AV
comparatives

Anti-Virus Comparative No.10

Proactive/retrospective test
(on-demand detection of virus/malware)

contains also

False positive test
&
Scanning speed test

Date: May 2006 (2006-05)

Last revision: 25th May 2006

Author: Andreas Clementi

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

1. Introduction

This test report is the second part of the February 2006 test. The same products were used and the results show the pure proactive detection capabilities that the products had three months ago. Many new viruses and other types of malware appear every day, this is why it's important that Anti-Virus products not only provide new updates, as often and as fast as possible, in order to identify those new threats, but also that they are able to detect such threats in advance with generic and/or heuristic techniques. Without this ability the user has to wait for an updated release of the Anti-Virus product. Even if nowadays most anti-virus products provide daily or hourly updates, without heuristic/generic methods there is always a time-frame where the user is not protected, and much more important than time to release an update, is the time it takes to get that update deployed.

The same products, with the same best possible detection settings that the scan engines had in the last comparative, were used for these tests. For this test we used new samples[1] received between 6th February and 6th May 2006, which were all new to all tested products.

The following 16 products were tested in this comparative (last signature updates and versions are from 6th 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 (with 5000 engine)
- 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

2. Description

Anti-Virus products often claim to have high proactive detection capabilities – far higher than those reached in this test. This isn't just a self-promotional statement; it's possible that products reach the stated percentages, but this depends on the duration of the test-period, the size of the sample set and the used samples. The data shows how good the proactive detection capabilities of the scanners were in detecting actual new/unknown threats. Users shouldn't be afraid if products have, in a retrospective test, low percentages. If the anti-virus software is always kept up-to-date, it will be able to detect most of the samples. For understanding how the detection rates of the Anti-Virus products look with updated signatures and programs, have a look at our regular on-demand detection tests. Only the on-demand detection capability was tested; some products may be had the ability to detect some samples e.g. on-execution or by other monitoring tools, like behaviour-blocker, etc.

[1] Typical Spyware, Adware, tools, etc. are not included.

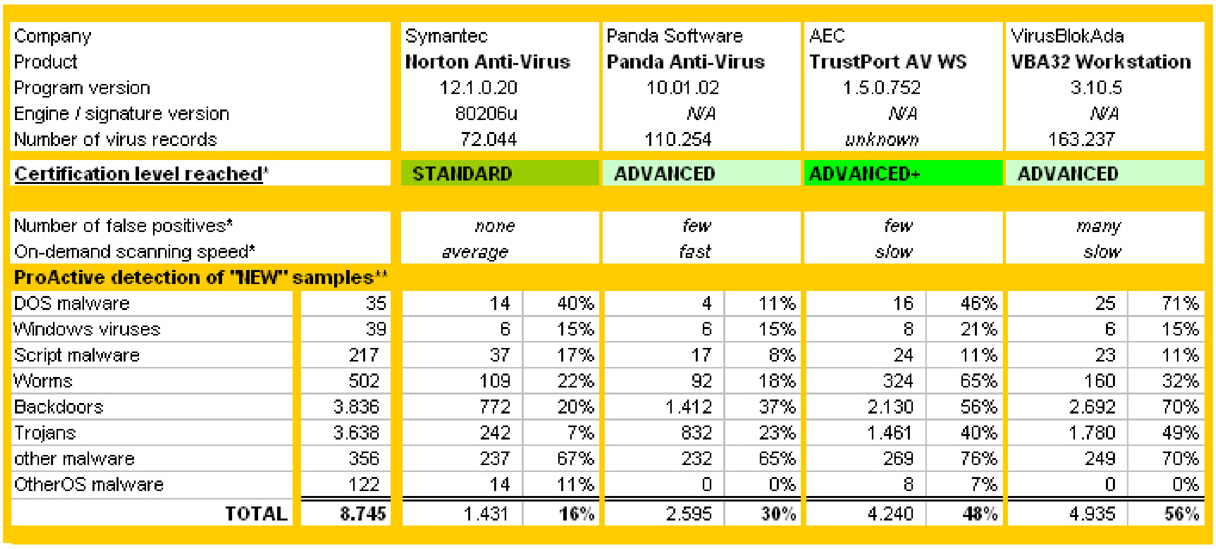
3. Test results

Below the detailed test result tables of all tested products:

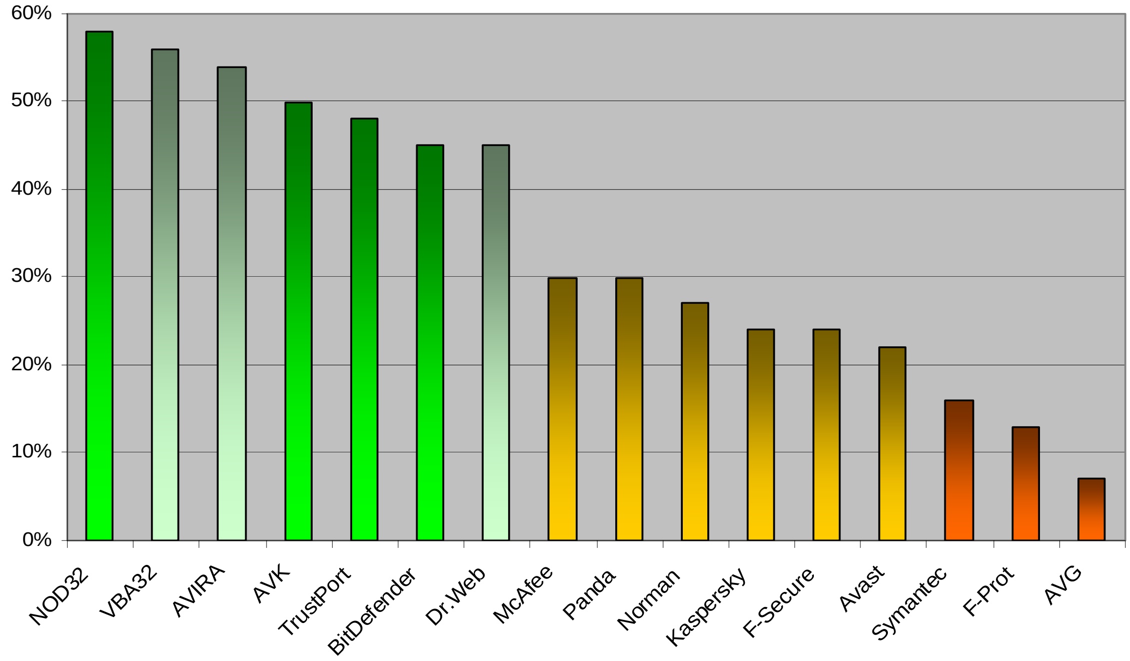
Company		AVIRA		G DATA Security		Alwil Software		GriSoft	
Product		**AntiVir PE Premium**		**AntiVirusKit (AVK)**		**Avast! Professional**		**AVG Professional**	
Program version		7.00.00.21		16.0.5		4.6.763		7.1.375	
Engine / signature version		6.33.0.36 / 6.33.0.210		16.5355 / 16.2619		0606-1		267.15.2/252	
Number of virus records		307.383		*unknown*		*unknown*		*unknown*	
Certification level reached'		**ADVANCED**		**ADVANCED+**		**ADVANCED**		**STANDARD**	
Number of false positives*		*many*		*few*		*few*		*few*	
On-demand scanning speed*		*fast*		*slow*		*average*		*average*	
ProActive detection of "NEW" samples''									
DOS malware	35	1	3%	16	46%	7	20%	16	46%
Windows viruses	39	7	18%	8	21%	8	21%	3	8%
Script malware	217	62	29%	36	17%	51	24%	137	63%
Worms	502	239	48%	306	61%	51	10%	25	5%
Backdoors	3.836	2.400	63%	2.277	59%	1.260	33%	153	4%
Trojans	3.638	1.726	47%	1.425	39%	296	8%	38	1%
other malware	356	263	74%	271	76%	217	61%	229	64%
OtherOS malware	122	29	24%	8	7%	8	7%	0	0%
TOTAL	**8.745**	4.727	**54%**	4.347	**50%**	1.898	**22%**	601	**7%**

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*	
Certification level reached'		**ADVANCED+**		**ADVANCED**		**STANDARD**		**ADVANCED**	
Number of false positives*		*few*		*many*		*few*		*few*	
On-demand scanning speed*		*average*		*average*		*average*		*slow*	
ProActive detection of "NEW" samples''									
DOS malware	35	16	46%	5	14%	16	46%	7	20%
Windows viruses	39	8	21%	7	18%	0	0%	2	5%
Script malware	217	24	11%	41	19%	1	0%	18	8%
Worms	502	302	60%	249	50%	120	24%	35	7%
Backdoors	3.836	1.973	51%	1.971	51%	599	16%	1.680	44%
Trojans	3.638	1.375	38%	1.428	39%	188	5%	74	2%
other malware	356	268	75%	199	56%	192	54%	232	65%
OtherOS malware	122	8	7%	1	1%	0	0%	8	7%
TOTAL	**8.745**	3.974	**45%**	3.901	**45%**	1.116	**13%**	2.056	**24%**

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*	
Certification level reached'		**ADVANCED**		**ADVANCED**		**ADVANCED+**		**ADVANCED**	
Number of false positives*		*few*		*very few*		*few*		*few*	
On-demand scanning speed*		*average*		*average*		*fast*		*average*	
ProActive detection of "NEW" samples''									
DOS malware	35	7	20%	9	26%	16	46%	5	14%
Windows viruses	39	2	5%	8	21%	19	49%	2	5%
Script malware	217	26	12%	35	16%	31	14%	58	27%
Worms	502	33	7%	111	22%	409	81%	201	40%
Backdoors	3.836	1.685	44%	1.477	39%	2.946	77%	1.316	34%
Trojans	3.638	76	2%	725	20%	1.382	38%	583	16%
other malware	356	232	65%	279	78%	223	63%	234	66%
OtherOS malware	122	8	7%	19	16%	8	7%	0	0%
TOTAL	**8.745**	2.069	**24%**	2.663	**30%**	5.034	**58%**	2.399	**27%**



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	
Certification level reached*		**STANDARD**		**ADVANCED**		**ADVANCED+**		**ADVANCED**	
Number of false positives*		*none*		*few*		*few*		*many*	
On-demand scanning speed*		*average*		*fast*		*slow*		*slow*	
ProActive detection of "NEW" samples**									
DOS malware	35	14	40%	4	11%	16	46%	25	71%
Windows viruses	39	6	15%	6	15%	8	21%	6	15%
Script malware	217	37	17%	17	8%	24	11%	23	11%
Worms	502	109	22%	92	18%	324	65%	160	32%
Backdoors	3.836	772	20%	1.412	37%	2.130	56%	2.692	70%
Trojans	3.638	242	7%	832	23%	1.461	40%	1.780	49%
other malware	356	237	67%	232	65%	269	76%	249	70%
OtherOS malware	122	14	11%	0	0%	8	7%	0	0%
TOTAL	**8.745**	1.431	**16%**	2.595	**30%**	4.240	**48%**	4.935	**56%**



4. Summary results

The results show the pure proactive on-demand[2] detection capabilities of the scan engines. The percentages are rounded to the nearest whole number.

