Anti-Virus Comparative No.15

On-demand detection of malicious software

Date: August 2007 (2007-08)

Last revision of this report: 1st September 2007

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. Due the high interest of Anti-Virus vendors to participate in our tests, the needed minimum detection rate is 85% and limited to about 17 well-known and worldwide used home user anti-virus products.

2. Tested products

All products were updated on the 5th August 2007 and set to use the best possible settings. The Malware sets and system Test-beds were frozen the 3rd August 2007. The following 17 products were included in this test:

Avast! 4.7.1029 Professional Edition
AVG Anti-Malware 7.5.476
AVIRA AntiVir Personal Edition Premium 7.04.00.57
BitDefender Anti-Virus 10 Professional Plus
Dr.Web Anti-Virus for Windows 95-XP 4.44.0 (Beta)
eScan Anti-Virus 9.0.722.1 (*)
ESET NOD32 Anti-Virus 2.70.39
Fortinet FortiClient 3.0.459
F-Prot Anti-Virus for Windows 6.0.7.1
F-Secure Anti-Virus 2007 7.01.128 (*)
Gdata AntiVirusKit (AVK) 17.0.6353 (*)
Kaspersky Anti-Virus 7.0.0.125
McAfee VirusScan Plus 11.2.121
Microsoft Live OneCare 1.6.2111.30
Norman Virus Control 5.91
Symantec Norton Anti-Virus 14.0.3.3
TrustPort Antivirus Workstation 1.4.2.428 (*)

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

- AVK 2007 contains the *Kaspersky* and *Avast* engines
- eScan uses various own engines, including the *Kaspersky* engine
- F-Secure uses engines such as *Orion*, *Kaspersky*, *Libra, Pegasus* & others
- TrustPort contains the *Norman*, the *Bitdefender* and the *AVG* engines
- AVG Anti-Malware (and also AVG Internet Security) includes also the Ewido engine, therefore its results are higher and can not be applied to the AVG Free Edition or AVG Professional Edition

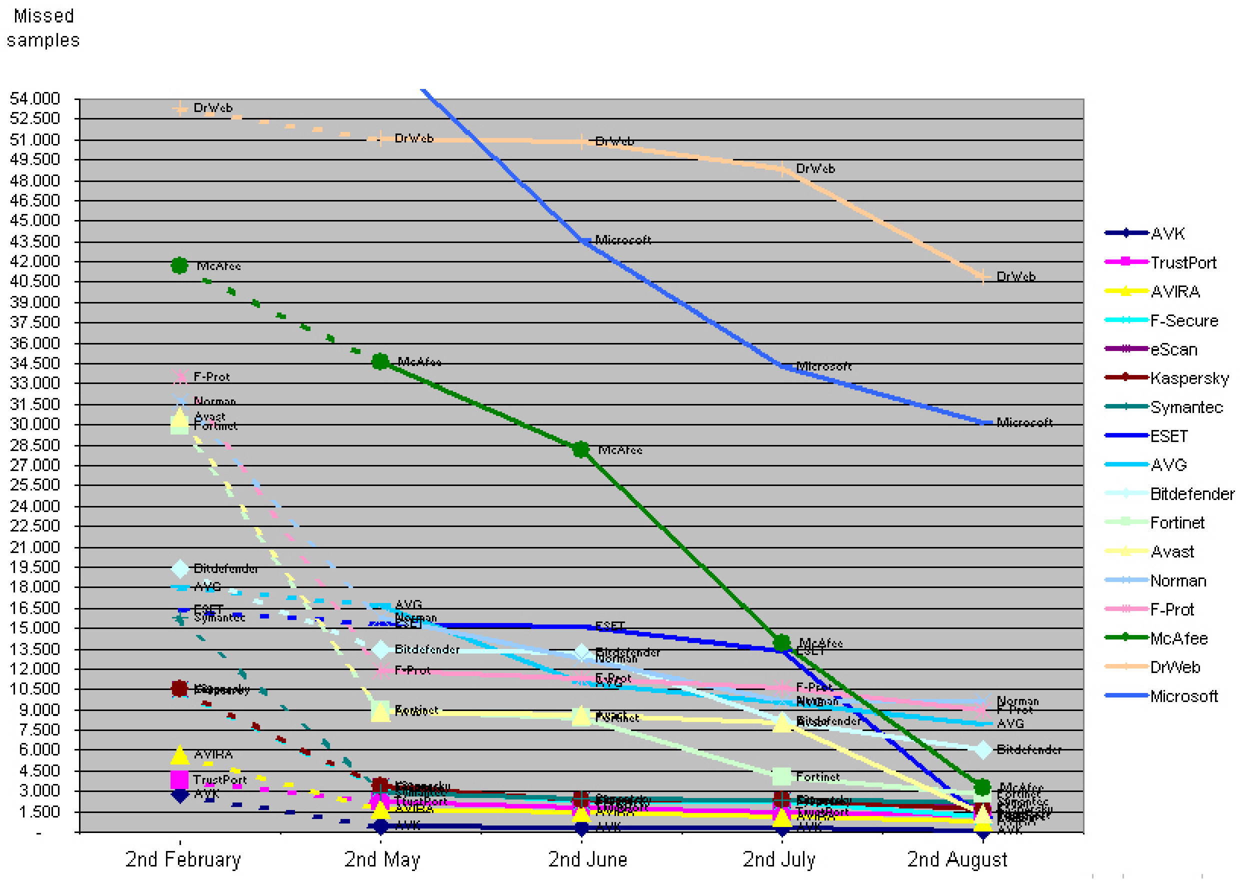
Some products may offer additional options/features. Please try them on your own system before making a purchase decision based on these tests. There are also many other program features and important factors (e.g. impact on system performance, compatibility, graphical user interface, language, price, update frequence, ease of management, 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.

