Anti-Virus Comparative No.9

On-demand detection of malicious software

Date: February 2006 (2006-02)

Last revision of this report: 1st March 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 (http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf). The products included in our tests constitute a selection of some very good anti-virus software with high on-demand detection rates, as this is one of the requirements needed to get 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 which did not want to participate this year were not tested.

2. Tested products

All products were updated on the 6th February 2006 and set to use the best possible settings. The Malware sets and system Test-beds were frozen the 2nd February 2006.

Avast! 4.6.763 Professional Edition
AVG Professional 7.1.375
AVIRA AntiVir Personal Edition Premium 7.00.00.21
BitDefender Anti-Virus 9.0 Professional Plus
Dr.Web Anti-Virus for Windows 95-XP 4.33.0.09293
ESET NOD32 Anti-Virus 2.51.20
F-Prot Anti-Virus for Windows 3.16f
F-Secure Anti-Virus 6.12 (*)
Gdata AntiVirusKit (AVK) 16.0.5 (*)
Kaspersky Anti-Virus Personal Pro 5.0.391
McAfee VirusScan 10.0.21 (**)
Norman Virus Control 5.81
Panda Platinum Internet Security 10.01.02
Symantec Norton Anti-Virus 12.1.0.20
TrustPort Antivirus Workstation 1.5.0.752 (*)
VBA32 Workstation 3.10.5

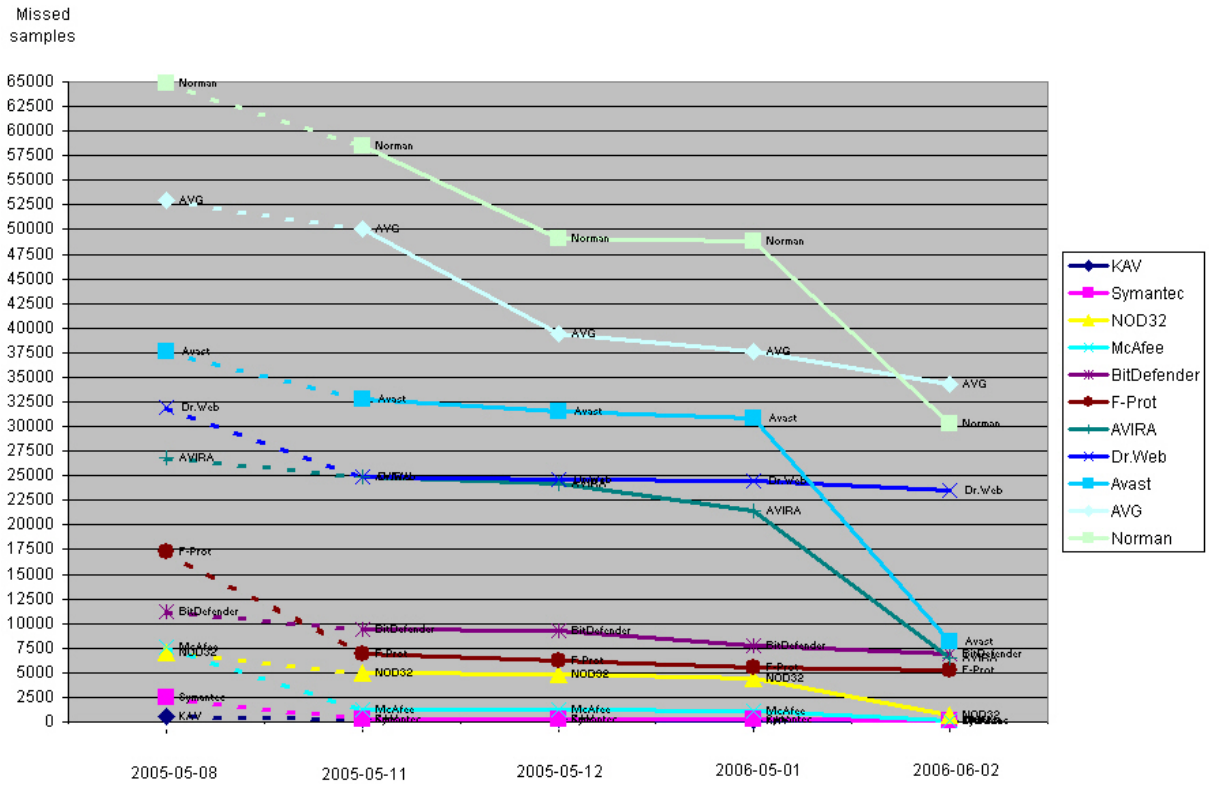
(*) AVK, F-Secure and TrustPort are multi-engine products:
- AVK contains the *Kaspersky* and *Bitdefender* engines
- TrustPort contains the *Norman* and the *Bitdefender* engines
- F-Secure uses engines such as *Orion*, *AVP*, *Libra* and others.