Do not take the results as an absolute assessment of quality - they just give an idea of who detected more, and who less, in this specific test. To know how these anti-virus products perform with updated signatures, please have a look at our on-demand tests of February and August.

Readers should take a look at the results and build an opinion based on their needs. All the tested products are already selected from a group of very good scanners and if used correctly and kept up-to-date, users can feel safe with any of them. Read more in the previous February 2006 comparative.

Please also have a look on our methodology document for further details (http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf).

[2] this test is performed on-demand – it is NOT a realtime/on-access test

Below are the results obtained by each scanner in the various categories, sorted by detection rate:

(a) ProActive detection of new Backdoors, Trojans and other malware:

1.	VBA32	60%
2.	NOD32	58%
3.	AVIRA	56%
4.	AVK	51%
5.	TrustPort	49%
6.	BitDefender, Dr.Web	46%
7.	McAfee, Panda	32%
8.	Norman	27%
9.	Kaspersky, F-Secure	25%
10.	Avast	23%
11.	Symantec	16%
12.	F-Prot	13%
13.	AVG	5%

(b) ProActive detection of new Worms, DOS, Windows, OtherOS and Script viruses/malware:

1.	NOD32	53%
2.	TrustPort, AVK	42%
3.	BitDefender	39%
4.	AVIRA	37%
5.	Dr.Web	33%
6.	Norman	29%
7.	VBA32	23%
8.	AVG, McAfee, Symantec	20%
9.	F-Prot	15%
10.	Avast	14%
11.	Panda	13%
12.	Kaspersky, F-Secure	8%

(c) ProActive detection of all new samples used in the test:

1.	NOD32	58%
2.	VBA32	56%
3.	AVIRA	54%
4.	AVK	50%
5.	TrustPort	48%
6.	BitDefender, Dr.Web	45%
7.	McAfee, Panda	30%
8.	Norman	27%
9.	Kaspersky, F-Secure	24%
10.	Avast	22%
11.	Symantec	16%
12.	F-Prot	13%
13.	AVG	7%

Please also have a look at the overviews that can be found on the website, to see how the scanners scored in this, and in past, tests. Always check for the latest data available on our website – the previous data of 6 months ago can now be considered outdated.

Note: AVK, F-Secure and TrustPort are multi-engine AV’s.

5. False positive/alarm test

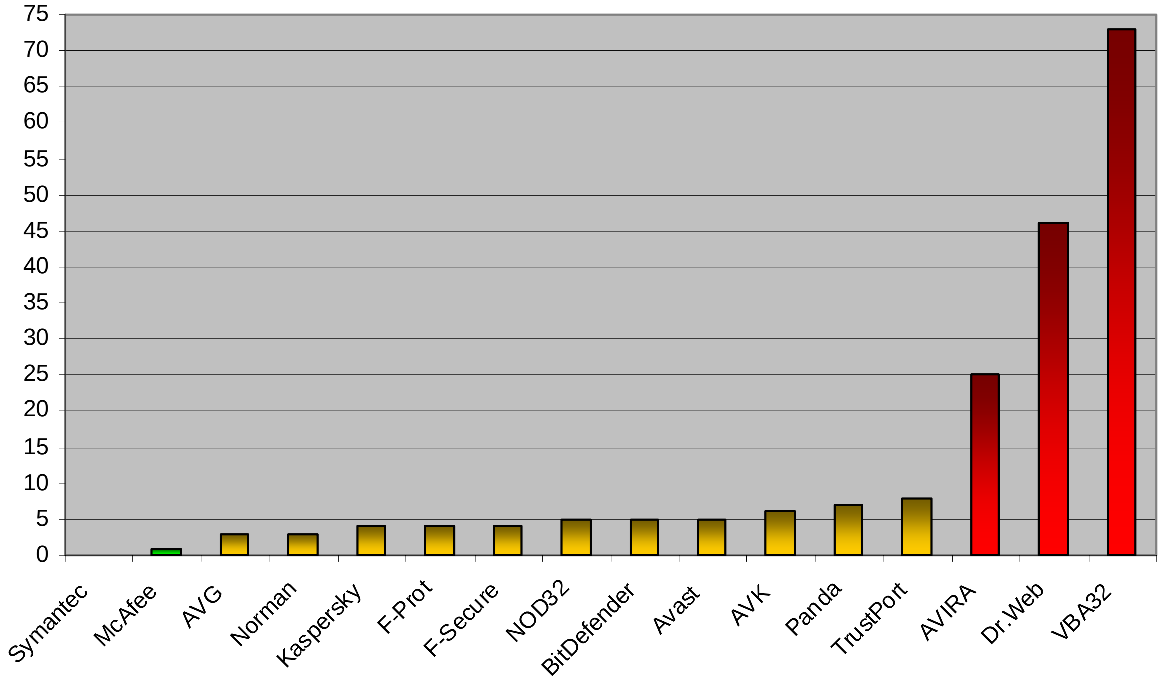
Starting from 2006, we provide in our retrospective test reports also a false alarm test, in order to better evaluate the quality of the proactive detection capabilities. Like every new test introduction, we will improve this test in the future and continuosly extend it. This test also demonstrates that also with deactivated heuristics false alarms can occur. A false alarm (false positive) is when an Anti-Virus product flags an innocent file to be infected when it is not. False alarms can sometimes cause as much troubles like a real infection.

