



Anti-Virus Comparative No.17

On-demand detection of malicious software

Date: February 2008 (2008-02)

Last revision of this report: 9th March 2008

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>¹. 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. The participation is currently limited to about 16-18 well-known and worldwide used high-quality anti-virus products with high detection rates, which vendors agreed to get tested and included in this public report.

2. Tested products

All products were updated on the 4th February 2008 and set to use the best possible settings². The Malware sets and system Test-beds were frozen the 2nd February 2008. The following 16 products were included in this test:

avast! Professional Edition 4.7.1098
AVG Anti-Malware 7.5.516
AVIRA AntiVir Personal Edition Premium 7.06.00.308
BitDefender Anti-Virus 2008 Professional Plus 11.0.15
eScan Anti-Virus 9.0.768.1
ESET NOD32 Antivirus 3.0.621.0
F-Secure Anti-Virus 2008 8.00.101
G DATA AntiVirusKit (AVK) 2008 18.0.7227.533
Kaspersky Anti-Virus 7.0.1.321a
McAfee VirusScan Plus 2008 12.0.176
Microsoft Live OneCare 2.0.2500.22
Norman SS Antivirus & Anti-Spyware 7.0
Sophos Anti-Virus 7.0.7
Symantec Norton Anti-Virus 2008 15.0.0.58
TrustPort³ Antivirus Workstation 2.8.0.1629
VBA32 Scanner for Windows 3.12.6.0

Some products may offer additional options/features e.g. to provide additional protection against malware during its execution (if not detected in advance on-access or on-demand). 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 frequency, ease of management, HIPS/behaviorblocker functions, etc.) to consider. Although extremely important, the detection rate of a product is only one aspect of a complete Anti-Virus product. AV-Comparatives will in future expand its testing range to cover also other areas, beside detection rate, proactive detection, false alarm rate, scanning speed and polymorphic virus detection only.

We suggest readers to research also other independent test results, as results provided by independent labs are usually quite consistent and do not differ much from each other - depending on the type of test, the used settings and the type/quality of the test samples. We encourage our readers to also have a look at various types of tests, to get a better overview of the detection and protection capabilities of the various security products.

¹ will be updated and probably completely rewritten this summer.

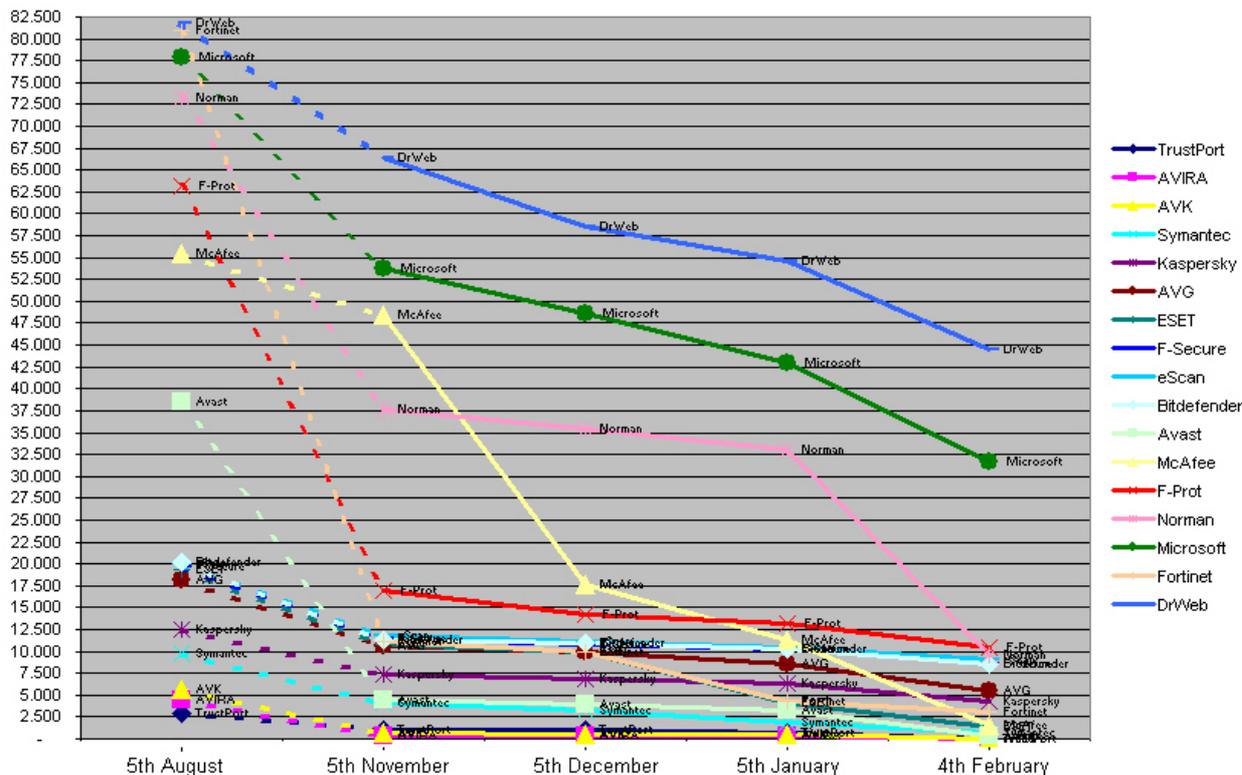
² On request of VBA32, "Thorough mode" and "Excessive heuristic" were disabled in their product, as they are "mostly useless, but increase scanning time" and do not make a big difference in this detection test.