(**) McAfee was tested by using the 5000 RC engine.

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 (examples under point 7.), as the results provided by independent labs are usually quite consistent and do not differ much from each other - depending from the type of test and of the quality of the test samples used. We encourage our readers to have a look also on 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 quite limited view of the detection capabilties, as do some magazine tests which only use very small test sets.

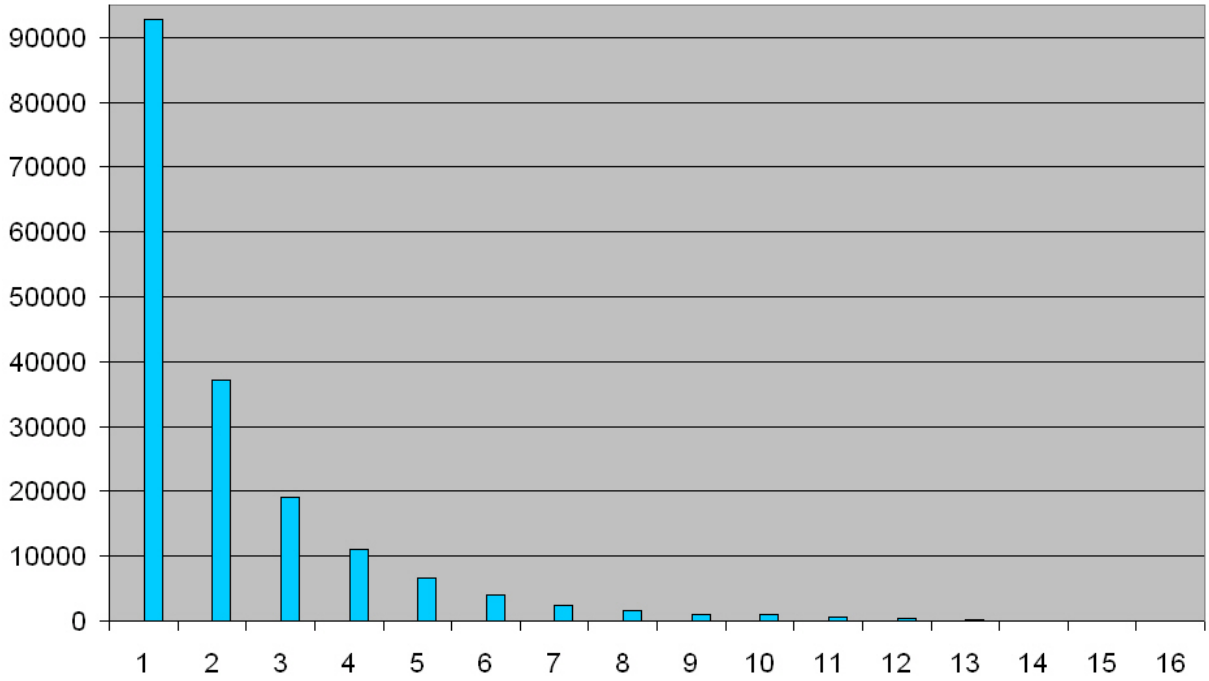
3. Progresses made since last comparative

Missed samples from the August 2005 comparative detected/added after 3, 4, 5 and 6 months by the respective companies:



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

About 62% of the test-set is detected by all 16 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 15 scanners missed more than 70 samples.