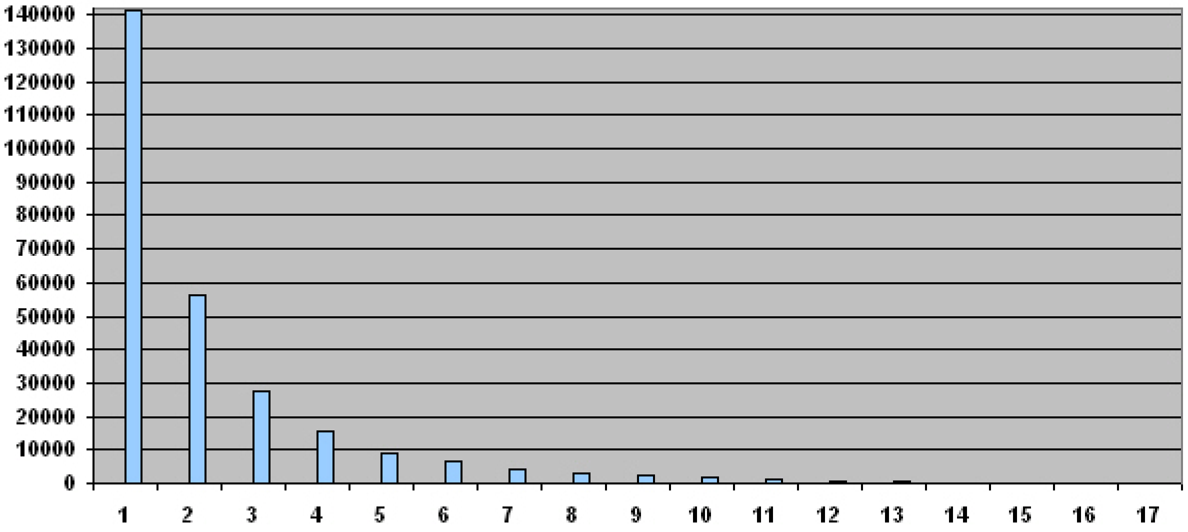
3. Progress made since last comparative

Missed samples from the February 2007 comparative detected/added after 3, 4, 5 and 6 months by the respective companies.



