Anti-Virus Comparative No.13

On-demand detection of malicious software

Date: February 2007 (2007-02)

Last revision of this report: 28th February 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, we increased the needed minimum detection rate again to 85% (instead 80%) and include for time and resource reasons only the top 17 products in this test - all other products (which some of them may maybe also meet the requirements) will take part in another test which will be released soon.

2. Tested products

All products were updated on the 2nd February 2007 and set to use the best possible settings. The Malware sets and system Test-beds were frozen the 1st February 2007. Over 1 million samples were used in this test. The following 17 products were included in this test:

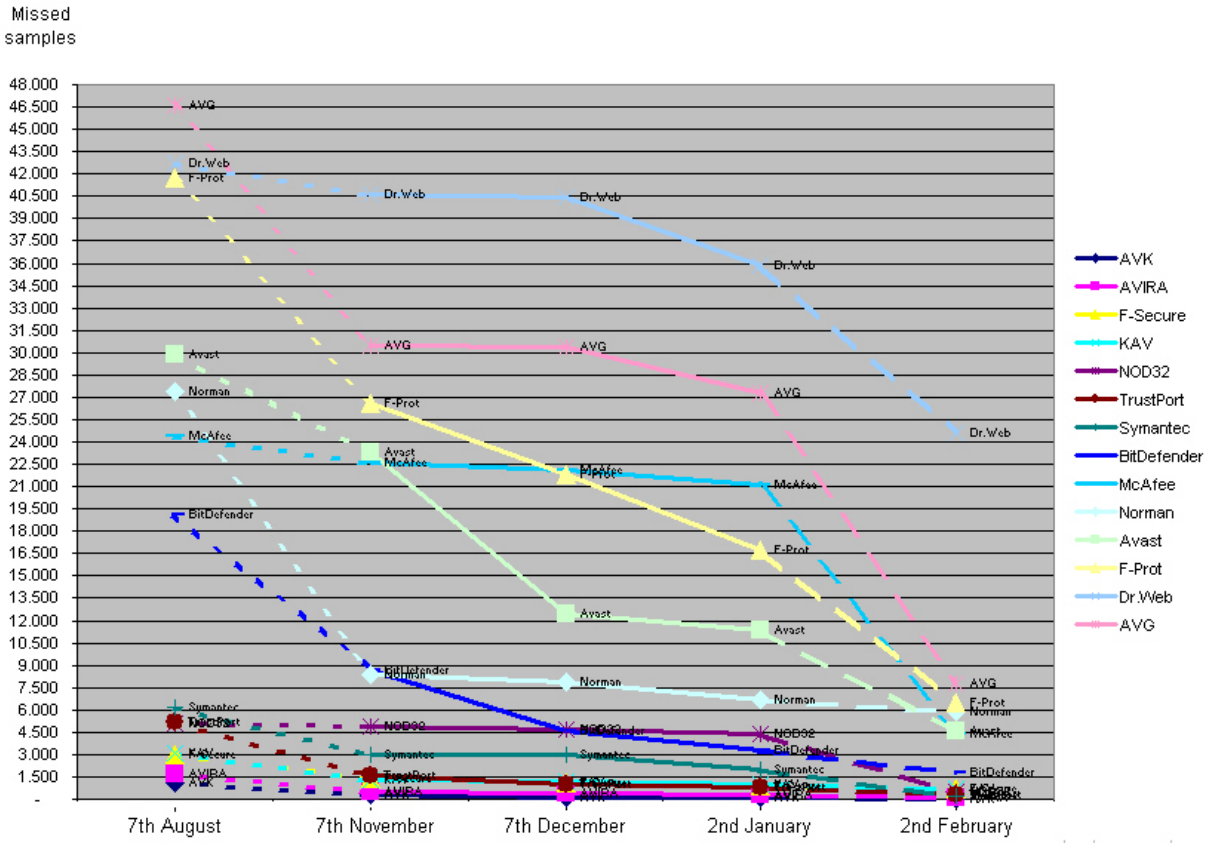
Avast! 4.7.942 Professional Edition
AVG Anti-Malware 7.5.411
AVIRA AntiVir Personal Edition Premium 7.03.01.34
BitDefender Anti-Virus 10 Professional Plus
Dr.Web Anti-Virus for Windows 95-XP 4.33.2
eScan Anti-Virus 8.0.671.1 (*)
ESET NOD32 Anti-Virus 2.70.23
Fortinet FortiClient 3.0.308
F-Prot Anti-Virus for Windows 6.0.5.1
F-Secure Anti-Virus 2007 7.01.128 (*)
Gdata AntiVirusKit (AVK) 17.0.6254 (*)
Kaspersky Anti-Virus 6.0.2.614
McAfee VirusScan 11.1.124
Microsoft Live OneCare 1.5.1890.18
Norman Virus Control 5.82
Symantec Norton Anti-Virus 14.0.0.89
TrustPort Antivirus Workstation 2.5.0.957 (*)

(*) 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*, *AVP*, *Libra, Pegasus* and others
- TrustPort contains the *Norman*, the *Bitdefender* and the *AVG* engines

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, 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.