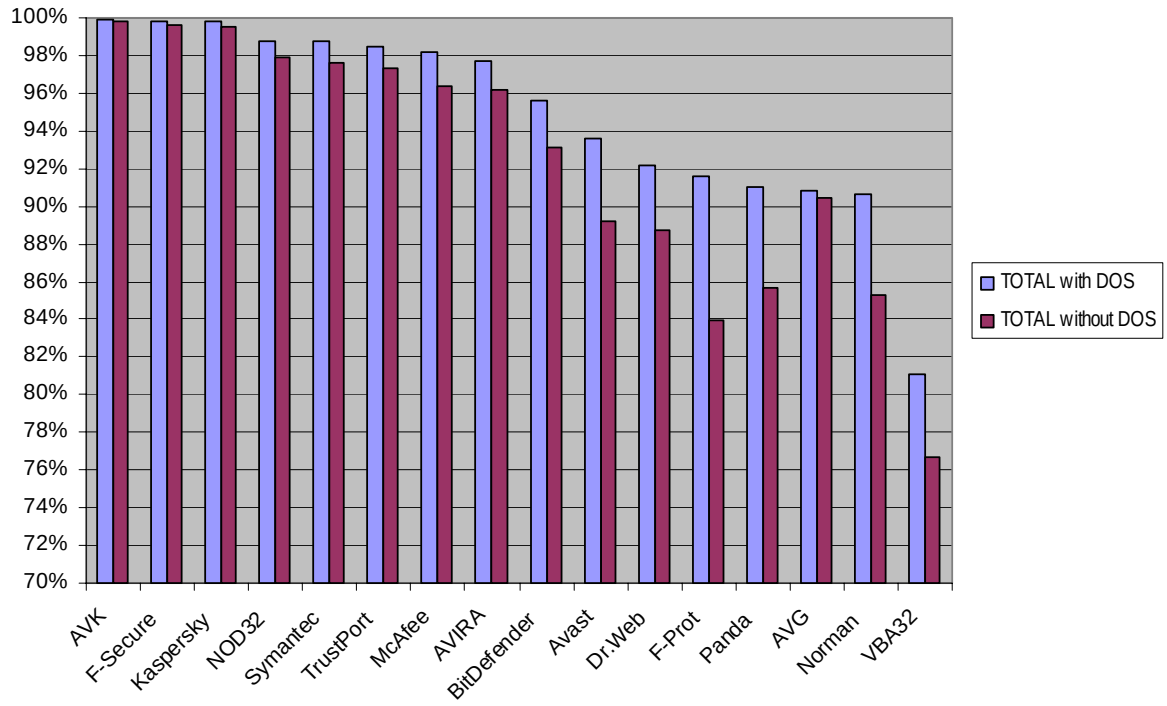
5. Test results

Company		AVIRA (aka H+B EDV)		G DATA Security		Alwil Software		GriSoft	
Product		**AntiVir PE Premium**		**AntiVirusKit (AVK)**		**Avast! Professional**		**AVG Professional**	
Program version		7.00.00.21		16.0.5		4.6.763		7.1.375	
Engine / signature version		6.33.0.36 / 6.33.0.210		16.5355 / 16.2619		0606-1		267.15.2/252	
Number of virus records		307.383		*unknown*		*unknown*		*unknown*	
On-demand detection of dialers (*)		*excellent*		*excellent*		*high*		*excellent*	
Certification level reached in this test		ADVANCED+		ADVANCED+		ADVANCED		STANDARD	
On-demand detection of virus/malware									
DOS viruses/malware	*231.088*	*229.494*	*99,31%*	*230.960*	*99,94%*	*226.849*	*98,17%*	*210.583*	*91,13%*
Windows viruses	20.546	18.798	91,49%	20.328	98,94%	19.102	92,97%	17.015	82,81%
Macro viruses	37.181	37.143	99,90%	37.181	100%	36.644	98,56%	37.137	99,88%
Script viruses/malware	7.449	5.712	76,68%	7.430	99,74%	6.652	89,30%	3.127	41,98%
Worms	23.398	22.573	96,47%	23.376	99,91%	22.352	95,53%	22.188	94,83%
Backdoors	78.092	77.181	98,83%	78.027	99,92%	71.076	91,02%	76.116	97,47%
Trojans	69.008	66.695	96,65%	68.992	99,98%	55.447	80,35%	62.364	90,37%
other malware	5.912	4.880	82,54%	5.874	99,36%	4.713	79,72%	2.129	36,01%
OtherOS viruses/malware	2.085	1.402	67,24%	2.072	99,38%	1.458	69,93%	376	18,03%
TOTAL	**243.671**	234.384	**96,19%**	243.280	**99,84%**	217.444	**89,24%**	220.452	**90,47%**
Total with DOS viruses/malware	474.759	463.878	97,71%	474.240	99,89%	444.293	93,58%	431.035	90,79%