Number of false positives found[3]:

1.	Symantec	0	none or very few FP's
2.	McAfee	1	
3.	AVG, Norman	3	few FP's
4.	Kaspersky, F-Prot, F-Secure	4	
5.	NOD32, BitDefender, Avast	5	
6.	AVK	6	
7.	Panda	7	
8.	TrustPort	8	
9.	AVIRA	25	many FP's
10.	Dr.Web	46	
11.	VBA32	73	

Products with high proactive detection, but many FP's (false positives) can not gain our ADVANCED+ award (in that case they would get the next lower award, ADVANCED).

The graph below demonstrates the number of false positives by the various Anti-Virus products:



[3] Lower is better

5.1 Details of the false positives detected

All listed false alarms were reported and sent to the Anti-Virus vendors and should now be fixed. As we sent the false alarms to the vendors, in future false alarm tests the number of false positives will possibly be much lower (hopefully near to zero). Please note that if a product caused a false alarm e.g. on various versions of a program in very similar packages, we count it here as only 1 false alarm.

False alarms caused by unencrypted data blocks in Anti-Virus related files are also not counted in this test.

Please also read the comments under the tables to know what we mean by "heuristic" and "signature" – sometimes it simply means the false alarm occurred with heuristics turned off and due to that it was counted as signature.

Below are the details on which packages the false alarms occurred by the following AV products: Avast, F-Prot, AntiVir (AVIRA), BitDefender, McAfee, Dr.Web, F-Secure, AVK (GDATA), Kaspersky, Norman, Symantec, NOD32 (ESET), Panda, TrustPort, AVG, VBA32.

Avast

False alarm found in some part(s) of	Detected as	By
Golden FTP Server package	Win32:Trojan-gen. {Other}	Signature
Kindersicherung package	Win32:Trojan-gen. {Other}	Signature
PEINFO tool	Win32:Simile	Signature
SharpPix package	Win32:Trojan-gen. {Other}	Signature
UNAFS package	Win32:Trojan-gen. {Other}	Signature

Avast and also other Anti-Virus products are very likely to have false alarms on Panda's signature database and files, but we do not count them as false alarms, as it is the "fault" of the companies which did not encrypt their signatures/databases properly (http://faq.avast.com/eng/faq_panda.html). The same applies, for example, to some stand-alone removers provided by various other companies (ghost positives[4]).

F-Prot

False alarm found in some part(s) of	Detected as	By
3Com WebCam Lite package	could be a destructive program	Heuristic
BusiMate package	could be a destructive program	Heuristic
M@xTax Standard package	could be a suspicious file	Signature
NewsBin Professional package	security risk or a "backdoor" program	Signature

The false alarms marked as 'Signature', will happen also if F-Prot's heuristics are disabled. Encrypted programs in archives may get flagged as suspicious, and also files with double executable extensions.

[4] unencrypted data blocks inside AV related files

AntiVir (AVIRA)

False alarm found in some part(s) of	Detected as	By
AutoDialRun package	HEURISTIC/Trojan.Keylogger	Heuristic
BlueSeries Splitting package	HEURISTIC/Malware.Layered	Heuristic
BootStrapper package	HEURISTIC/Malware.Modified	Heuristic
CleanFormat package	HEURISTIC/Macro.Word2000	Heuristic
Dashboard package	W32/HLLW.Antinn.H.2	Signature
Datawest ConCentre Support package	WORM/Vimover	Signature
Desktop Icon Manager package	HEURISTIC/Trojan.Keylogger	Heuristic
E-mail Scanner package	HEURISTIC/Trojan.Keylogger	Heuristic
IDA package (Keil C166)	HEURISTIC/Virus.Win32	Heuristic
lySoft package	HEURISTIC/Hijacker	Heuristic
Medion driver package (attrib.com)	Wonder virus	Signature
Microsoft Windows 2000 SP3 Hotfix	HEURISTIC/Hijacker	Heuristic
Microsoft Windows 2000 SP2 update package	HEURISTIC/Hijacker	Heuristic
MR-Toolbox package	HEURISTIC/Macro.Excel2000	Heuristic
Softboot package	HEURISTIC/Hijacker	Heuristic
Spirex Screensaver package	HEURISTIC/Hijacker	Heuristic
T-Mobile package (ByteMobile)	HEURISTIC/Hijacker	Heuristic
TrendMicro OfficeScan ClientUtility	HEURISTIC/Backdoor.Dropper	Heuristic
TrendMicro OfficeScan POP3pack	HEURISTIC/Backdoor.Dropper	Heuristic
TrendMicro OfficeScan Webinstall	HEURISTIC/Backdoor.Generic	Heuristic
TrendMicro PC-Cillin package (tmproxy.exe)	HEURISTIC/Backdoor.Generic	Heuristic
TuxPaint package	EXP/JS.Active.8	Signature
VirSort package (help file)	WORM/Manymize	Signature
Webroot SpyAudit package	HEURISTIC/Trojan.Downloader	Heuristic
WinHex package	HEURISTIC/Hijacker	Heuristic

AVIRA had 25 false alarms, including on some files from Microsoft products. Due to this, it can not gain our ADVANCED+ award in the retrospective test.

BitDefender

False alarm found in some part(s) of	Detected as	By
Corel Linux package	UNIX.Klizan.A	Signature
MiniMail package	Trojan.PWS.Bancos.142	Signature
PCW add-on package	Type_VBS_Infector	Heuristic
TransMac package	Backdoor.Agobot.AFZ	Signature
Weather Display package	BehavesLike:Trojan.HangUp	Heuristic

Bitdefender had relatively few false alarms.