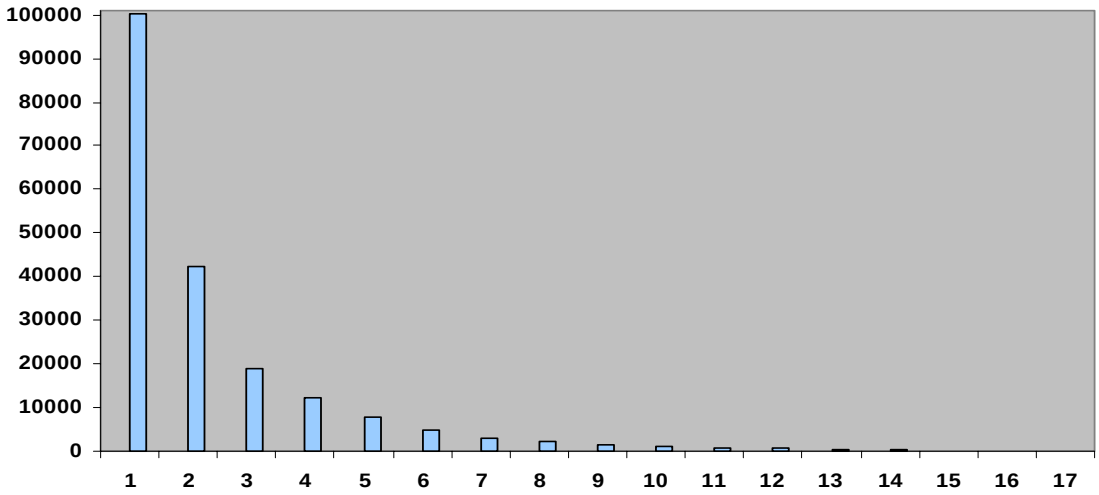
3. Progress made since last comparative

Missed samples from the August 2006 comparative detected/added after 3, 4, 5 and 6 months by the respective companies. Please note that the DOS samples were removed during January 2007. Based on this graph and the results in this test, the vendors that are fastest in detecting new malware samples are: AVIRA, Kaspersky, Symantec, NOD32, AVG and Bitdefender.



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

About 64% 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 78 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		7.03.01.34		17.0.6254		4.7.942		7.5.441	
Engine / signature version		6.37.01.26		17.2423 / 17.124		0709-2		268.17.20 / 664	
Number of virus records		*662.365*		*unknown*		*unknown*		*unknown*	
Detection of over 222000 dialers (*)		*excellent*		*excellent*		*excellent*		*excellent*	
Detection of over 130000 PUP's (**)		*high*		*high*		*mediocre*		*high*	
Detection of over 230000 DOS viruses (***)		*excellent*		*excellent*		*very high*		*mediocre*	
Detection of polymorphic viruses (****)			*11 of 12*		*9 of 12*		*2 of 12*		*2 of 12*
Certification level reached in this test		**ADVANCED+**		**ADVANCED+**		**ADVANCED**		**ADVANCED**	
On-demand detection of virus/malware									
Windows viruses	27.570	27.254	98,85%	27.536	99,88%	26.333	95,51%	24.549	89,04%
Macro viruses	38.372	38.367	99,99%	38.372	100%	37.801	98,51%	38.325	99,88%
Script viruses/malware	11.035	10.035	90,94%	10.796	97,83%	8.170	74,04%	7.415	67,20%
Worms	41.713	41.506	99,50%	41.519	99,53%	39.656	95,07%	40.734	97,65%
Backdoors	155.780	154.695	99,30%	155.321	99,71%	150.049	96,32%	153.085	98,27%
Trojans	210.721	208.308	98,85%	209.029	99,20%	196.159	93,09%	205.754	97,64%
other malware	9.807	9.295	94,78%	9.670	98,60%	7.194	73,36%	7.892	80,47%
OtherOS viruses/malware	2.610	2.445	93,68%	2.604	99,77%	1.684	64,52%	1.799	68,93%
TOTAL	**497.608**	491.905	**98,85%**	494.847	**99,45%**	467.046	**93,86%**	479.553	**96,37%**