On-demand detection of polymorphic viruses (**)			*90,7%*		*99,9%*		*26,7%*		*10,0%*

Company		Softwin		Doctor Web		Frisk Software		F-Secure	
Product		**BitDefender Prof.+**		**Dr. Web**		**F-Prot Anti-Virus**		**F-Secure Anti-Virus**	
Program version		9.0 (Build 9)		4.33.0.09293		3.16f		6.12.90	
Engine / signature version		7.05596		4.33.0.10250		3.16.13		6.11.11450	
Number of virus records		269.149		102.156		232.823		*unknown*	
On-demand detection of dialers (*)		*excellent*		*high*		*not present*		*not present*	
Certification level reached in this test		ADVANCED		STANDARD		STANDARD		ADVANCED+	
On-demand detection of virus/malware									
DOS viruses/malware	*231.088*	*227.290*	*98,36%*	*221.422*	*95,82%*	*230.561*	*99,77%*	*231.028*	*99,97%*
Windows viruses	20.546	19.152	93,22%	18.576	90,41%	18.667	90,85%	20.513	99,84%
Macro viruses	37.181	36.791	98,95%	37.144	99,90%	37.174	99,98%	37.181	100%
Script viruses/malware	7.449	6.891	92,51%	5.709	76,64%	6.802	91,31%	7.405	99,41%
Worms	23.398	22.797	97,43%	22.077	94,35%	21.101	90,18%	23.296	99,56%
Backdoors	78.092	73.934	94,68%	73.032	93,52%	65.656	84,08%	77.906	99,76%
Trojans	69.008	60.650	87,89%	55.188	79,97%	49.653	71,95%	68.488	99,25%
other malware	5.912	5.159	87,26%	3.578	60,52%	4.179	70,69%	5.803	98,16%
OtherOS viruses/malware	2.085	1.447	69,40%	977	46,86%	1.232	59,09%	2.065	99,04%
TOTAL	**243.671**	226.821	**93,08%**	216.281	**88,76%**	204.464	**83,91%**	242.657	**99,58%**
Total with DOS viruses/malware	474.759	454.111	95,65%	437.703	92,19%	435.025	91,63%	473.685	99,77%
On-demand detection of polymorphic viruses (**)			*79,5%*		*93,3%*		*90,0%*		*99,4%*

