AV
comparatives

Anti-Virus Comparative No.11

On-demand detection of malicious software

Date: August 2006 (2006-08)

Last revision of this report: 31th August 2006

Author: Andreas Clementi

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

1. Conditions for participation

The conditions for participation in our tests are listed in the methodology document at http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf. The products included in our tests constitute some very good anti-virus software with high on-demand detection rates, as this is one of the requirements needed to be included in our tests. Only products of vendors who have agreed to participate were included in the test. Products with detection rates lower than our specified standard, or from vendors not wanting to participate this year were not tested.

2. Tested products

All products were updated on the 7th August 2006 and set to use the best possible settings. The Malware sets and system Test-beds were frozen the 4th August 2006. The following 15 products[1] were included in this test[2]:

Avast! 4.7.869 Professional Edition
AVG Professional 7.1.405
AVIRA AntiVir Personal Edition Premium 7.01.01.02
BitDefender Anti-Virus 9.5 Professional Plus
Dr.Web Anti-Virus for Windows 95-XP 4.33.2
ESET NOD32 Anti-Virus 2.51.26
F-Prot Anti-Virus for Windows 3.16f[3]
F-Secure Anti-Virus 6.12.90 (*)
Gdata AntiVirusKit (AVK) 16.0.7 (*)
Kaspersky Anti-Virus 6.0.0.303
McAfee VirusScan 11.0.209
Norman Virus Control 5.81
Symantec Norton Anti-Virus 12.2.0.13
TrustPort Antivirus Workstation 2.0.0.843 (*)
VBA32 Workstation 3.11.0

(*) AVK, F-Secure and TrustPort are multi-engine products:

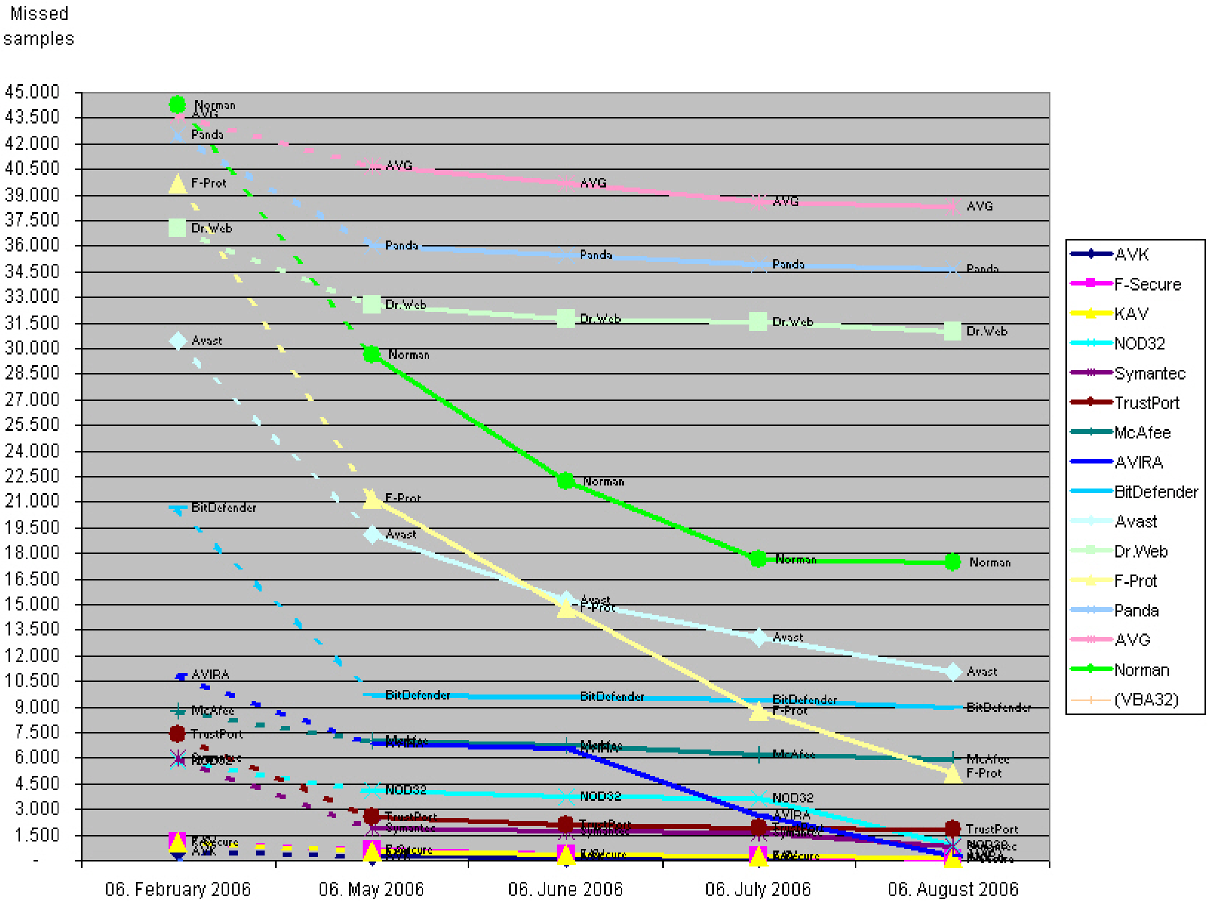
- AVK[4] contains the *Kaspersky* and *Bitdefender* engines
- TrustPort contains the *Norman* and the *Bitdefender* engines
- F-Secure uses engines such as *Orion*, *AVP*, *Libra* and others.