Company		Softwin		Doctor Web		MicroWorld		Fortinet	
Product		**BitDefender Prof.+**		**Dr. Web**		**eScan Anti-Virus**		**FortiClient**	
Program version		10		4.33.5.10110		8.0.671.1		3.0.308	
Engine / signature version		7.11190		4.33.2.10060		*N/A*		2.86 / 7.111	
Number of virus records		*453.630*		*173.398*		*unknown*		*unknown*	
Detection of over 222000 dialers (*)		*excellent*		*excellent*		*excellent*		*high*	
Detection of over 130000 PUP's (**)		*high*		*high*		*high*		*mediocre*	
Detection of over 230000 DOS viruses (***)		*excellent*		*high*		*excellent*		*low*	
Detection of polymorphic viruses (****)			*8 of 12*		*8 of 12*		*8 of 12*		*6 of 12*
Certification level reached in this test		**ADVANCED**		**STANDARD**		**ADVANCED+**		**ADVANCED**	
On-demand detection of virus/malware									
Windows viruses	27.570	26.450	95,94%	25.455	92,33%	27.462	99,61%	27.402	99,39%
Macro viruses	38.372	38.287	99,78%	38.317	99,86%	38.372	100%	36.836	96,00%
Script viruses/malware	11.035	9.469	85,81%	7.586	68,74%	10.780	97,69%	7.679	69,59%
Worms	41.713	41.140	98,63%	39.363	94,37%	40.871	97,98%	40.009	95,91%
Backdoors	155.780	151.128	97,01%	144.008	92,44%	154.018	98,87%	149.393	95,90%
Trojans	210.721	201.019	95,40%	182.124	86,43%	203.418	96,53%	196.625	93,31%
other malware	9.807	8.769	89,42%	6.200	63,22%	9.579	97,68%	7.842	79,96%
OtherOS viruses/malware	2.610	1.978	75,79%	1.177	45,10%	2.603	99,73%	1.918	73,49%
TOTAL	**497.608**	478.240	**96,11%**	444.230	**89,27%**	487.103	**97,89%**	467.704	**93,99%**

Company		Frisk Software		F-Secure		Kaspersky Labs		McAfee	
Product		**F-Prot Anti-Virus**		**F-Secure Anti-Virus**		**Kaspersky AV**		**McAfee VirusScan**	
Program version		6.0.5.1		7.01.128		6.0.2.614		11.1.124	
Engine / signature version		4.3.1		7.00.12371		*N/A*		5100.0194 / 4955	
Number of virus records		*491.050*		*unknown*		*264.410*		*225.413*	
Detection of over 222000 dialers (*)		*excellent*		*excellent*		*excellent*		*excellent*	
Detection of over 130000 PUP's (**)		*high*		*high*		*high*		*high*	
Detection of over 230000 DOS viruses (***)		*excellent*		*excellent*		*excellent*		*excellent*	
Detection of polymorphic viruses (****)			*11 of 12*		*8 of 12*		*8 of 12*		*8 of 12*
Certification level reached in this test		**ADVANCED**		**ADVANCED+**		**ADVANCED+**		**STANDARD**	
On-demand detection of virus/malware									
Windows viruses	27.570	26.646	96,65%	27.462	99,61%	27.462	99,61%	27.464	99,62%
Macro viruses	38.372	38.371	~100%	38.372	100%	38.372	100%	38.372	100%
Script viruses/malware	11.035	9.031	81,84%	10.829	98,13%	10.780	97,69%	9.694	87,85%
Worms	41.713	39.565	94,85%	40.873	97,99%	40.871	97,98%	37.890	90,83%
Backdoors	155.780	149.128	95,73%	154.018	98,87%	154.018	98,87%	147.781	94,87%
Trojans	210.721	191.288	90,78%	203.419	96,53%	203.418	96,53%	183.519	87,09%
other malware	9.807	7.910	80,66%	9.617	98,06%	9.579	97,68%	8.940	91,16%
OtherOS viruses/malware	2.610	2.196	84,14%	2.604	99,77%	2.603	99,73%	2.278	87,28%
TOTAL	**497.608**	464.135	**93,27%**	487.194	**97,91%**	487.103	**97,89%**	455.938	**91,63%**

Note: the test results (detection rates) of e.g. the paid product versions AVG Anti-Malware and AVIRA PE Premium do NOT apply also to the offered free product versions and may in some areas differ considerably.