McAfee

False alarm found in some part(s) of	Detected as	By
AddTime package	Generic Delphi	Signature

McAfee had only one false alarm. The false alarm occurred even with heuristics turned off, so it is counted here as signature detection. Like Symantec, also McAfee shows to have a high quality assurance before releasing updates, in order to avoid false positives. Even so, mistakes can happen occasionally even after stringent QA testing.

Dr.Web

False alarm found in some part(s) of	Detected as	By
Acrobat Reader package	modification of VBS.FreeLink	Signature
ADV Grid package	modification of Win32.Swaduk.6891	Signature
AntiVir package	probably WIN.WORM.Virus	Heuristic
Anvil Studio package	modification of BAT.Mtr.1429	Signature
AOL package	probably BACKDOOR.Trojan	Heuristic
Application Access Server package	modification of BackDoor.Generic.1261	Signature
ASAP Utilities package	W97M.Iseng	Signature
Autostart Application Checker package	probably SCRIPT.BATCH.Virus	Heuristic
Clip Magic package	probably DLOADER.Trojan	Heuristic
CPU Info package	probably WIN.WORM.Virus	Heuristic
Datei Commander package	probably BACKDOOR.Trojan	Heuristic
Desktop Icons Manager package	probably DLOADER.Trojan	Heuristic
Favorite Startpage package	probably SCRIPT.Virus	Heuristic
FixFoto package	probably SCRIPT.Virus	Heuristic
FlexInfo package	probably BACKDOOR.Trojan	Heuristic
GoogleDesktopSearch package	probably DLOADER.Trojan	Heuristic
HardwareLister package	probably SCRIPT.Virus	Heuristic
IRCView package	probably BACKDOOR.IRC.Trojan	Heuristic
JDTricks package	probably DLOADER.Trojan	Heuristic
KidKey Internet Access Control package	probably BACKDOOR.Trojan	Heuristic
MessengerPlus! package	Trojan.Swizzor	Signature
Microsoft NetMeeting package	modification of Win32.Bumblebee.3649	Signature
Microsoft Office Standard 2003 Trial	modification of VBS.Petik	Signature
MiniMail package	Trojan.PWS.Bancos.142	Signature
NewsGroup Server Searcher package	modification of BackDoor.Generic.1116	Signature
PaintShopPro package	modification of Win32.Bumblebee.3833	Signature
ParanoIT package	probably DLOADER.Trojan	Heuristic
PDF Experte package	probably BACKDOOR.Trojan	Heuristic
PDF Machine package	probably BACKDOOR.Trojan	Heuristic
Pit's WinToys package	probably WIN.SCRIPT.BATCH.Virus	Heuristic
Registry System Wizard package	probably BACKDOOR.Trojan	Heuristic
RemoteKeys package	probably BACKDOOR.Trojan	Heuristic
SnipeMonkey package	probably DLOADER.Trojan	Heuristic
SoviewImageViewer package	probably DLOADER.Trojan	Heuristic
Synchronization Wizard package	probably SCRIPT.BATCH.Virus	Heuristic
ThunderBird Conpresso package	probably SCRIPT.Virus	Heuristic
TIF package	probably SCRIPT.Virus	Heuristic
ToolbarCop package	probably WIN.SCRIPT.Virus	Heuristic
TrendMicro InterScanVirusWall Samba package	modification of Trojan.DelSys.191	Signature
TrendMicro OfficeScan package	probably BACKDOOR.Trojan	Heuristic
VIA RhineFamily FastEthernetAdapter package	probably BACKDOOR.Trojan	Heuristic
Webroot Cache & Cookie Washer package	probably STPAGE.Trojan	Heuristic
WinAmp Bookmark package	probably SCRIPT.Virus	Heuristic
WinFAQ package	probably SCRIPT.BATCH.Virus	Heuristic
WinGuruXP Console package	probably BACKDOOR.Trojan	Heuristic
ZoneAlarm TrueVectorService package	probably BACKDOOR.Trojan	Heuristic

If Dr.Web’s heuristic analysis is turned off, the false alarms caused by the heuristics would not occur, but the others marked as “Signature” would happen anyway. Dr.Web had relatively many false positives, so it can not gain our ADVANCED+ award.

F-Secure

False alarm found in some part(s) of	Detected as	By
Autographics package	Type_Win32	Heuristic
Datawest ConCentre Support package	Email-Worm.Win32.Vimover	Heuristic
Fedora package	Trojan-Downloader.Win32.Delf.ij	Signature
TransMac package	Backdoor.Win32.Agobot.afz	Signature

In F-Secure it is not possible to turn off the heuristics. F-Secure had the same false positives as Kaspersky in this test because F-Secure’s product uses the AVP engine.

G DATA AVK

False alarm found in some part(s) of	Detected as	By
Autographics package	Type_Win32	Heuristic
Corel Linux package	UNIX.Klizan.A	Signature
MiniMail package	Trojan.PWS.Bancos.142	Signature
PCW add-on package	Type_VBS_Infector	Heuristic
TransMac package	Backdoor.Win32.Agobot.afz	Signature
Weather Display package	Trojan.HangUp	Heuristic

If the heuristic in AVK is turned off, the false alarms caused by the heuristics will not occur.

Kaspersky

False alarm found in some part(s) of	Detected as	By
Autographics package	Type_Win32	Heuristic
Datawest ConCentre Support package	Email-Worm.Win32.Vimover	Heuristic
Fedora package	Trojan-Downloader.Win32.Delf.ij	Signature
TransMac package	Backdoor.Win32.Agobot.afz	Signature

In Kaspersky’s product it is not possible to turn off the heuristics.