4. Non-detected samples in the test-bed of August 2007

About 67% of the main test-set is detected by all 17 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 16 scanners missed more than 50 samples.

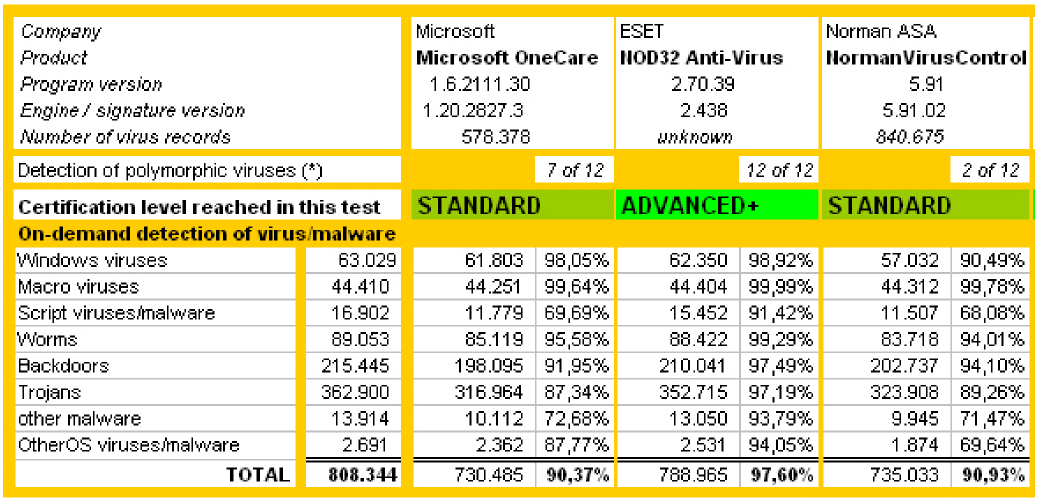
5. Test results

Company		AVIRA		G DATA Security		Alwil Software		GriSoft	
Product		**AntiVir PE Premium**		**AntiVirusKit (AVK)**		**avast! Professional**		**AVG Anti-Malware**	
Program version		7.04.00.57		17.0.6353		4.7.1029		7.5.476	
Engine / signature version		6.39.00.213		17.6648 / 17.326		0763-5		269.11.6 / 938	
Number of virus records		*1.000.742*		*unknown*		*unknown*		*unknown*	
Detection of polymorphic viruses (*)			*11 of 12*		*12 of 12*		*3 of 12*		*3 of 12*
Certification level reached in this test		ADVANCED+		ADVANCED+		ADVANCED		ADVANCED+	
On-demand detection of virus/malware									
Windows viruses	63.029	62.719	99,51%	62.798	99,63%	60.393	95,82%	60.993	96,77%
Macro viruses	44.410	44.355	99,88%	44.401	99,98%	43.696	98,39%	44.307	99,77%
Script viruses/malware	16.902	15.663	92,67%	16.449	97,32%	12.040	71,23%	13.126	77,66%
Worms	89.053	88.896	99,82%	88.913	99,84%	85.185	95,66%	87.761	98,55%
Backdoors	215.445	214.996	99,79%	214.013	99,34%	208.903	96,96%	213.271	98,99%
Trojans	362.900	361.173	99,52%	359.816	99,15%	345.848	95,30%	356.674	98,28%
other malware	13.914	13.503	97,05%	13.695	98,43%	11.414	82,03%	11.993	86,19%
OtherOS viruses/malware	2.691	2.571	95,54%	2.689	99,93%	2.383	88,55%	2.035	75,62%
TOTAL	**808.344**	803.876	**99,45%**	802.774	**99,31%**	769.862	**95,24%**	790.160	**97,75%**