Some products may offer additional options/features. Please try them on your own system before making a purchase decision based on these tests. There are also many other program features and important factors (e.g. compatibility, graphical user interface, speed, language, price, update frequence, spyware detection, ease of management, system resource usage, etc.) to consider. Although extremely important, the detection rate of a product is only one aspect of a complete Anti-Virus product. We suggest readers to research other independent test results, as the results provided by independent labs are usually quite consistent and do not differ much from each other - depending on the type of test and the quality of the test samples used. We encourage our readers to also have a look at tests done by other test-centers with large collections of verified malware, as tests based solely on viruses listed on the Wildlist (ITW-Tests) give a fairly limited view of the detection capabilties, as do some magazine tests which only use very small test sets.

[1] Panda decided to do not take part in the tests of August and November, because they were not happy about the results their product reached in the previous tests.
[2] Microsoft OneCare will be included in our tests starting from 2007.
[3] A comparison test between F-Prot v3 and the new F-Prot v4 will be released soon on www.av-comparatives.org .
[4] The new version of AVK - which will use the Kaspersky and Avast engines - will be tested starting from 2007.

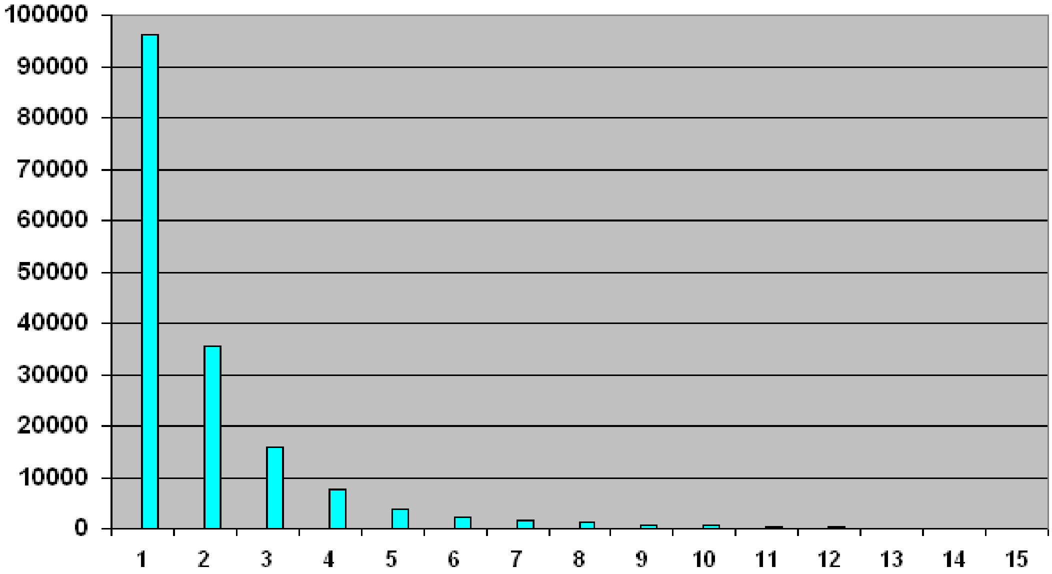
3. Progress made since last comparative

Missed samples from the February 2006 comparative detected/added after 3, 4, 5 and 6 months by the respective companies:



4. Non-detected samples in the test-bed of August 2006

About 70% of the test-set is detected by all 15 scanners. The non-detected samples are as follow:



This figure shows the number of scanners that missed the given proportion of samples in the test-set. All samples in the set were detected by at least one scanner. For instance 14 scanners missed more than 45 samples.

