to virus writers, or other parties without legitimate need or experience and discretion to handle samples safely will be excluded from tests. Any company that has violated this requirement may not be accepted for testing.
m) Any company that wants to join tests must send all samples that are being detected by their product and are not already in the test set. Companies that do not agree to provide these samples can still participate in the tests but will not be able to get any missed samples. New candidates for the test must be accepted by us and additionally accepted by 60% of the already participating companies before they can be included in our tests.
n) Companies that do not respond to attempts to collect required information will be excluded from the tests at our discretion.
o) We keep the right to change the conditions at any time and to exclude products included in the test.

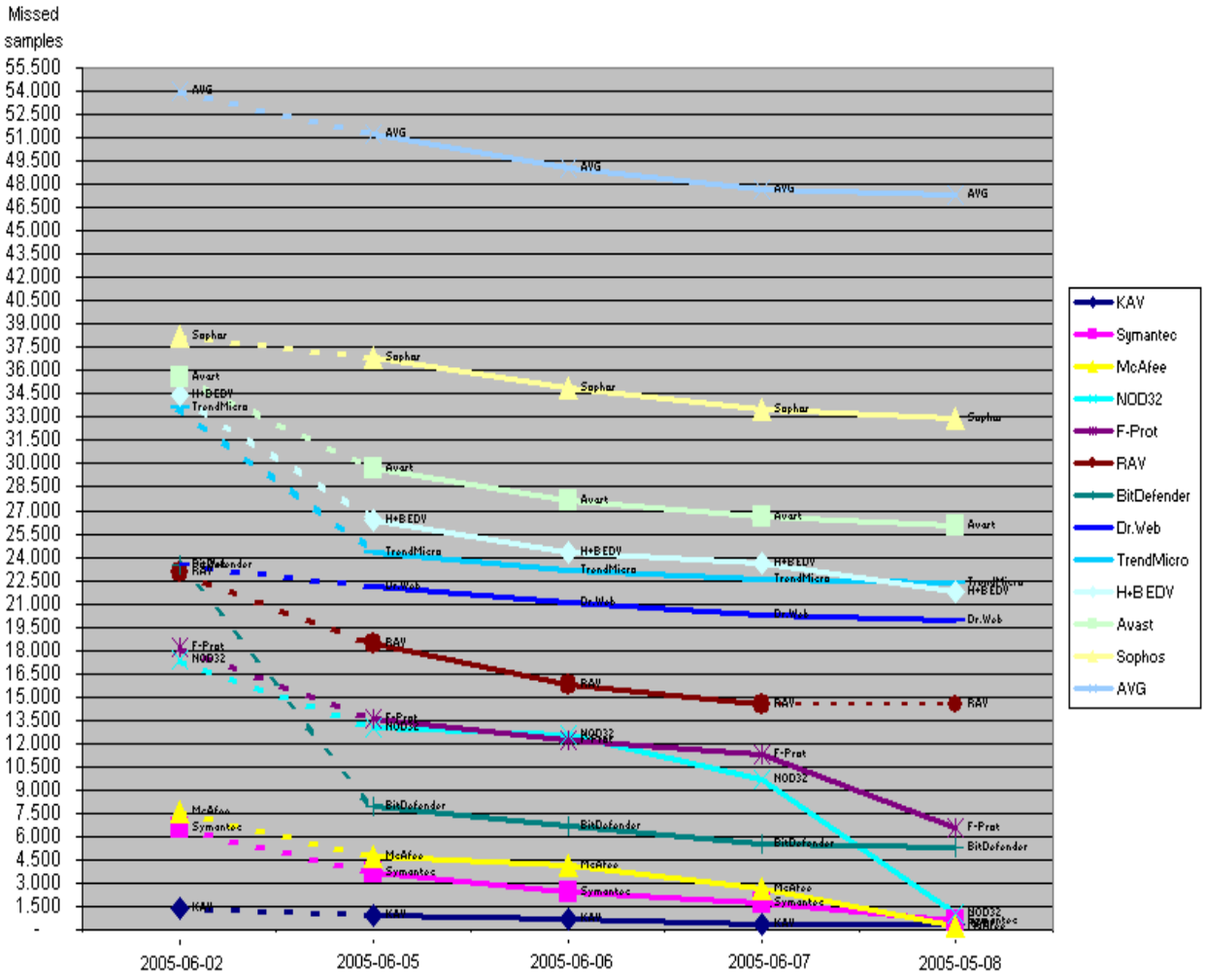
2. Tested products

Avast! 4.6.691 Professional Edition
AVG Professional 7.0.338
BitDefender Anti-Virus 8.0.200 Professional Plus
Dr.Web Anti-Virus for Windows 95-XP 4.32b
ESET NOD32 2.51.8
F-Prot Anti-Virus for Windows 3.16c
H+B EDV AntiVir Professional Edition 6.31.00.03
Kaspersky Anti-Virus Personal Pro 5.0.372
McAfee VirusScan 10.0.21
Symantec Norton Anti-Virus 11.0.11.4
Sophos Anti-Virus 5.0.5
Trend Micro Internet Security 12.1.1034

All products were updated the 5th August 2005 and set to use the best possible settings. Test-beds were frozen the 2nd August 2005. The tested product versions were chosen by the respective companies. GeCAD Reliable Anti-Virus (RAV) is no longer included in the test as the signatures updates stopped the 12th June 2005.

3. Progresses made since last comparative

Below you see how many of the missed samples in the February 2005 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	
Product		**AntiVir Workstation**		**Avast! Prof.**		**AVG Professional**		**BitDefender Prof.+**	
Program version		6.31.00.03		4.6.691		7.0.338		8.0.200	
Engine / signature version		6.31.1.0 / 6.31.1.62		0531-4		267.10.1/64		7.02560	
Signature date (mm/dd/yyyy)		08/05/2005		08/05/2005		08/04/2005		08/05/2005	
Number of virus records		202.710		*unknown*		*unknown*		198.395	
On-demand detection rate of dialers (*)		*excellent*		*high*		*excellent*		*excellent*	
On-demand detection of virus/malware									