Company		Kaspersky Labs		McAfee		ESET		Norman ASA	
Product		**KAV Personal Pro**		**McAfee VirusScan**		**NOD32 Anti-Virus**		**NormanVirusControl**	
Program version		5.0.391		10.0.21		2.51.20		5.81	
Engine / signature version		*N/A*		5.0.00 / 4690		1.1395		5.83.11	
Number of virus records		175.260		175.087		*unknown*		*unknown*	
On-demand detection of dialers (*)		*excellent*		*excellent*		*excellent*		*low*	
Certification level reached in this test		ADVANCED+		ADVANCED+		ADVANCED+		STANDARD	
On-demand detection of virus/malware									
DOS viruses/malware	*231.088*	*231.029*	*99,97%*	*231.073*	*99,99%*	*230.399*	*99,70%*	*222.625*	*96,34%*
Windows viruses	20.546	20.513	99,84%	20.501	99,78%	20.468	99,62%	16.285	79,26%
Macro viruses	37.181	37.181	100%	37.180	100%	37.164	99,95%	37.147	99,91%
Script viruses/malware	7.449	7.386	99,15%	7.201	96,67%	7.269	97,58%	2.591	34,78%
Worms	23.398	23.294	99,56%	23.335	99,73%	23.288	99,53%	18.100	77,36%
Backdoors	78.092	77.906	99,76%	75.786	97,05%	76.946	98,53%	74.192	95,01%
Trojans	69.008	68.494	99,26%	63.569	92,12%	66.445	96,29%	57.845	83,82%
other malware	5.912	5.788	97,90%	5.468	92,49%	5.100	86,27%	1.228	20,77%
OtherOS viruses/malware	2.085	2.065	99,04%	1.894	90,84%	1.843	88,39%	508	24,36%
TOTAL	**243.671**	242.627	**99,57%**	234.934	**96,41%**	238.523	**97,89%**	207.896	**85,32%**
Total with DOS viruses/malware	474.759	473.656	99,77%	466.007	98,16%	468.922	98,77%	430.521	90,68%
On-demand detection of polymorphic viruses (**)			*99,4%*		*84,0%*		*94,3%*		*36,0%*

Company		Symantec		Panda Software		AEC		VirusBlokAda	
Product		**Norton Anti-Virus**		**Panda Anti-Virus**		**TrustPort AV WS**		**VBA32 Workstation**	
Program version		12.1.0.20		10.01.02		1.5.0.752		3.10.5	
Engine / signature version		80206u		*N/A*		*N/A*		*N/A*	
Number of virus records		72.044		110.254		*unknown*		163.237	
On-demand detection of dialers (*)		*excellent*		*excellent*		*excellent*		*high*	
Certification level reached in this test		**ADVANCED+**		**STANDARD**		**ADVANCED+**			
On-demand detection of virus/malware									
DOS viruses/malware	*231.088*	*230.847*	*99,90%*	*223.429*	*96,69%*	*230.148*	*99,59%*	*197.847*	*85,62%*
Windows viruses	20.546	20.526	99,90%	17.736	86,32%	20.051	97,59%	13.414	65,29%
Macro viruses	37.181	37.178	99,99%	37.065	99,69%	37.177	99,99%	27.481	73,91%
Script viruses/malware	7.449	7.227	97,02%	5.813	78,04%	6.962	93,46%	2.379	31,94%
Worms	23.398	23.192	99,12%	20.623	88,14%	23.022	98,39%	17.754	75,88%
Backdoors	78.092	76.723	98,25%	68.817	88,12%	76.815	98,36%	68.207	87,34%
Trojans	69.008	65.618	95,09%	53.364	77,33%	66.485	96,34%	54.675	79,23%
other malware	5.912	5.449	92,17%	4.020	68,00%	5.211	88,14%	2.749	46,50%
OtherOS viruses/malware	2.085	1.942	93,14%	1.383	66,33%	1.488	71,37%	233	11,18%
TOTAL	**243.671**	237.855	**97,61%**	208.821	**85,70%**	237.211	**97,35%**	186.892	**76,70%**
Total with DOS viruses/malware	474.759	468.702	98,72%	432.250	91,05%	467.359	98,44%	384.739	81,04%
On-demand detection of polymorphic viruses (**)			*100%*		*37,0%*		*84,9%*		*15,1%*



6. Summary results

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

1. F-Secure*, Kaspersky, AVK* 99.9%
2. McAfee 99.8%
3. Symantec 99.7%
4. NOD32 99.6%
5. TrustPort* 99.1%
6. F-Prot 98.1%
7. AVIRA 97.9%
8. BitDefender 97.7%
9. Avast 97.3%
10. Panda, Dr.Web 95.1%
11. Norman 92.4%
12. AVG 90.3%
13. VBA32 80.5%