³ version with 5 engines (AVG, Norman, Dr. Web, Ewido, VBA32)

3. Progress made since last comparative

Missed samples from the August 2007 comparative detected/added after 3, 4, 5 and 6 months by the respective companies. Compared to the overviews of added samples of past years, it can be observed that most vendors are now faster in adding malware samples to their databases.

Missed samples



4. Comments

In future (maybe already in August 2008), we will probably use less samples for this kind of test (focus on only more actual/prevalent/representative samples).

This is an on-demand test. The results of this on-demand test are usually applicable 1:1 also for the on-access scanner (if configured the same way), but not for on-execution detection/protection technologies (HIPS, behaviorblocker, etc.), which some of the above tested Anti-Virus products (e.g. BitDefender, F-Secure, GDATA, Kaspersky, McAfee, Microsoft, Sophos, Symantec, etc.) already include, and more products will probably follow.

AV-Comparatives plans to include dynamic tests in its yearly test-series starting from next year, in order to cover also this protection aspect. It will not replace the current way of testing, but will be an additional evaluation criteria (so all kind of users may benefit from it, independently on how they use the Anti-Virus software or what their needs are). Even if we will deliver many various tests and show our readers different aspects of the anti-virus software, it does not and will never replace the good old way of evaluating (anti-virus) software: try it by yourself on your system and build your own opinion about the product. Test data or reviews just gives you a guidance to some aspects that you can not evaluate by yourself.

5. Test results

About 73% of the test-set used in February 2008 is detected by all 16 scanners. The graph with the distribution of missed samples can be found at <http://www.av-comparatives.org/forum/index.php?page=Thread&threadID=798>

Company		AVIRA		G DATA Security		Alwil Software		AVG Technologies	
Product		AntiVir PE Premium		AntiVirusKit (AVK)		avast! Professional		AVG Anti-Malware	
Program version		7.06.00.308		18.0.7227.533		4.7.1098		7.5.516	
Engine / signature version		7.06.00.62 / 7.00.02.90		18.2654 / 18.123		080203-0		269.19.19 / 1258	
Number of virus records		1.092.160		unknown		unknown		unknown	
Certification level reached in this test		ADVANCED+		ADVANCED+		ADVANCED+		ADVANCED+	
On-demand detection of virus/malware									
Windows viruses	149.202	148.903	99,8%	149.119	99,9%	148.387	99,5%	143.393	96,1%
Macro viruses	95.059	95.034	~100%	95.059	100%	94.631	99,5%	94.823	99,8%
Script viruses	14.284	13.916	97,4%	14.165	99,2%	13.010	91,1%	12.055	84,4%
Worms	190.952	190.530	99,8%	190.564	99,8%	188.006	98,5%	188.821	98,9%
Backdoors/Bots	400.986	399.900	99,7%	399.536	99,6%	391.432	97,6%	395.103	98,5%
Trojans	817.043	813.233	99,5%	811.200	99,3%	793.223	97,1%	803.376	98,3%
other malware	15.838	15.447	97,5%	15.715	99,2%	14.402	90,9%	14.078	88,9%
TOTAL	1.683.364	1.676.963	99,6%	1.675.358	99,5%	1.643.091	97,6%	1.651.649	98,1%

GDATA AVK uses the Kaspersky (v6 without new heuristic) and Avast engine. AVG Anti-Malware includes the AVG antivirus engine and the AVG antispyware engine (aka Ewido engine).