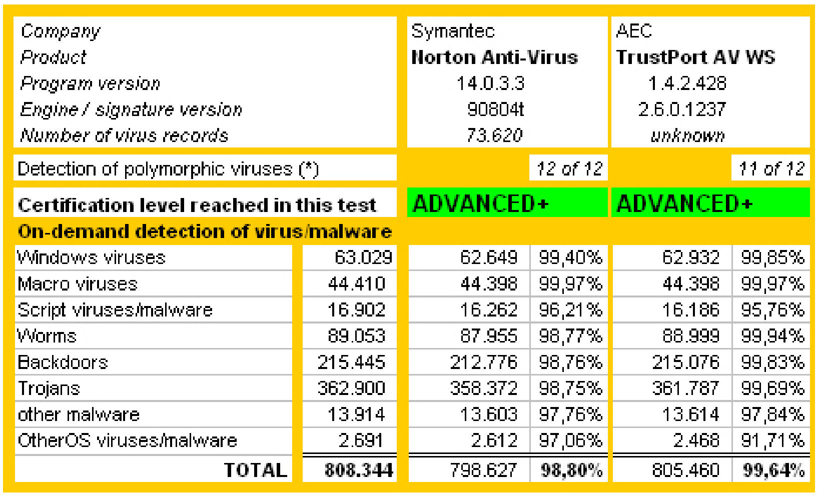
Company		Softwin		Doctor Web		MicroWorld		Fortinet	
Product		**BitDefender Prof.+**		**Dr. Web**		**eScan Anti-Virus**		**FortiClient**	
Program version		10.247		4.44.04060		9.0.722.1		3.0.459	
Engine / signature version		7.14211		4.44.0.07060		N/A		3.11 / 7.923	
Number of virus records		*752.905*		*227.123*		*unknown*		*unknown*	
Detection of polymorphic viruses (*)			*11 of 12*		*8 of 12*		*12 of 12*		*9 of 12*
Certification level reached in this test		ADVANCED+		STANDARD		ADVANCED+		STANDARD	
On-demand detection of virus/malware									
Windows viruses	63.029	61.805	98,06%	60.326	95,71%	62.448	99,08%	60.459	95,92%
Macro viruses	44.410	44.261	99,66%	44.333	99,83%	44.401	99,98%	44.219	99,57%
Script viruses/malware	16.902	15.385	91,02%	10.080	59,64%	16.238	96,07%	14.488	85,72%
Worms	89.053	88.500	99,38%	85.145	95,61%	88.317	99,17%	83.827	94,13%
Backdoors	215.445	209.124	97,07%	194.319	90,19%	209.227	97,11%	191.721	88,99%
Trojans	362.900	354.038	97,56%	322.090	88,75%	351.583	96,88%	318.414	87,74%
other malware	13.914	13.087	94,06%	8.911	64,04%	13.472	96,82%	12.006	86,29%
OtherOS viruses/malware	2.691	2.020	75,07%	1.277	47,45%	2.684	99,74%	2.240	83,24%
TOTAL	**808.344**	788.220	**97,51%**	726.481	**89,87%**	788.370	**97,53%**	727.374	**89,98%**

In accordance with Dr.Web, we tested exceptionally the beta version of Dr.Web 4.44. In accordance with Fortinet, FortiClient was tested without heuristic, due the high rate of false alarms caused by it (see report of May 2007).

Company		Frisk Software		F-Secure		Kaspersky Labs		McAfee	
Product		**F-Prot Anti-Virus**		**F-Secure Anti-Virus**		**Kaspersky AV**		**McAfee VirusScan+**	
Program version		6.0.7.1		7.01.128		7.0.0.125		11.2.121	
Engine / signature version		4.3.3		7.00.12371		N/A		5200 / 5090	
Number of virus records		*685.078*		*unknown*		*373.197*		*303.739*	
Detection of polymorphic viruses (*)			*11 of 12*		*12 of 12*		*12 of 12*		*11 of 12*
Certification level reached in this test		STANDARD		ADVANCED+		ADVANCED+		ADVANCED	
On-demand detection of virus/malware									
Windows viruses	63.029	57.351	90,99%	62.449	99,08%	62.696	99,47%	61.995	98,36%
Macro viruses	44.410	44.332	99,82%	44.403	99,98%	44.401	99,98%	44.407	99,99%
Script viruses/malware	16.902	14.069	83,24%	16.441	97,27%	16.238	96,07%	14.362	84,97%
Worms	89.053	84.803	95,23%	88.333	99,19%	88.572	99,46%	86.275	96,88%
Backdoors	215.445	201.032	93,31%	209.232	97,12%	211.882	98,35%	202.913	94,18%
Trojans	362.900	330.322	91,02%	351.642	96,90%	355.916	98,08%	328.197	90,44%
other malware	13.914	11.123	79,94%	13.548	97,37%	13.535	97,28%	12.292	88,34%
OtherOS viruses/malware	2.691	2.225	82,68%	2.684	99,74%	2.684	99,74%	2.512	93,35%
TOTAL	**808.344**	745.257	**92,20%**	788.732	**97,57%**	795.924	**98,46%**	752.953	**93,15%**