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

1.	AVK*	99.9%
2.	F-Secure*, Kaspersky	99.5%
3.	AVIRA	97.2%
4.	NOD32, TrustPort*	97.1%
5.	Symantec	96.6%
6.	McAfee	94.7%
7.	AVG	91.9%
8.	BitDefender	91.3%
9.	Norman	87.1%
10.	Dr.Web	86.1%
11.	Avast	85.8%
12.	Panda	82.5%
13.	VBA32	82.1%
14.	F-Prot	78.1%

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

1.	AVK*	99.84%
2.	F-Secure*	99.58%
3.	Kaspersky	99.57%
4.	NOD32	97.89%
5.	Symantec	97.61%
6.	TrustPort*	97.35%
7.	McAfee	96.41%
8.	AVIRA	96.19%
9.	BitDefender	93.08%
10.	AVG	90.47%
11.	Avast	89.24%
12.	Dr.Web	88.76%
13.	Panda	85.70%
14.	Norman	85.32%
15.	F-Prot	83.91%
16.	VBA32	76.70%

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

1.	AVK*	99.89%
2.	F-Secure*, Kaspersky	99.77%
3.	NOD32	98.77%
4.	Symantec	98.72%
5.	TrustPort*	98.44%
6.	McAfee	98.16%
7.	AVIRA	97.71%
8.	BitDefender	95.65%
9.	Avast	93.58%
10.	Dr.Web	92.19%
11.	F-Prot	91.63%
12.	Panda	91.05%
13.	AVG	90.79%
14.	Norman	90.68%
15.	VBA32	81.04%

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

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

7. 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+ ★★★ Feb 06 on-demand detection test	AVIRA F-Secure GDATA AVK Kaspersky McAfee NOD32 Symantec TrustPort
AV comparatives ADVANCED ★★ Feb 06 on-demand detection test	Avast Bitdefender
AV comparatives STANDARD ★ Feb 06 on-demand detection test	AVG Dr.Web F-Prot Norman Panda
No certification	VBA32

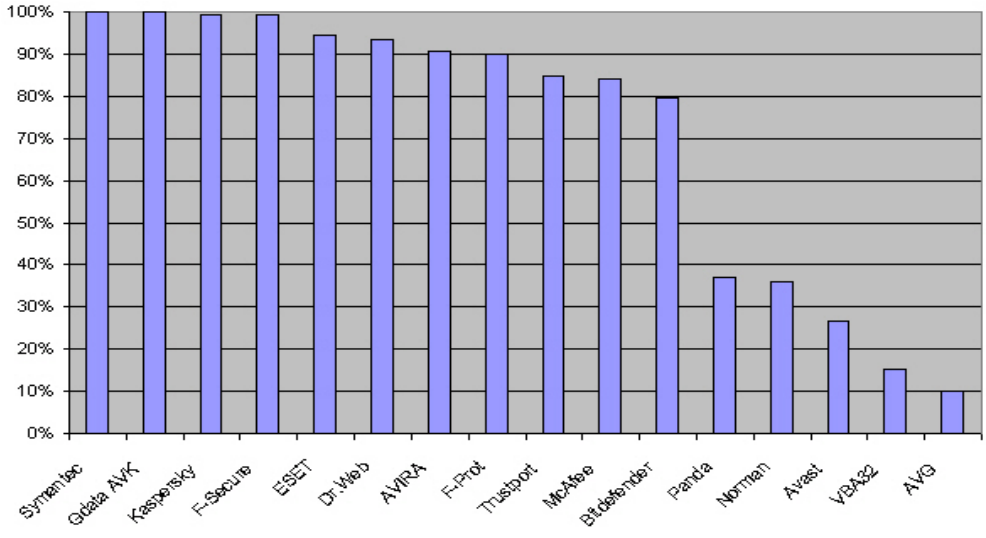
All products in the ADVANCED+ category offer a very high level of on-demand detection. Selection of a product from this category should not be based on detection score alone. For example the quality of support, easy of use and system resources consumed when the product is in use should be considered 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 certified (www.westcoastlabs.org/checkmarkcertification.asp), or consistently achieve Virus Bulletin 100% awards (www.virusbtn.com/vb100/archive).
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.