Company		BitDefender		MicroWorld		F-Secure		Kaspersky Labs	
Product		BitDefender Prof.+		eScan Anti-Virus		F-Secure Anti-Virus		Kaspersky AV	
Program version		11.0.15		9.0.768.1		8.00.101		7.0.1.321a	
Engine / signature version		7.17325		N/A		7.30.13161		N/A	
Number of virus records		978.896		unknown		unknown		574.209	
Certification level reached in this test		ADVANCED		ADVANCED+		ADVANCED+		ADVANCED+	
On-demand detection of virus/malware									
Windows viruses	149.202	147.022	98,5%	148.683	99,7%	148.684	99,7%	148.909	99,8%
Macro viruses	95.059	94.736	99,7%	95.054	~100%	95.055	~100%	95.054	~100%
Script viruses	14.284	13.372	93,6%	13.949	97,7%	14.102	98,7%	13.949	97,7%
Worms	190.952	189.084	99,0%	189.484	99,2%	189.515	99,2%	189.893	99,4%
Backdoors/Bots	400.986	382.706	95,4%	390.205	97,3%	390.239	97,3%	392.713	97,9%
Trojans	817.043	782.493	95,8%	788.147	96,5%	788.288	96,5%	798.083	97,7%
other malware	15.838	14.710	92,9%	15.299	96,6%	15.345	96,9%	15.390	97,2%
TOTAL	1.683.364	1.624.123	96,5%	1.640.821	97,5%	1.641.228	97,5%	1.653.991	98,3%

eScan and F-Secure use various engines, including the Kaspersky engine (v6 without new heuristic).

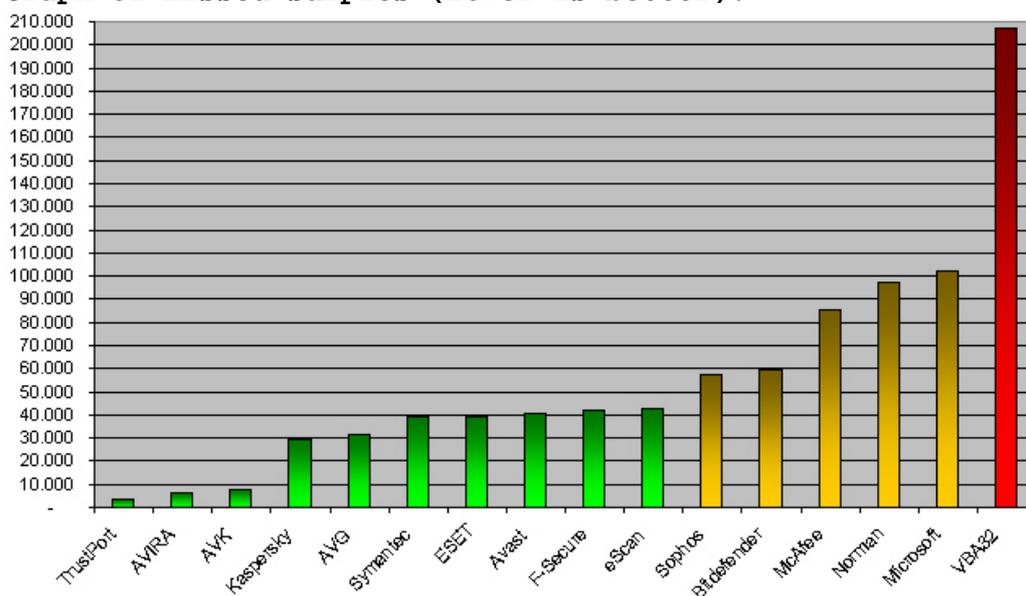
Company		McAfee		Microsoft		ESET		Norman ASA	
Product		McAfee VirusScan+		Microsoft OneCare		IOD32 Antivirus		Norman ISS AV+AS	
Program version		12.0.176		2.0.2500.22		3.0.621.0		7.0	
Engine / signature version		5200.2160 / 5222		1.27.6270.0 / 1.3204		2847		5.91.10	
Number of virus records		371.817		723.778		unknown		1.310.735	
Certification level reached in this test		ADVANCED		ADVANCED		ADVANCED+		ADVANCED	
On-demand detection of virus/malware									
Windows viruses	149.202	147.115	98,6%	146.690	98,3%	148.453	99,5%	140.874	94,4%
Macro viruses	95.059	95.056	~100%	94.624	99,5%	95.044	~100%	94.869	99,8%
Script viruses	14.284	12.855	90,0%	11.963	83,8%	13.338	93,4%	10.753	75,3%
Worms	190.952	188.318	98,6%	185.743	97,3%	189.659	99,3%	185.448	97,1%
Backdoors/Bots	400.986	383.059	95,5%	376.054	93,8%	391.015	97,5%	380.204	94,8%
Trojans	817.043	757.305	92,7%	753.863	92,3%	792.222	97,0%	761.830	93,2%
other malware	15.838	14.370	90,7%	12.044	76,0%	14.226	89,8%	12.272	77,5%
TOTAL	1.683.364	1.598.078	94,9%	1.580.981	93,9%	1.643.957	97,7%	1.586.250	94,2%