DOS viruses/malware	240.449	226.936	94,38%	231.502	96,28%	218.854	91,02%	235.678	98,02%
Windows viruses	19.393	14.830	76,47%	17.710	91,32%	15.794	81,44%	18.602	95,92%
Macro viruses	37.206	37.159	99,87%	36.680	98,59%	37.150	99,85%	36.813	98,94%
Script viruses/malware	6.802	4.260	62,63%	4.226	62,13%	2.298	33,78%	6.318	92,88%
Worms	19.331	18.304	94,69%	16.446	85,08%	17.920	92,70%	18.820	97,36%
Backdoors	55.011	54.040	98,23%	45.311	82,37%	53.107	96,54%	53.533	97,31%
Trojans	36.234	33.945	93,68%	26.583	73,36%	21.365	58,96%	34.045	93,96%
other malware	5.011	3.977	79,37%	4.066	81,14%	1.431	28,56%	4.798	95,75%
OtherOS viruses/malware	1.734	888	51,21%	1.008	58,13%	334	19,26%	1.344	77,51%
TOTAL	**421.171**	394.339	**93,63%**	383.532	**91,06%**	368.253	**87,44%**	409.951	**97,34%**
Total without DOS & OtherOS	*178.988*	*166.515*	*93,0%*	*151.022*	*84,4%*	*149.065*	*83,3%*	*172.929*	*96,6%*

Company		Doctor Web		Frisk Software		Trend Micro		Kaspersky Labs	
Product		**Dr. Web**		**F-Prot Anti-Virus**		**Internet Security**		**KAV Personal Pro**	
Program version		4.32b		3.16c		12.1.1034		5.0.372	
Engine / signature version		4.32b		3.16.6		7.510.1002 / 2.761.00		*N/A*	
Signature date (mm/dd/yyyy)		08/05/2005		08/05/2005		08/04/2005		08/05/2005	
Number of virus records		82.894		191.534		*unknown*		142.285	
On-demand detection rate of dialers (*)		*high*		*not present*		*not present*		*excellent*	
On-demand detection of virus/malware									
DOS viruses/malware	240.449	230.341	95,80%	239.904	99,77%	228.305	94,95%	240.367	99,97%
Windows viruses	19.393	17.441	89,93%	18.218	93,94%	16.841	86,84%	19.376	99,91%
Macro viruses	37.206	37.172	99,91%	37.206	100%	37.088	99,68%	37.206	100%
Script viruses/malware	6.802	5.456	80,21%	6.505	95,63%	4.823	70,91%	6.772	99,56%
Worms	19.331	17.820	92,18%	17.840	92,29%	17.670	91,41%	19.315	99,92%
Backdoors	55.011	49.836	90,59%	49.235	89,50%	47.642	86,60%	54.963	99,91%
Trojans	36.234	26.945	74,36%	29.731	82,05%	27.266	75,25%	36.154	99,78%
other malware	5.011	3.311	66,07%	3.995	79,72%	3.749	74,82%	4.995	99,68%
OtherOS viruses/malware	1.734	904	52,13%	1.185	68,34%	937	54,04%	1.529	88,18%
TOTAL	**421.171**	389.226	**92,42%**	403.819	**95,88%**	384.321	**91,25%**	420.677	**99,88%**
Total without DOS & OtherOS	*178.988*	*157.981*	*88,3%*	*162.730*	*90,9%*	*155.079*	*86,6%*	*178.781*	*99,9%*