Norman

False alarm found in some part(s) of	Detected as	By
GXTranscoder package	Trojan W32/Zapchast.DA	Signature
eDonkey package	Worm W32/Mytob.RG	Signature
NetGroup package	Worm W32/HLLW.Gaobot.LY	Signature

Norman had few false positives in our test. Interesting that even though Norman is known for its heuristics, the 3 false alarms occurred all by signatures.

Symantec (NAV)

Symantec Norton Anti-Virus was the only Anti-Virus product in this test which had no false positives. This is an indication of high quality assurance tests before the release of updates in order to avoid false positives.

NOD32 (ESET)

False alarm found in some part(s) of	Detected as	By
AOL package	probably unknown NewHeur_PE virus (AH)	Heuristic
EmailArchitect Server 2004 package	probably unknown NewHeur_PE virus (AH)	Heuristic
MR-Toolbox package	probably unknown MACRO virus	Heuristic
NVIDIA Detonator 4 drivers package	probably unknown NewHeur_PE virus (AH)	Heuristic
SFX archives	Win95/SK virus (AH)	Heuristic

'AH' is NOD32 'Advanced Heuristic'. If AH is disabled, the false alarms with '(AH)' will not occur. The false alarm on the macro file occurs if NOD32's 'standard' heuristic is enabled. The false alarm on the SFX archives was due to an incorrect detection algorithm. As it happened only if AH is turned on, it will be counted here as heuristic detection.

Panda

False alarm found in some part(s) of	Detected as	By
AntiSpamWolf package	Suspicious file	Heuristic
ASUS Firmware packages	Suspicious file	Heuristic
DirectX package	Suspicious file	Heuristic
Gmail Notifier for Miranda package	Suspicious file	Heuristic
MobileNetSwitch package	Suspicious file	Heuristic
Mozilla package	Univ	Signature
PhotoArtMaster Classic package	Suspicious file	Heuristic

Panda had 7 false alarms: 6 with heuristics turned on and 1 with heuristics turned off.

TrustPort

False alarm found in some part(s) of	Detected as	By
Corel Linux package	UNIX.Klizan.A	Signature
eDonkey package	Worm W32/Mytob.RG	Signature
GXTranscoder package	Trojan W32/Zapchast.DA	Signature
MiniMail package	Trojan.PWS.Bancos.142	Signature
NetGroup package	Worm W32/HLLW.Gaobot.LY	Signature
PCW add-on package	Type_VBS_Infector	Heuristic
TransMac package	Backdoor.Agobot.AFZ	Signature
Weather Display package	BehavesLike:Trojan.HangUp	Heuristic

TrustPort had the same false positives as the two engines it uses: Bitdefender and Norman.

AVG

False alarm found in some part(s) of	Detected as	By
DOS4ME package	unknown virus .TSR	Heuristic
GDATA AVK package	Trojan.PSW.Generic.OI	Signature
MP3Totale package	Trojan.Small.AN	Signature

AVG had few false positives: 2 by signatures and 1 by heuristic.