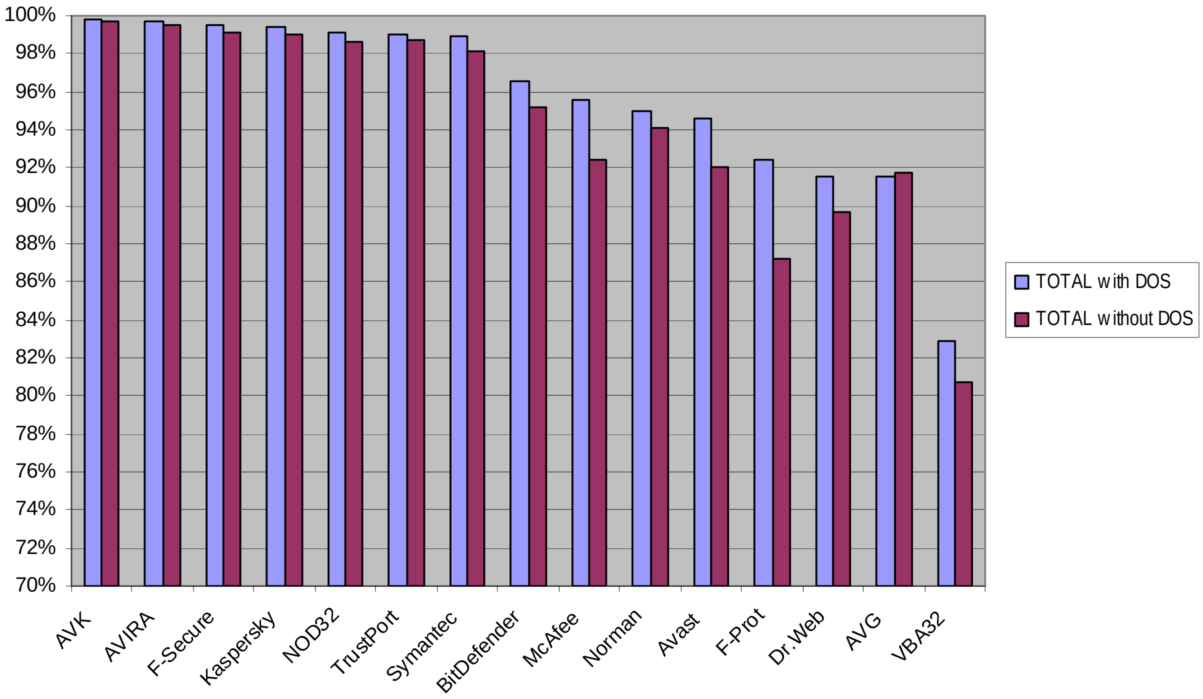
5. Test results

Company		AVIRA		G DATA Security		Alwil Software		GriSoft	
Product		**AntiVir PE Premium**		**AntiVirusKit (AVK)**		**Avast! Professional**		**AVG Professional**	
Program version		7.01.02		16.0.7		4.7.869		7.1.405	
Engine / signature version		6.35.01.60		16.8976 / 16.5352		0631-3		268.10.7 / 411	
Number of virus records		*477.718*		*unknown*		*unknown*		*unknown*	
On-demand detection of over 205000 dialers (*)		*excellent*		*excellent*		*excellent*		*excellent*	
On-demand detection of polymorphic viruses (**)			*10 of 10*		*8 of 10*		*2 of 10*		*1 of 10*
Certification level reached in this test		ADVANCED+		ADVANCED+		ADVANCED		STANDARD	
On-demand detection of virus/malware									
DOS viruses/malware	*230.456*	*230.337*	*99,95%*	*230.340*	*99,95%*	*226.213*	*98,16%*	*210.520*	*91,35%*
Windows viruses	21.985	21.608	98,29%	21.964	99,90%	20.558	93,51%	18.600	84,60%
Macro viruses	38.295	38.282	99,97%	38.294	~100%	37.738	98,55%	38.245	99,87%
Script viruses/malware	7.865	7.722	98,18%	7.811	99,31%	6.691	85,07%	3.330	42,34%
Worms	28.573	28.504	99,76%	28.553	99,93%	27.283	95,49%	27.172	95,10%
Backdoors	104.816	104.610	99,80%	104.446	99,65%	98.655	94,12%	100.812	96,18%
Trojans	110.648	110.023	99,44%	110.168	99,57%	97.759	88,35%	102.537	92,67%
other malware	6.801	6.689	98,35%	6.732	98,99%	5.389	79,24%	3.417	50,24%
OtherOS viruses/malware	2.356	2.321	98,51%	2.352	99,83%	1.585	67,28%	530	22,50%
TOTAL	**321.339**	319.759	**99,51%**	320.320	**99,68%**	295.658	**92,01%**	294.643	**91,69%**
Total with DOS viruses/malware	551.795	550.096	99,69%	550.660	99,79%	521.871	94,58%	505.163	91,55%