Note: a separate Technology Preview Test of McAfee (total score: 99,2%) - which technology will be included in McAfee products later this year - will be released soon on our website.

Company	Symantec	Sophos	AEC	VirusBlokAda	
Product	Horton Anti-Virus	Sophos Anti-Virus	TrustPort AV WS	VBA32 Anti-Virus	
Program version	15.0.0.58	7.0.7	2.8.0.1629	3.12.6.0	
Engine / signature version	100204 / 78215	2.70.1 / 4.26E+132	2.8.0.1630	unknown	
Number of virus records	73.845	345.615	unknown	unknown	
Certification level reached in this test	ADVANCED+	ADVANCED	ADVANCED+	STANDARD	
On-demand detection of virus/malware					
Windows viruses	149.202	149.128 ~100%	145.076 97,2%	149.037 99,9%	132.863 89,0%
Macro viruses	95.059	95.059 100%	94.810 99,7%	95.053 ~100%	92.909 97,7%
Script viruses	14.284	14.049 98,4%	10.730 75,1%	13.979 97,9%	7.200 50,4%
Worms	190.952	190.551 99,8%	185.065 96,9%	190.781 99,9%	171.497 89,8%
Backdoors/Bots	400.986	384.939 96,0%	394.944 98,5%	400.503 99,9%	351.683 87,7%
Trojans	817.043	794.816 97,3%	783.006 95,8%	815.262 99,8%	708.649 86,7%
other malware	15.838	15.464 97,6%	12.135 76,6%	15.458 97,6%	11.498 72,6%
TOTAL	1.683.364	1.644.006 97,7%	1.625.766 96,6%	1.680.073 99,8%	1.476.299 87,7%

TrustPort uses 5 engines, including AVG, Ewido, Norman, Dr.Web and VBA32.

Graph of missed samples (lower is better):



In 2007 we removed all DOS viruses/malware from our test-sets. This time we removed also all non-Windows malware (the OtherOS category) and some malware/viruses that do not work under Windows NT/2000/XP/Vista. Some old malware has also been removed and will be removed further from next test-sets, narrowing the samples to more actual/prevalent ones. Our test-set does not contain adware/spyware/dialers/tools etc., which is why it consists of "only" ~1,7 million samples.

Please do not miss the second part of the report (will be published on June 1st) containing the retrospective test (which may be of more importance to know how well products are at detecting new/unknown malware), false positive test (important to take in relation with the results in this report) and the scan speed of the above products.

A good on-demand/on-access detection is still one of the most important and reliable features of an antivirus product. Additionally, some products included in this test provide already at least some kind of HIPS-, behavior-based or other functionalities to block (or at least warn about the possibility of) malicious actions e.g. during the execution of malware, when all other on-access and on-demand detection/protection mechanism failed (even with highest settings).