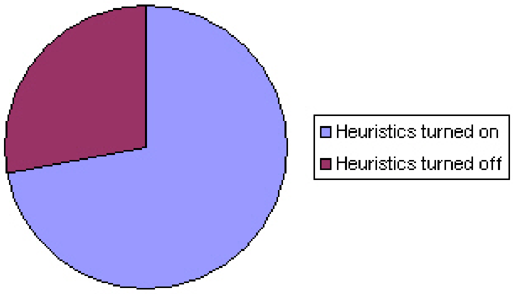
VBA32

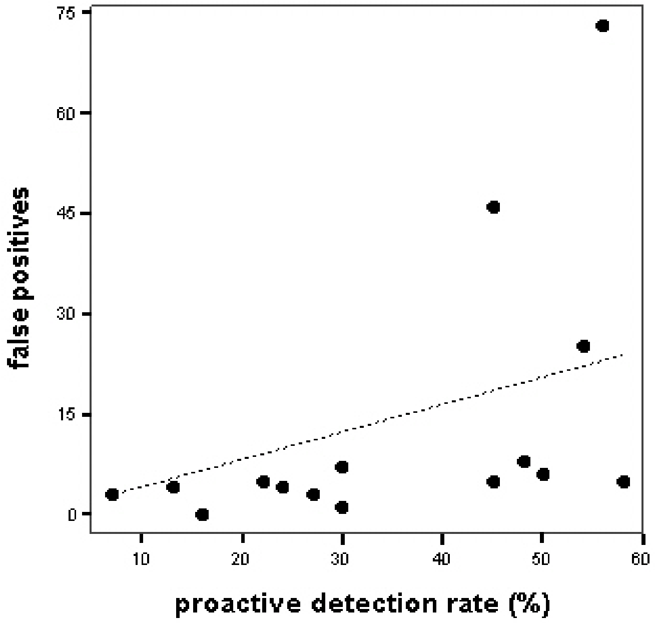
False alarm found in some part(s) of	Detected as	By
A+Webfilter package	Trojan-Downloader.Agent.34 (+)	Heuristic
Acearth package	Unknown.OvrVirus (+)	Heuristic
ADSLKeepAlive package	Email-Worm.VB.3	Heuristic
AHM Triton Tools package	Unknown.OvrVirus (+)	Heuristic
Airscanner Mobile Anti-Virus package	Backdoor.WinCE.Brador.a	Signature
AirSnare package	Trojan-PSW.VB.14 (+)	Heuristic
AmP package	Trojan.Delf.51 (+)	Heuristic
ANDRoute 2004 package	Trojan-Spy.Win32.SCKeyLog.o	Signature
Application LogServer package	Trojan-Downloader.Agent.59 (+)	Heuristic
AutoDialRun package	SMS-Flooder.Delf.1	Heuristic
AVI FourCC Changer package	Backdoor.Delf.187 (+)	Heuristic
Beam4Free package	Malware.Agent.21 (+)	Heuristic
BrandAwareness 2006 package	Trojan-PSW.Delf.53 (+)	Heuristic
Buggy MP3 Player package	Backdoor.Delf.151 (+)	Heuristic
CD Hopper package	Backdoor.Delf.151 (+)	Heuristic
CDH Productions package	Malware.VB.11 (+)	Heuristic
cFosSpeed package	Backdoor.PcClient.36 (+)	Heuristic
Clipboard Manager package	Trojan-Downloader.Agent.101	Heuristic
Cookie Muncher package	Backdoor.Delf.151 (+)	Heuristic
DeepBurner package	Trojan-Spy.Banker.66 (+)	Heuristic
DiaShow package	Trojan-Downloader.Delf.34	Heuristic
DropUpload package	Downloader.Small.60 (+)	Heuristic
EZMem Optimizer package	Malware.VB.38 (+)	Heuristic
FahrschuleXP package	Malware.VB.38 (+)	Heuristic
FastreamFTP package	Backdoor.Delf.83 (+)	Heuristic
Fedora package	Unknown.OvrVirus (+)	Heuristic
F-Secure OnlineScanner package	Porn-Dialer.Win32.Agent.p	Signature
FullMotion Video package	Trojan.VB.36 (+)	Heuristic
GoldMine package	Backdoor.Delf.151 (+)	Heuristic
KomaMail package	Backdoor.GrayBird.1 (+)	Heuristic
LittleBigBar package	Trojan-Downloader.Delf.28 (+)	Heuristic
MapCreator package	Backdoor.IRC.Zcrew	Signature
Messenger Plus! package	Trojan-Downloader.Win32.Swizzor.ag	Signature
MIA package	Malware.Delf.6 (+)	Heuristic
Microsoft Windows 2000 package	Unknown.OvrVirus (+)	Heuristic
Microsoft Windows XP Pro SP1 package	Unknown.OvrVirus (+)	Heuristic
Microsoft Windows XP Pro SP2 package	Unknown.OvrVirus (+)	Heuristic
Microsoft Windows XP Pro SP2 Update package	Unknown.OvrVirus (+)	Heuristic
Mr.Mirror package	Trojan-Downloader.IstBar.39	Heuristic
MusicBase package	Backdoor.Delf.159 (+)	Heuristic
Mystik Media package	Malware.VB.11 (+)	Heuristic
NaturalVoice Reader package	Malware.VB.40	Heuristic
NCN Messenger package	Worm.VB.1 (+)	Heuristic
OpenClipArt package	Unknown.OvrVirus (+)	Heuristic
OpenOffice package	Unknown.OvrVirus (+)	Heuristic
OutlookUncut package	Trojan-Downloader.Delf.34	Heuristic
PACSpamPro package	Malware.VB.30	Heuristic
PC Monitoring package	Trojan-Spy.Delf.1	Heuristic
PCW add-on package	Trojan-Downloader.Delf.28	Heuristic
PCW Trigger package	Trojan.Delf.51 (+)	Heuristic

PestPatrol package	Trojan-Spy.Win32.SCKeyLog.o	Signature
Portable OpenOffice package	Unknown.OvrVirus (+)	Heuristic
PVAStrumento package	Unknown.OvrVirus (+)	Heuristic
Safe2Bid package	Malware.VB.38 (+)	Heuristic
SoundControl package	Backdoor.Delf.151 (+)	Heuristic
SPSS package	Backdoor.WinCE.Brador.a	Signature
Star package	Malware.Agent.31 (+)	Heuristic
Symantec Anti-Virus package	Trojan-Proxy.Win32.Agent.ay	Signature
TeleGeiz package	Backdoor.Delf.74 (+)	Heuristic
TinyResMeter package	Trojan-Downloader.Delf.31 (+)	Heuristic
TrafficMonitor package	Backdoor.Delf.117	Heuristic
TransMac package	Backdoor.Win32.Agobot.afz	Signature
TrendMicro InternetSecurity package	Trojan-Spy.Agent.45 (+)	Heuristic
TuneUp Utilities package	Trojan-PSW.Delf.10	Heuristic
USR X11R6 package	Unknown.OvrVirus (+)	Heuristic
VersionBackupMaster package	Trojan-Downloader.Delf.10 (+)	Heuristic
VoltoCDDB package	Trojan.StartPage.77 (+)	Heuristic
WebCreator package	Trojan-Spy.Delf.61	Heuristic
WinAce package	Backdoor.Delf.150 (+)	Heuristic
WinComma package	Trojan-Dropper.Delf.35 (+)	Heuristic
WinSettings2005 package	I-Worm.Psw-protected	Heuristic
XPlite2000 package	Trojan.Delf.51 (+)	Heuristic
Zoner Draw package	Trojan-Spy.Win32.SCKeyLog.o	Signature

The heuristic detections marked with (+) occur if VBA32 heuristics are set to high/excessive. The other heuristic detections occur even if the heuristics are set to optimal. VBA32 had many false positives, including on some quite well known applications.

The following graph on the left side shows that around 1/4 of the false positives occurred even with heuristic options turned off.
As there is in general a positive correlation between the number of false positives and the proactive detection rates (graphical demonstration on the right side), products with many false positives will not receive the ADVANCED+ certification.