Company		Softwin		Doctor Web		Frisk Software		F-Secure	
Product		**BitDefender Prof.+**		**Dr. Web**		**F-Prot Anti-Virus**		**F-Secure Anti-Virus**	
Program version		9.5		4.33.4.07270		3.16f		6.12.90	
Engine / signature version		7.08453		4.33.2.06080		3.16.13		6.11.11450	
Number of virus records		*458.019*		*134.337*		*313.508*		*unknown*	
On-demand detection of over 205000 dialers (*)		*excellent*		*high*		*not present*		*not present*	
On-demand detection of polymorphic viruses (**)			*5 of 10*		*7 of 10*		*4 of 10*		*6 of 10*
Certification level reached in this test		ADVANCED		STANDARD		STANDARD		ADVANCED+	
On-demand detection of virus/malware									
DOS viruses/malware	*230.456*	*226.718*	*98,38%*	*220.770*	*95,80%*	*229.879*	*99,75%*	*230.428*	*99,99%*
Windows viruses	21.985	20.660	93,97%	19.984	90,90%	20.918	95,15%	21.942	99,80%
Macro viruses	38.295	38.201	99,75%	38.253	99,89%	38.290	99,99%	38.294	~100%
Script viruses/malware	7.865	7.425	94,41%	5.859	74,49%	7.329	93,18%	7.764	98,72%
Worms	28.573	28.185	98,64%	27.080	94,77%	26.338	92,18%	28.455	99,59%
Backdoors	104.816	102.116	97,42%	98.180	93,67%	91.834	87,61%	103.878	99,11%
Trojans	110.648	101.288	91,54%	93.592	84,59%	88.008	79,54%	109.028	98,54%
other malware	6.801	6.305	92,71%	4.231	62,21%	5.975	87,85%	6.682	98,25%
OtherOS viruses/malware	2.356	1.772	75,21%	1.092	46,35%	1.450	61,54%	2.323	98,60%
TOTAL	**321.339**	305.952	**95,21%**	288.271	**89,71%**	280.142	**87,18%**	318.366	**99,07%**
Total with DOS viruses/malware	551.795	532.670	96,53%	509.041	92,25%	510.021	92,43%	548.794	99,46%

Company		Kaspersky Labs		McAfee		ESET		Norman ASA	
Product		**Kaspersky AV**		**McAfee VirusScan**		**NOD32 Anti-Virus**		**NormanVirusControl**	
Program version		6.0.0.303		11.0.209		2.51.26		5.81	
Engine / signature version		*N/A*		5100.0194 / 4823		1.1695		5.90.23	
Number of virus records		*213.193*		*203.043*		*unknown*		*unknown*	
On-demand detection of over 205000 dialers (*)		*excellent*		*excellent*		*excellent*		*mediocre*	
On-demand detection of polymorphic viruses (**)			*6 of 10*		*5 of 10*		*8 of 10*		*1 of 10*
Certification level reached in this test		ADVANCED+		ADVANCED		ADVANCED+		ADVANCED	
On-demand detection of virus/malware									
DOS viruses/malware	*230.456*	*230.427*	*99,99%*	*230.445*	*~100%*	*229.786*	*99,71%*	*222.065*	*96,36%*
Windows viruses	21.985	21.942	99,80%	21.878	99,51%	21.743	98,90%	18.052	82,11%
Macro viruses	38.295	38.294	~100%	38.295	100%	38.292	99,99%	38.274	99,95%
Script viruses/malware	7.865	7.733	98,32%	7.438	94,57%	7.709	98,02%	6.910	87,86%
Worms	28.573	28.455	99,59%	28.221	98,77%	28.487	99,70%	26.777	93,71%
Backdoors	104.816	103.877	99,10%	98.086	93,58%	103.546	98,79%	102.253	97,55%
Trojans	110.648	109.030	98,54%	94.847	85,72%	108.324	97,90%	104.582	94,52%
other malware	6.801	6.659	97,91%	6.024	88,58%	6.627	97,44%	4.863	71,50%
OtherOS viruses/malware	2.356	2.323	98,60%	2.131	90,45%	2.159	91,64%	589	25,00%
TOTAL	**321.339**	318.313	**99,06%**	296.920	**92,40%**	316.887	**98,61%**	302.300	**94,08%**
Total with DOS viruses/malware	551.795	548.740	99,45%	527.365	95,57%	546.673	99,07%	524.365	95,03%