Company		Microsoft		ESET		Norman ASA	
Product		**Microsoft OneCare**		**NOD32 Anti-Virus**		**NormanVirusControl**	
Program version		1.6.2111.30		2.70.39		5.91	
Engine / signature version		1.20.2827.3		2.438		5.91.02	
Number of virus records		578.378		*unknown*		*840.675*	
Detection of polymorphic viruses (*)			*7 of 12*		*12 of 12*		*2 of 12*
Certification level reached in this test		STANDARD		ADVANCED+		STANDARD	
On-demand detection of virus/malware							
Windows viruses	63.029	61.803	98,05%	62.350	98,92%	57.032	90,49%
Macro viruses	44.410	44.251	99,64%	44.404	99,99%	44.312	99,78%
Script viruses/malware	16.902	11.779	69,69%	15.452	91,42%	11.507	68,08%
Worms	89.053	85.119	95,58%	88.422	99,29%	83.718	94,01%
Backdoors	215.445	198.095	91,95%	210.041	97,49%	202.737	94,10%
Trojans	362.900	316.964	87,34%	352.715	97,19%	323.908	89,26%
other malware	13.914	10.112	72,68%	13.050	93,79%	9.945	71,47%
OtherOS viruses/malware	2.691	2.362	87,77%	2.531	94,05%	1.874	69,64%
TOTAL	**808.344**	730.485	**90,37%**	788.965	**97,60%**	735.033	**90,93%**



Company		Symantec		AEC	
Product		**Norton Anti-Virus**		**TrustPort AV WS**	
Program version		14.0.3.3		1.4.2.428	
Engine / signature version		90804t		2.6.0.1237	
Number of virus records		*73.620*		*unknown*	
Detection of polymorphic viruses (*)			*12 of 12*		*11 of 12*
Certification level reached in this test		ADVANCED+		ADVANCED+	
On-demand detection of virus/malware					
Windows viruses	63.029	62.649	99,40%	62.932	99,85%
Macro viruses	44.410	44.398	99,97%	44.398	99,97%
Script viruses/malware	16.902	16.262	96,21%	16.186	95,76%
Worms	89.053	87.955	98,77%	88.999	99,94%
Backdoors	215.445	212.776	98,76%	215.076	99,83%
Trojans	362.900	358.372	98,75%	361.787	99,69%
other malware	13.914	13.603	97,76%	13.614	97,84%
OtherOS viruses/malware	2.691	2.612	97,06%	2.468	91,71%
TOTAL	**808.344**	798.627	**98,80%**	805.460	**99,64%**

All products protect well enough against the limited risks posed by DOS malware and Dialers. Due that, we do not list that results anymore. We may provide again a separate test regarding the detection rate of potentially unwanted programs somewhen in future.

Please do not miss the second part of the report (will be published on December 1st) containing the retrospective test, false positive test (important to take in relation with the results in this report) and the on-demand scanning speed of the above products.

Problems observed during the testing:

Bitdefender: it appears that BitDefender tends to crash or to not clean all files (in contrary to what it displays) if multiple instances of the on-demand scanner are running.

Dr.Web: like in all on-demand tests so far, also this time Dr.Web crashed on several (10) trojan and backdoor samples.