6. Summary results

Compared to the results of last year, in general most products improved their detection rates. Note that some products which scored only STANDARD (or lower) in past are not included this year in the tests.

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

1.	AVK, TrustPort	99.9%
2.	Symantec, AVIRA	99.8%
3.	Kaspersky	99.6%
4.	F-Secure, eScan	99.5%
5.	NOD32	99.3%
6.	BitDefender, Avast	98.8%
7.	McAfee	98.6%
8.	AVG, Microsoft	97.7%
9.	Sophos	96.9%
10.	Norman	96.1%
11.	VBA32	90.0%

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

1.	TrustPort	99.8%
2.	AVIRA	99.6%
3.	AVK	99.4%
4.	AVG	98.3%
5.	Kaspersky	97.8%
6.	Avast	97.2%
7.	NOD32	97.0%
8.	Symantec	96.9%
9.	F-Secure	96.8%
10.	eScan	96.7%
11.	Sophos	96.5%
12.	BitDefender	95.6%
13.	McAfee, Norman	93.6%
14.	Microsoft	92.6%
15.	VBA32	86.6%

(c) Total detection rates:

1.	TrustPort	99.8%
2.	AVIRA	99.6%
3.	AVK	99.5%
4.	Kaspersky	98.3%
5.	AVG	98.1%
6.	Symantec, NOD32	97.7%
7.	Avast	97.6%
8.	F-Secure, eScan	97.5%
9.	Sophos	96.6%
10.	BitDefender	96.5%
11.	McAfee	94.9%
12.	Norman	94.2%
13.	Microsoft	93.9%
14.	VBA32	87.7%

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

7. Detection rates against some high polymorphic viruses

The test set includes some thousands of replicants for each of the following 8 high polymorphic viruses⁴: W32/Bakaver.A, W32/Etap.D, W32/Insane.A, W32/Stepan.E, W32/Tuareg.H, W32/Zelly.A, W32/Zmist.B and W32/Zmist.D. Those 8 complex viruses are all known to the AV vendors and variants have been submitted several times in the past. The polymorphic test evaluates the quality of the detection routines for polymorphic viruses - it reflects the ability to detect difficult malware. 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.A	W32/Zmist.B	W32/Zmist.D	W32/Etap.D	W32/Zelly.A	W32/Stepan.E	W32/Tuareg.H	W32/Insane.A
Symantec	100%	100%	100%	100%	100%	100%	100%	100%
ESET NOD32	100%	100%	100%	100%	100%	100%	100%	100%
G DATA AVK	100%	100%	100%	100%	100%	100%	100%	100%
Kaspersky, F-Secure, eScan	100%	100%	100%	100%	100%	100%	100%	100%
AVIRA	100%	100%	100%	100%	100%	100%	100%	100%
Trustport	100%	100%	100%	100%	100%	100%	100%	100%
McAfee	100%	97,9%	100%	100%	100%	100%	100%	100%
Bitdefender	100%	100%	100%	100%	96,3%	100%	100%	100%
Avast	100%	52,3%	60,9%	100%	100%	100%	100%	100%
Sophos	0%	98,4%	99,5%	100%	100%	100%	100%	100%
AVG	0%	94,7%	93,8%	93,2%	95,0%	99,6%	75,0%	98,0%
Microsoft	0%	99,0%	99,0%	0%	37,6%	100%	100%	100%
VBA32	75,0%	0%	0%	100%	51,3%	84,6%	100%	100%
Norman	0%	0%	0%	0%	25,6%	36,0%	100%	99,2%

The results of the polymorphic test are of interest, 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 low 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.

In future we may replace this polymorphic virus detection test with another type of test, maybe with an active rootkit detection/removal test. The above test-set will be re-used maybe in future to see if anything changed.

⁴ Some easy to detect (or detected to 100% by all products) polymorphic viruses are no longer included.

8. Award levels reached in this test

AV-Comparatives provides 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>).

<u>AWARD LEVELS</u>	<u>PRODUCTS</u>
	TrustPort AVIRA GDATA AVK Kaspersky AVG Symantec ESET NOD32 Avast F-Secure eScan
	Sophos BitDefender McAfee Norman Microsoft
	VBA32

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.virusb1n.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

This publication is Copyright (c) 2008 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 (February 2008)