8. Additional Tests

Starting from the year 2006, we have included a small polymorphic test set in our on-demand tests. In the second part of the tests (which are performed in May and November), we will include a false-positive test along with the report of the retrospective tests.

The test set includes around a thousand replicants for each of the following 10 complex high polymorphic viruses[1]: 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 at least 1 year old and variants have been submitted several times to the participating companies in the past. None of the actual test replicants were or will be sent to any companies. The polymorphic test tries to evaluate any emulation engine of the anti-virus products or the quality of the detection routines for polymorphic viruses – it reflects the ability to detect difficult malware. This polymorphic test is an experimental introduction, so please do not pay too much attention to it at this stage – it will be more meaningful in the August report, when e.g. only exact detections (e.g. virus family name) will be counted and detection rates may be improved. Scores under 100% of a virus can be considered as failed detection or not reliable detection, as even one missed replicant can cause a reinfection.

	W32/	Tuareg.H	Zelly.A	Zmist.B	Zmist.D	Stepan.E	Deadcode.B	Etap.D	Insane.A	Andras.A	Zperm.A	TOTAL
1.	Symantec	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100,0%
2.	Gdata AVK	100%	99,6%	100%	99,9%	100%	100%	100%	100%	100%	100%	99,9%
3.	Kaspersky	100%	99,6%	100%	98,3%	97,9%	100%	97,8%	100%	100%	100%	99,4%
3.	F-Secure	100%	99,6%	100%	98,3%	97,9%	100%	97,8%	100%	100%	100%	99,4%
4.	ESET	100%	74,9%	100%	100%	100%	100%	100%	66,4%	100%	100%	94,3%
5.	Dr.Web	37,5%	100%	100%	100%	99,3%	100%	100%	96,7%	100%	100%	93,3%
6.	AVIRA	100%	100%	100%	100%	94,8%	12,5%	100%	100%	100%	100%	90,7%
7.	F-Prot	37,5%	98,9%	64,8%	100%	100%	100%	99,9%	100%	99,5%	100%	90,0%
8.	Trustport	65,5%	25,6%	94,7%	98,1%	100%	100%	100%	65,6%	100%	100%	84,9%
9.	McAfee	43,8%	99,8%	96,6%	99,9%	0%	100%	100%	100%	100%	100%	84,0%
10.	Bitdefender	36,6%	0%	94,7%	98,1%	100%	100%	100%	65,6%	100%	100%	79,5%
11.	Panda	0%	0,8%	0%	0%	99,3%	0%	4,9%	65,7%	100%	100%	37,0%
12.	Norman	35,8%	25,6%	0%	0%	21,6%	35,0%	0%	59,4%	100%	82,8%	36,0%
13.	Avast	0%	0%	0%	0%	0%	35,0%	100%	34,9%	0%	100%	26,7%
14.	VBA32	0%	0%	0,7%	0,9%	0%	0%	0%	49,4%	0%	100%	15,1%
15.	AVG	0%	0%	0%	0%	0%	100%	0%	0%	0%	0%	10,0%



[1] Those viruses are currently not listed on the official Wildlist.

8.1 Other tests

AV-Comparatives does currently not provide scanning speed tests or comparisons of system resources usage, because such tests can be easily misinterpreted, as the results may differ much depending on which hardware the test is performed, which Operating System is used, the type of files used and the system configuration and program settings. As every user will have a different system configuration, we suggest that readers evaluate these aspects of the anti-virus software themselves. This can be done by using trial versions of AV software before choosing which solution best suits the individual system. We do not provide any price comparisons of AV software, as prices may differ from time to time, from country to country, from store to store and from version to version, etc. Please contact the vendors directly, or use their websites in order to discover which license type or product version applies to your needs.

9. Copyright and Disclaimer

Andreas Clementi, AV-Comparatives (February 2006)