Company		Symantec		AEC		VirusBlokAda	
Product		**Norton Anti-Virus**		**TrustPort AV WS**		**VBA32 Workstation**	
Program version		12.2.0.13		2.0.0.843		3.11.0	
Engine / signature version		80807		*N/A*		*N/A*	
Number of virus records		*72.713*		*unknown*		*unknown*	
On-demand detection of over 205000 dialers (*)		*excellent*		*excellent*		*high*	
On-demand detection of polymorphic viruses (**)			*10 of 10*		*5 of 10*		*1 of 10*
Certification level reached in this test		**ADVANCED+**		**ADVANCED+**			
On-demand detection of virus/malware							
DOS viruses/malware	*230.456*	*230.250*	*99,91%*	*229.514*	*99,59%*	*197.982*	*85,91%*
Windows viruses	21.985	21.954	99,86%	21.517	97,87%	14.855	67,57%
Macro viruses	38.295	38.292	99,99%	38.288	99,98%	33.525	87,54%
Script viruses/malware	7.865	7.704	97,95%	7.666	97,47%	4.351	55,32%
Worms	28.573	28.427	99,49%	28.422	99,47%	25.374	88,80%
Backdoors	104.816	103.613	98,85%	104.061	99,28%	90.613	86,45%
Trojans	110.648	106.854	96,57%	108.864	98,39%	86.478	78,16%
other malware	6.801	6.285	92,41%	6.414	94,31%	4.093	60,18%
OtherOS viruses/malware	2.356	2.217	94,10%	1.887	80,09%	236	10,02%
TOTAL	**321.339**	315.346	**98,13%**	317.119	**98,69%**	259.525	**80,76%**
Total with DOS viruses/malware	551.795	545.596	98,88%	546.633	99,06%	457.507	82,91%



6. Summary results

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

1.	AVK*	99.9%
2.	F-Secure*, Kaspersky	99,7%
3.	Symantec	99.5%
4.	AVIRA	99.4%
5.	NOD32	99.3%
6.	McAfee	98.9%
7.	TrustPort*	98.7%
8.	BitDefender	97.1%
9.	F-Prot	95.2%
10.	Avast	94.7%
11.	Dr.Web	93.1%
12.	Norman	91.4%
13.	AVG	88.7%
14.	VBA32	79.1%

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

1.	AVK*, AVIRA	99.6%
2.	F-Secure*, Kaspersky	98.8%
3.	TrustPort*	98.7%
4.	NOD32	98.3%
5.	Symantec	97.5%
6.	Norman	95.2%
7.	BitDefender	94.4%
8.	AVG	93.0%
9.	Avast	90.8%
10.	McAfee	89.5%
11.	Dr.Web	88.2%
12.	F-Prot	83.6%
13.	VBA32	81.5%

(c) Total detection rates (without the DOS category):

1.	AVK*	99.68%
2.	AVIRA	99.51%
3.	F-Secure*	99.07%
4.	Kaspersky	99.06%
5.	TrustPort*	98.69%
6.	NOD32	98.61%
7.	Symantec	98.13%
8.	BitDefender	95.21%
9.	Norman	94.08%
10.	McAfee	92.40%
11.	Avast	92.01%
12.	AVG	91.69%
13.	Dr.Web	89.71%
14.	F-Prot	87.18%
15.	VBA32	80.76%

(d) Total detection rates with ‘DOS’ viruses/malware:

1.	AVK*	99.79%
2.	AVIRA	99.69%
3.	F-Secure*	99.46%
4.	Kaspersky	99.45%
5.	NOD32	99.07%
6.	TrustPort*	99.06%
7.	Symantec	98.88%
8.	BitDefender	96.53%
9.	McAfee	95.57%
10.	Norman	95.03%
11.	Avast	94.58%
12.	F-Prot	92.43%
13.	Dr.Web	92.25%
14.	AVG	91.55%
15.	VBA32	82.91%

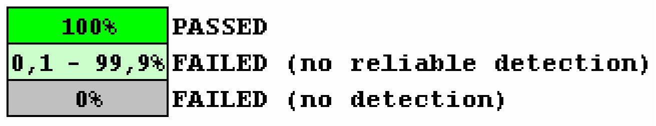
(*) AVK, F-Secure and TrustPort are multi-engine products.

Because VBA32 did not reach in the two on-demand tests of February and August 2006 at least the STANDARD level, its reinclusion in the regular test-series of 2007 have to be re-evaluated by the Tester.

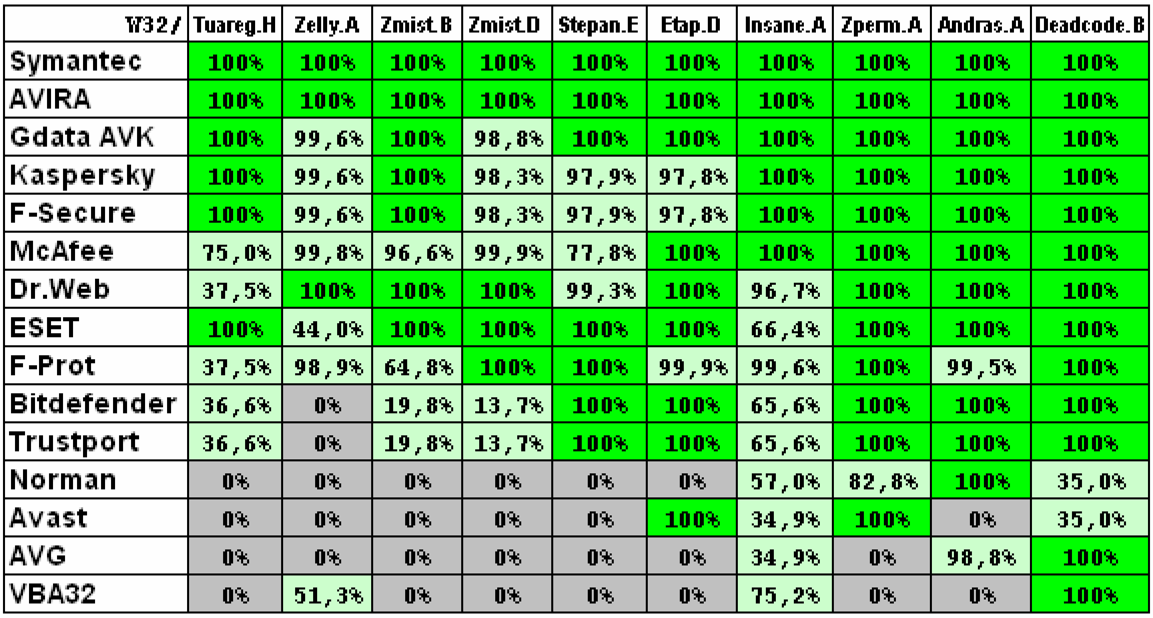
Important note: Please try anti-virus products on your own system before making a purchase decision based on these tests.

7. Detection rates against some polymorphic viruses

The test set includes some thousands of replicants for each of the following 10 complex highly polymorphic viruses: W32/Andras.A, W32/Deadcode.B, W32/Etap.D, W32/Insane.A, W32/Stepan.E, W32/Tuareg.H, W32/Zelly.A, W32/Zmist.B, W32/Zmist.D and W32/Zperm.A. Those 10 viruses are all known to the AV vendors and variants have been submitted several times to the participating companies in the past – additionally, they are the same viruses also used in the test done in February. The polymorphic test evaluates the quality of the detection routines for polymorphic viruses – it reflects the ability to detect difficult malware. In this polymorphic test only exact detections (e.g. virus family name) were counted due the test scope. Scores under 100% of a polymorphic virus are considered as failed detection or not reliable detection, as even one missed replicant can cause a reinfection.