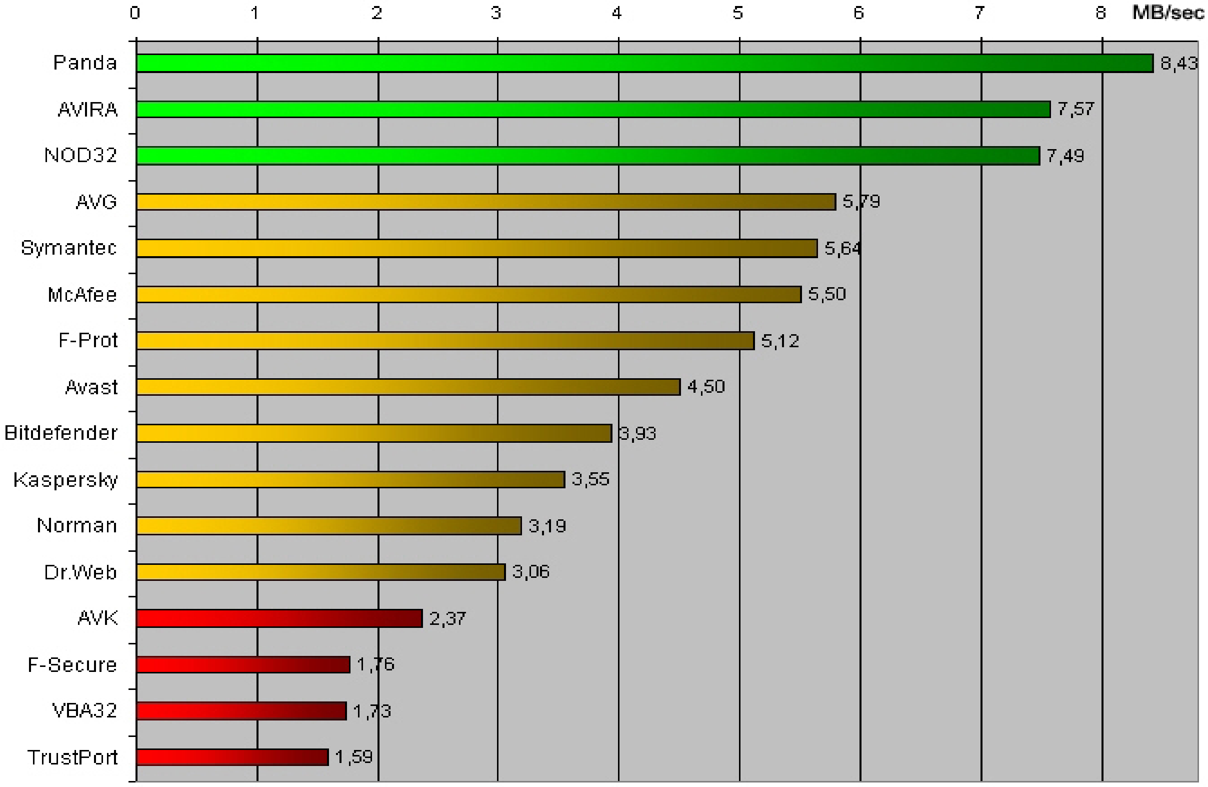


6. Scanning speed test

Starting from 2006, we now provide in our retrospective test reports a scanning speed test. Like every new test introduction, we will improve this test in the future and expand it in order to provide better and more data.

Some scanners may be slower than others due various reasons. It has to be taken in account how reliable the detection rate of an Anti-Virus is; if the Anti-Virus product will detects difficult polymorphic viruses (emulation: some Anti-Virus vendors do not include detection for some difficult polymorphic viruses in their products to avoid performance problems with their engine), deep heuristic scan analysis, unpacking and un-archiving support, hardware used, etc.

The following graph shows the throughput rate in MB/sec (higher is faster) of the various Anti-Virus products when scanning (on-demand) our whole clean files set (used for the false alarm testing). The scanning throughput rate will vary based on the set of clean files[5] and the settings in the product[6]. In future[7] we will provide more data, e.g. scanning speed based on various sets of clean files (OS system files, etc.) and using various settings.



The average scanning throughput rate (scan speed) is calculated by size of clean-set in MB’s divided by time needed to finish the scan in seconds. The scanning throughput rate of this test can not be compared with future tests or with other tests, as it varies from the set of files used etc.

The scanning speed tests were done under Windows XP SP2, on a PC with Intel Pentium 4 HT 2.8 GHz, ASUS P4C800, 512 MB RAM and without network connection.

[5] to know how fast the various products would be on your PC at scanning *your* files, try yourself the products

[6] we used the best possible detection settings

[7] we can not do it already this year, because most of us are quite busy with finishing the university studies. After we all have finished our studies, we will probably be able to provide even better comparatives.

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). The following certification levels are for the results reached in the retrospective test:

CERTIFICATION LEVELS	PRODUCTS (in alphabetical order)
AV comparatives ADVANCED+ ★★★ May 06 proactive/retrospective test	AVK BitDefender NOD32 TrustPort
AV comparatives ADVANCED ★★ May 06 proactive/retrospective test	Avast AVIRA Dr.Web F-Secure Kaspersky McAfee Norman Panda VBA32
AV comparatives STANDARD ★ May 06 proactive/retrospective test	AVG F-Prot Symantec

Please note that products with a high rate of false alarms can not gain the ADVANCED+ level, even if they had a high detection rate in the retrospective test (i.e. AVIRA, Dr.Web, VBA32).

8. 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 AV-Comparatitves, 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 (May 2006)