Company		Microsoft		ESET		Norman ASA	
Product		**Microsoft OneCare**		**NOD32 Anti-Virus**		**NormanVirusControl**	
Program version		1.5.1890.18		2.70.23		5.82	
Engine / signature version		1.15.2227.7		2.031		5.90.30	
Number of virus records		367.307		*unknown*		*654.451*	
Detection of over 222000 dialers (*)		*excellent*		*excellent*		*high*	
Detection of over 130000 PUP's (**)		*mediocre*		*high*		*high*	
Detection of over 230000 DOS viruses (***)		*very high*		*excellent*		*excellent*	
Detection of polymorphic viruses (****)			*4 of 12*		*12 of 12*		*1 of 12*
Certification level reached in this test				ADVANCED		ADVANCED	
On-demand detection of virus/malware							
Windows viruses	27.570	26.198	95,02%	27.463	99,61%	24.163	87,64%
Macro viruses	38.372	38.103	99,30%	38.371	~100%	38.350	99,94%
Script viruses/malware	11.035	7.454	67,55%	9.827	89,05%	8.031	72,78%
Worms	41.713	37.213	89,21%	40.720	97,62%	39.853	95,54%
Backdoors	155.780	128.026	82,18%	150.550	96,64%	149.688	96,09%
Trojans	210.721	165.869	78,71%	203.097	96,38%	197.372	93,67%
other malware	9.807	5.725	58,38%	8.792	89,65%	7.282	74,25%
OtherOS viruses/malware	2.610	1.436	55,02%	2.399	91,92%	1.150	44,06%
TOTAL	**497.608**	410.024	**82,40%**	481.219	**96,71%**	465.889	**93,63%**

Company		Symantec		AEC	
Product		**Norton Anti-Virus**		**TrustPort AV WS**	
Program version		14.0.0.89		2.5.0.957	
Engine / signature version		90202ai		*N/A*	
Number of virus records		*73.132*		*unknown*	
Detection of over 222000 dialers (*)		*excellent*		*excellent*	
Detection of over 130000 PUP's (**)		*high*		*high*	
Detection of over 230000 DOS viruses (***)		*excellent*		*excellent*	
Detection of polymorphic viruses (****)			*12 of 12*		*9 of 12*
Certification level reached in this test		ADVANCED		ADVANCED+	
On-demand detection of virus/malware					
Windows viruses	27.570	27.483	99,68%	27.450	99,56%
Macro viruses	38.372	38.366	99,98%	38.371	~100%
Script viruses/malware	11.035	9.889	89,61%	10.209	92,51%
Worms	41.713	41.385	99,21%	41.594	99,71%
Backdoors	155.780	150.612	96,68%	155.286	99,68%
Trojans	210.721	202.829	96,25%	209.863	99,59%
other malware	9.807	8.913	90,88%	9.315	94,98%
OtherOS viruses/malware	2.610	2.373	90,92%	2.333	89,39%
TOTAL	**497.608**	481.850	**96,83%**	494.421	**99,36%**

Notes about the detection of DOS viruses/malware: since 2007 the DOS viruses/malware category is not counted anymore; only labels about the detection capability of this category are still available in the result tables above. The labels can be read with this key: not present (0-50%), very low (51-80%), low (81-91%), mediocre (92-95%), high (96-97%), very high (98-99,9%), excellent (99,91-100%).

Notes about the on-demand detection of Dialers: The labels for this category can be read with this key: not present (0-5%), low (6-40%), mediocre (41-70%), high (71-95%), excellent (96-100%).

Notes about the detection of potentially unwanted programs (PUPs): The labels for this category can be read with this key: low (0-64%), mediocre (65-84%), high (85-100%). For some few more details about this type of PUP-test please read the report of October 2006 at http://www.av-comparatives.org/seiten/ergebnisse/puptest1.pdf. *The 'unwanted files' test-set contains harmful Adware, Spyware, Ad-Spy-related downloaders, Hijackers, Keyloggers, Trojans, RAT's, Rootkits, Backdoor tools, constructors/kits, various potentially dangerous or potentially unwanted (virus/hacker) tools and applications which may require some user input. The PUP-Test does not just determine the level of protection - as it contains also Greyware, user preference has to be taken into account: If an user does not think such applications are an issue, some products may annoy him with the alerts. If an user thinks those applications are an issue, then some products may be more comforting. So, the available labels are only low, mediocre and high.*