100%	PASSED
0,1 - 99,9%	FAILED (no reliable detection)
0%	FAILED (no detection)



W32/	Tuareg.H	Zelly.A	Zmist.B	Zmist.D	Stepan.E	Etap.D	Insane.A	Zperm.A	Andras.A	Deadcode.B
Symantec	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
AVIRA	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
Gdata AVK	100%	99,6%	100%	98,8%	100%	100%	100%	100%	100%	100%
Kaspersky	100%	99,6%	100%	98,3%	97,9%	97,8%	100%	100%	100%	100%
F-Secure	100%	99,6%	100%	98,3%	97,9%	97,8%	100%	100%	100%	100%
McAfee	75,0%	99,8%	96,6%	99,9%	77,8%	100%	100%	100%	100%	100%
Dr.Web	37,5%	100%	100%	100%	99,3%	100%	96,7%	100%	100%	100%
ESET	100%	44,0%	100%	100%	100%	100%	66,4%	100%	100%	100%
F-Prot	37,5%	98,9%	64,8%	100%	100%	99,9%	99,6%	100%	99,5%	100%
Bitdefender	36,6%	0%	19,8%	13,7%	100%	100%	65,6%	100%	100%	100%
Trustport	36,6%	0%	19,8%	13,7%	100%	100%	65,6%	100%	100%	100%
Norman	0%	0%	0%	0%	0%	0%	57,0%	82,8%	100%	35,0%
Avast	0%	0%	0%	0%	0%	100%	34,9%	100%	0%	35,0%
AVG	0%	0%	0%	0%	0%	0%	34,9%	0%	98,8%	100%
VBA32	0%	51,3%	0%	0%	0%	0%	75,2%	0%	0%	100%

The results of the polymorphic test are of importance, because they show how flexible an anti-virus scan engine is and how good the detection quality of complex viruses is. In some cases some Anti-Virus products score 0% not because they are not aware of the existence of this virus, but because to detect such viruses with the technology/engine of their product it may be necessary to rewrite the engine, or because such an alteration to their engine would mean a significantly slow-down of the scanning speed. Because of this, they may not add detection for such complex viruses. Anti-virus products which have a 100% reliable detection rate for those complex viruses show a higher detection quality and engine flexibility, as they are able to protect against those viruses without too many problems. It is worth bearing these results in mind when you are looking at the scanning speed rates – an AV product could be fast in scanning but will not provide a reliable protection against complex viruses. Better is an AV product which is capable of fast scanning and also providing reliable detection of complex viruses.

8. Certification levels reached in this test

We provide a 3-level-ranking-system (STANDARD, ADVANCED and ADVANCED+). Overviews of levels reached in past can be found on our website (http://www.av-comparatives.org/seiten/overview.html).
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.

CERTIFICATION LEVELS	**PRODUCTS** (in alphabetical order)
AV comparatives ADVANCED+ ★★★ Aug 06 on-demand detection test	**AVIRA** **F-Secure** **Gdata AVK** **Kaspersky** **NOD32** **Symantec** **TrustPort**
AV comparatives ADVANCED ★★ Aug 06 on-demand detection test	**Avast** **BitDefender** **McAfee** **Norman**
AV comparatives STANDARD ★ Aug 06 on-demand detection test	**AVG** **Dr.Web** **F-Prot**
No certification	**VBA32**

All products in the ADVANCED+ category offer a very high level of on-demand detection. Selection of a product from this category should not be based on detection score alone. For example the quality of support, easy of use and system resources consumed when the product is in use should be considered when selecting a product.
Products in the ADVANCED category offer a high level of detection, but slightly less than those in the ADVANCED+. These products are suitable for many users. 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 & 2 certified (www.westcoastlabs.org), or consistently achieve Virus Bulletin 100% awards (www.virusbtn.com).
Another very good source for independent anti-virus software testing is AV-Test.org (www.av-test.org). AV-Test.org test results can be found in various magazines.
Tests which are based purely on the Wildlist (www.wildlist.org) are not necessarily as meaningful as tests based on a wide range and large collection of malware which best tests the overall detection capabilities of Anti-Virus products.
At the end of the year - we may maybe try to determine the "winner" of Best Anti-Virus product of the year.

9. Copyright and Disclaimer

This publication is Copyright (c) 2006 by AV-Comparatives. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of Andreas Clementi, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

Andreas Clementi, AV-Comparatives (August 2006)