Fortinet: had to scan the same test-sets several times, as it continuosly skipped large amounts of malware without detecting threats which after several scans it was finally able to detect.

Norman: with enabled sandbox it hanged on a Trojan sample.

All encountered problems and/or samples where the problems occurred were submitted to the vendors above and should in the meantime be already fixed.

6. Summary results

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

1.	AVK*	99.6%
2.	TrustPort*	99.5%
3.	Kaspersky	99.3%
4.	F-Secure*	99.2%
5.	AVIRA, eScan*	99.1%
6.	Symantec	99.0%
7.	NOD32	98.6%
8.	BitDefender	98.1%
9.	McAfee	97.0%
10.	AVG	96.4%
11.	Microsoft, Fortinet	95.0%
12.	Avast	94.3%
13.	F-Prot	93.8%
14.	Dr.Web	93.1%
15.	Norman	91.8%

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

1.	TrustPort*	99.7%
2.	AVIRA	99.6%
3.	AVK*	99.2%
4.	Symantec	98.7%
5.	AVG	98.3%
6.	Kaspersky	98.2%
7.	BitDefender	97.3%
8.	NOD32	97.2%
9.	eScan*, F-Secure*	97.0%
10.	Avast	95.6%
11.	McAfee	91.8%
12.	F-Prot	91.6%
13.	Norman	90.6%
14.	Dr.Web, Microsoft	88.7%
15.	Fortinet	88.2%

(c) Total detection rates:

1.	TrustPort*	99.64%
2.	AVIRA	99.45%
3.	AVK*	99.31%
4.	Symantec	98.80%
5.	Kaspersky	98.46%
6.	AVG	97.75%
7.	NOD32	97.60%
8.	F-Secure*	97.57%
9.	eScan*	97.53%
10.	BitDefender	97.51%
11.	Avast	95.24%
12.	McAfee	93.15%
13.	F-Prot	92.20%
14.	Norman	90.93%
15.	Microsoft	90.37%
16.	Fortinet	89.98%
17.	Dr.Web	89.87%

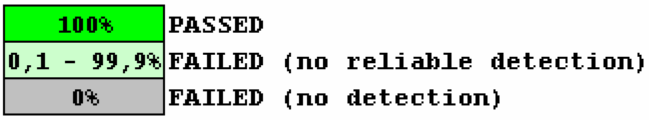
(*) AVK, eScan, F-Secure and TrustPort are multi-engine products.

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

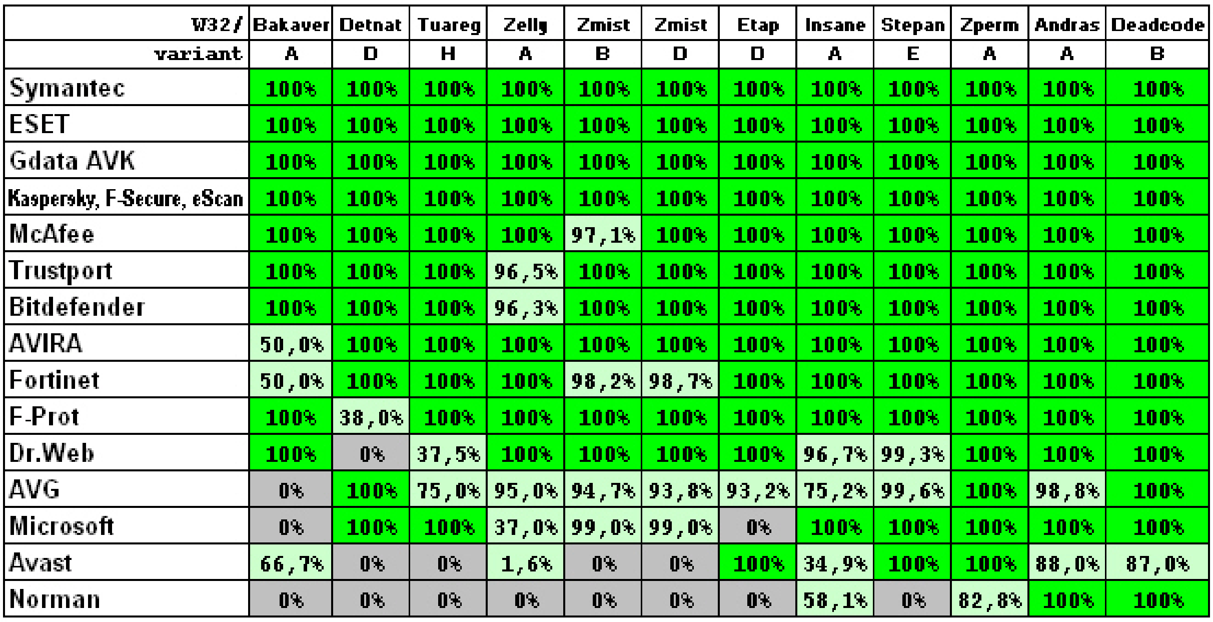
7. Detection rates against some high polymorphic viruses