6. Summary results

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

1.	AVK*	99.6%
2.	KAV, eScan*, F-Secure*	99.0%
3.	TrustPort*	98.9%
4.	AVIRA	98.6%
5.	Symantec	98.5%
6.	NOD32	97.9%
7.	BitDefender	96.7%
8.	F-Prot	95.5%
9.	McAfee	95.4%
10.	Fortinet	93.9%
11.	Avast	93.7%
12.	AVG	93.0%
13.	Dr.Web	92.2%
14.	Norman	92.0%
15.	Microsoft	91.0%

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

1.	TrustPort*	99.5%
2.	AVK*	99.4%
3.	AVIRA	98.9%
4.	AVG, KAV, eScan*, F-Secure*	97.5%
5.	Symantec, NOD32	96.3%
6.	BitDefender	95.9%
7.	Norman	94.2%
8.	Fortinet	94.0%
9.	Avast	93.9%
10.	F-Prot	92.6%
11.	McAfee	90.4%
12.	Dr.Web	88.3%
13.	Microsoft	79.6%

(c) Total detection rates:

1.	AVK*	99.45%
2.	TrustPort*	99.36%
3.	AVIRA	98.85%
4.	F-Secure*	97.91%
5.	Kaspersky, eScan*	97.89%
6.	Symantec	96.83%
7.	NOD32	96.71%
8.	AVG	96.37%
9.	BitDefender	96.11%
10.	Fortinet	93.99%
11.	Avast	93.86%
12.	Norman	93.63%
13.	F-Prot	93.27%
14.	McAfee	91.63%
15.	Dr.Web	89.27%
16.	Microsoft	82.40%

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

Important notes: Please try anti-virus products on your own system before making a purchase decision based on these tests.
Would the DOS category be still counted in the total detection rates, those with excellent DOS detection would score higher.

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[1]: 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[2]. In August 2007 the same virus set will be used again. 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/ variant	Detnat D	Bakaver A	Zelly A	Stepan E	Etap D	Zmist B	Zmist D	Tuareg H	Insane A	Deadcode B	Zperm A	Andras A
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%	99,8%	97,9%	100%	100%	98,3%	100%	100%	100%	100%	100%
Kaspersky, F-Secure, eScan	100%	100%	99,8%	97,9%	97,8%	100%	98,3%	100%	100%	100%	100%	100%
Trustport	100%	91,7%	95,2%	100%	100%	100%	100%	100%	65,7%	100%	100%	100%
McAfee	75,3%	100%	98,2%	78,4%	100%	96,6%	100%	100%	100%	100%	100%	100%
F-Prot	0%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
AVIRA	100%	0%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
Dr.Web	0%	100%	100%	99,3%	100%	100%	100%	37,5%	96,7%	100%	100%	100%
Bitdefender	0%	91,7%	0%	100%	100%	100%	100%	100%	65,6%	100%	100%	100%
Fortinet	0%	50,0%	99,7%	100%	100%	11,8%	16,6%	100%	99,5%	100%	100%	100%
AVG	100%	0%	95,0%	0%	0%	94,7%	93,8%	75,0%	75,2%	100%	0%	98,8%
Microsoft	0%	0%	0%	100%	0%	99,0%	99,0%	98,8%	100%	0%	100%	100%
Avast	0%	0%	0,7%	0%	100%	0%	0%	0%	34,9%	87,0%	100%	0%
Norman	0%	0%	0%	0%	0%	0%	0%	0%	58,1%	35,0%	82,8%	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/Polip.A and W32/Sality.Q were detected reliably (100%) by all products.

[2] 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+ Feb 07 on-demand detection test	**Gdata AVK TrustPort AVIRA F-Secure Kaspersky eScan**
AV comparatives ADVANCED Feb 07 on-demand detection test	**Symantec* NOD32* AVG BitDefender Fortinet Avast Norman F-Prot**
AV comparatives STANDARD Feb 07 on-demand detection test	**McAfee Dr.Web**
No certification	**Microsoft**

Microsoft OneCare performed very low in the test and did not reach the minimum requirements for participation. Due that, its inclusion in future tests of this year have to be re-evaluated.

NOTE (*): Symantec and ESET NOD32 (which both have 100% detection of polymorphic viruses) missed the ADVANCED+ level for a handful of files, as to get the ADVANCED+ level it is needed to detect at least 97% of the test-set. If the DOS category would still be counted, those two products (and some other products) would score higher.

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). 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.

9. Copyright and Disclaimer

Andreas Clementi, AV-Comparatives (February 2007)