Company		McAfee		ESET		Symantec		Sophos	
Product		**McAfee VirusScan**		**NOD32 Anti-Virus**		**Norton Anti-Virus**		**Sophos Anti-Virus**	
Program version		10.0.21		2.51.8		11.0.11.4		5.0.5	
Engine / signature version		4.4.00 / 4551		1.1187		70805q		2.30.12 / 3.96	
Signature date (mm/dd/yyyy)		08/05/2005		08/05/2005		08/05/2005		08/05/2005	
Number of virus records		141.156		*unknown*		70.431		108.226	
On-demand detection rate of dialers (*)		*excellent*		*excellent*		*excellent*		*high*	
On-demand detection of virus/malware									
DOS viruses/malware	240.449	240.429	99,99%	238.266	99,09%	240.243	99,91%	233.765	97,22%
Windows viruses	19.393	19.329	99,67%	19.264	99,33%	19.364	99,85%	17.478	90,13%
Macro viruses	37.206	37.206	100%	37.190	99,96%	37.186	99,95%	37.143	99,83%
Script viruses/malware	6.802	6.682	98,24%	6.562	96,47%	6.630	97,47%	4.657	68,47%
Worms	19.331	19.283	99,75%	19.147	99,05%	19.233	99,49%	15.796	81,71%
Backdoors	55.011	52.935	96,23%	53.837	97,87%	54.403	98,89%	42.053	76,44%
Trojans	36.234	31.377	86,60%	33.580	92,68%	35.124	96,94%	20.158	55,63%
other malware	5.011	4.648	92,76%	4.780	95,39%	4.826	96,31%	2.981	59,49%
OtherOS viruses/malware	1.734	1.675	96,60%	1.423	82,06%	1.674	96,54%	1.309	75,49%
TOTAL	**421.171**	413.564	**98,19%**	414.049	**98,31%**	418.683	**99,41%**	375.340	**89,12%**
Total without DOS & OtherOS	*178.988*	*171.460*	*95,8%*	*174.360*	*97,4%*	*176.766*	*98,8%*	*140.266*	*78,4%*

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 & Scripts detection:

1.	Kaspersky	99.9%
2.	McAfee	99.7%
3.	Symantec	99.6%
4.	NOD32	99.3%
5.	BitDefender	97.4%
6.	F-Prot	96.4%
7.	Dr.Web	94.1%
8.	TrendMicro	92.4%
9.	Sophos, Avast	90.7%
10.	H+BEDV	90.1%
11.	AVG	88.4%

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

1.	Kaspersky	99.9%
2.	Symantec	98.0%
3.	BitDefender	96.0%
4.	NOD32	95.8%
5.	H+BEDV	95.5%
6.	McAfee	92.4%
7.	F-Prot	86.2%
8.	Dr.Web	83.2%
9.	TrendMicro	81.7%
10.	Avast, AVG	78.9%
11.	Sophos	67.7%

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

1.	Kaspersky	99.9%
2.	Symantec	98.8%
3.	NOD32	97.4%
4.	BitDefender	96.6%
5.	McAfee	95.8%
6.	H+BEDV	93.0%
7.	F-Prot	90.9%
8.	Dr.Web	88.3%
9.	TrendMicro	86.6%
10.	Avast	84.4%
11.	AVG	83.3%
12.	Sophos	78.4%