The test set includes some thousands of replicants for each of the following 12 high polymorphic viruses: W32/Andras.A, W32/Bakaver.A, W32/Deadcode.B, W32/Detnat.D, 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 12 complex viruses are all known to the AV vendors and variants have been submitted several times to the participating companies in the past[1]. The same test-set like in February 2007 was used. 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/	Bakaver	Detnat	Tuareg	Zelly	Zmist	Zmist	Etap	Insane	Stepan	Zperm	Andras	Deadcode
variant	A	D	H	A	B	D	D	A	E	A	A	B
Symantec	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
ESET	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
Gdata AVK	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
Kaspersky, F-Secure, eScan	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
McAfee	100%	100%	100%	100%	97,1%	100%	100%	100%	100%	100%	100%	100%
Trustport	100%	100%	100%	96,5%	100%	100%	100%	100%	100%	100%	100%	100%
Bitdefender	100%	100%	100%	96,3%	100%	100%	100%	100%	100%	100%	100%	100%
AVIRA	50,0%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
Fortinet	50,0%	100%	100%	100%	98,2%	98,7%	100%	100%	100%	100%	100%	100%
F-Prot	100%	38,0%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
Dr.Web	100%	0%	37,5%	100%	100%	100%	100%	96,7%	99,3%	100%	100%	100%
AVG	0%	100%	75,0%	95,0%	94,7%	93,8%	93,2%	75,2%	99,6%	100%	98,8%	100%
Microsoft	0%	100%	100%	37,0%	99,0%	99,0%	0%	100%	100%	100%	100%	100%
Avast	66,7%	0%	0%	1,6%	0%	0%	100%	34,9%	100%	100%	88,0%	87,0%
Norman	0%	0%	0%	0%	0%	0%	0%	58,1%	0%	82,8%	100%	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.

[1] W32/Bakaver.A was used also for the support response test (www.av-comparatives.org/seiten/ergebnisse/AVsupport.pdf)

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).

CERTIFICATION LEVELS	PRODUCTS
AV comparatives ADVANCED+ ★★★ Aug 07 on-demand detection test	**TrustPort** **AVIRA** **Gdata AVK** **Symantec** **Kaspersky** **AVG** **NOD32** **F-Secure** **eScan** **BitDefender**
AV comparatives ADVANCED ★★ Aug 07 on-demand detection test	**Avast** **McAfee**
AV comparatives STANDARD ★ Aug 07 on-demand detection test	**F-Prot** **Norman** **Microsoft** **Fortinet** **Dr.Web**

All products in the ADVANCED+ category (>97%) offer a very high level of on-demand/on-access 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 (as well as other protection mechanism offered, like e.g. behavior blockers, etc.). Products in the ADVANCED category (93-97%) 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 (87-93%) 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). 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.

The percentage ranges of the certification levels may (perhaps) be increased (+1%) in future (2008).

9. Copyright and Disclaimer

This publication is Copyright (c) 2007 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 2007)