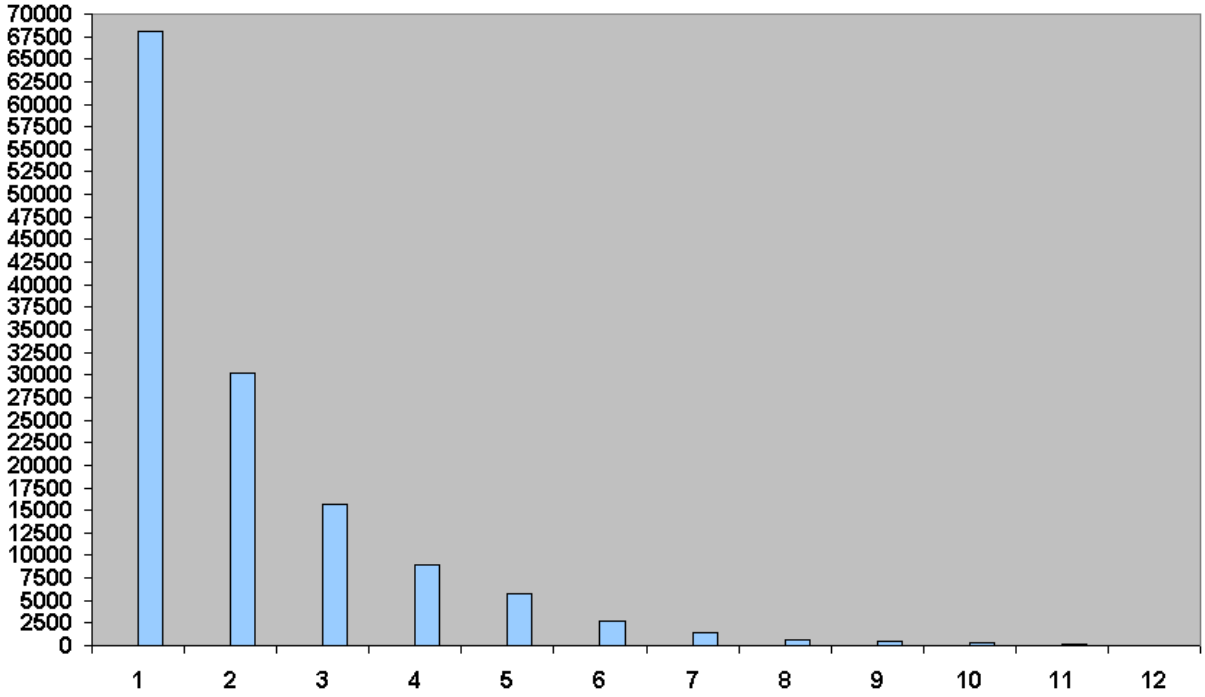
(d) Total detection rates (including DOS and OtherOS):

1.	Kaspersky	99.88%	ADVANCED+
2.	Symantec	99.41%	ADVANCED+
3.	NOD32	98.31%	ADVANCED+
4.	McAfee	98.19%	ADVANCED+
5.	BitDefender	97.34%	ADVANCED+
6.	F-Prot	95.88%	ADVANCED
7.	H+BEDV	93.63%	ADVANCED
8.	Dr.Web	92.42%	STANDARD
9.	TrendMicro	91.25%	STANDARD
10.	Avast	91.06%	STANDARD
11.	Sophos	89.12%	STANDARD
12.	AVG	87.44%	STANDARD

We provide a 3-level-ranking-system (STANDARD, ADVANCED and ADVANCED+). All the overviews can be found on our website. Products belonging to a category can be considered to be as good as the other products in the same category regarding the on-demand detection rate. All products in the ADVANCED+ category offer very high level of on-demand detection. Selection of a product from this category should not be based on detection score alone. The quality of support, easy of use and system resource use should be considered when selecting a product. Products in the ADVANCED category offer a high level of detection, but less than those in the ADVANCED+. These products are suitable for many users. In our opinion, products in the STANDARD category or below are suitable for use if they also are ICSA certified (www.icsalabs.com) or CheckMark Anti-Virus Level 1 certified (www.westcoastlabs.org/checkmarkcertification.asp), or frequently achieve Virus Bulletin 100% awards (www.virusbtn.com/vb100/archives/products.xml - *requires free registration*).

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

About 68% of the test-set is detected by all 12 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 102 samples were not detected by 11 scanners; one (NOT a single scanner!) of the 12 scanners detected them. Around 68.101 samples were detected by 11 scanners and not by one scanner (NOT a single scanner!).

7. Copyright and Disclaimer

Andreas Clementi, Austria (August 2005)