Anti-Virus Comparative No.12

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

contains also

False positive test
&
Scanning speed test

Date: November 2006 (2006-11)

Last revision: 22th November 2006

Author: Andreas Clementi

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

1. Introduction

This test report is the second part of the August 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[1] that the scan engines had in the last comparative, were used for this tests. For this test we used new samples[2] received between 7th August and 7th November 2006, which were all new to any tested product. The following 16 products were tested in this comparative (last signature updates and versions are from 7th August 2006):

- Avast! 4.7.869 Professional Edition
- AVG Professional 7.1.405
- AVIRA AntiVir Personal Edition Premium 7.01.01.02
- BitDefender Anti-Virus 9.5 Professional Plus
- Dr.Web Anti-Virus for Windows 95-XP 4.33.2
- ESET NOD32 Anti-Virus 2.51.26
- F-Prot Anti-Virus for Windows 3.16f
- F-Secure Anti-Virus 6.12.90
- Gdata AntiVirusKit (AVK) 16.0.7 (2006)
- Kaspersky Anti-Virus 6.0.0.303
- McAfee VirusScan 11.0.209
- Norman Virus Control 5.81
- Symantec Norton Anti-Virus 12.2.0.13
- TrustPort Antivirus Workstation 2.0.0.843
- VBA32 Workstation 3.11.0

2. Description

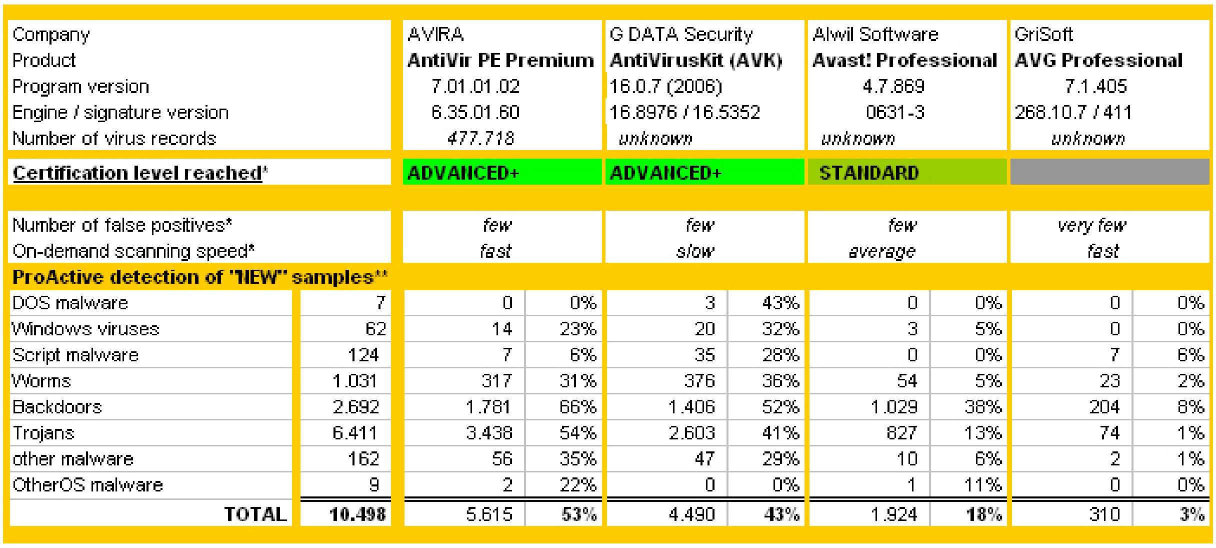
Anti-Virus products often claim to have high proactive detection capabilities – far higher than those reached in this test. This isn't just a self-promotional statement; it's possible that products reach the stated percentages, but this depends on the duration of the test-period, the size of the sample 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] The best possible detection settings were used in all the tests included in this report.

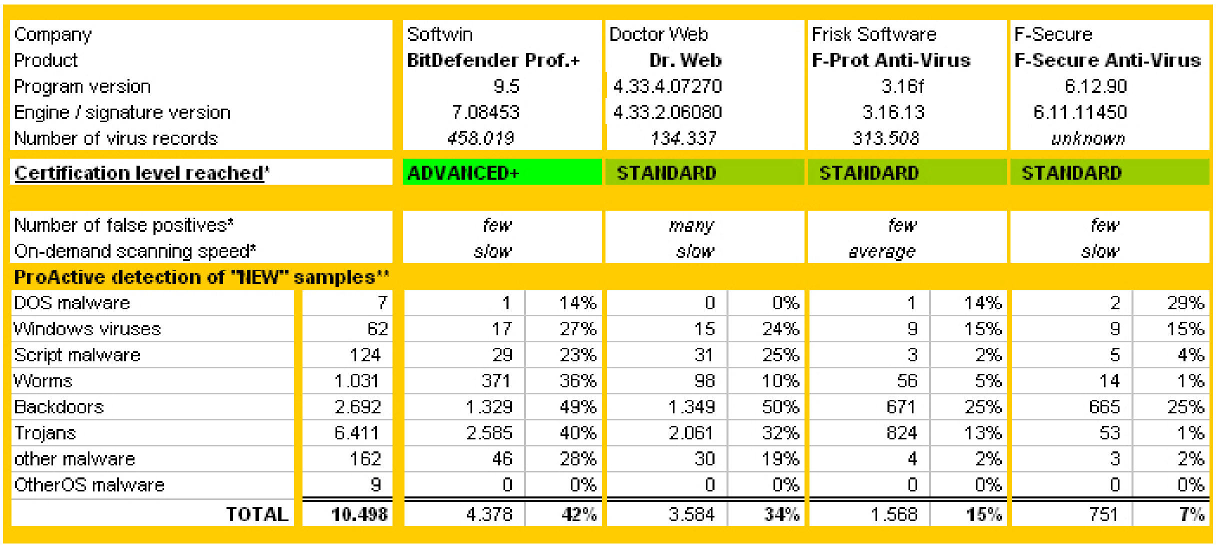
[2] Typical Spyware, Adware, tools, etc. are not included.

3. Test results

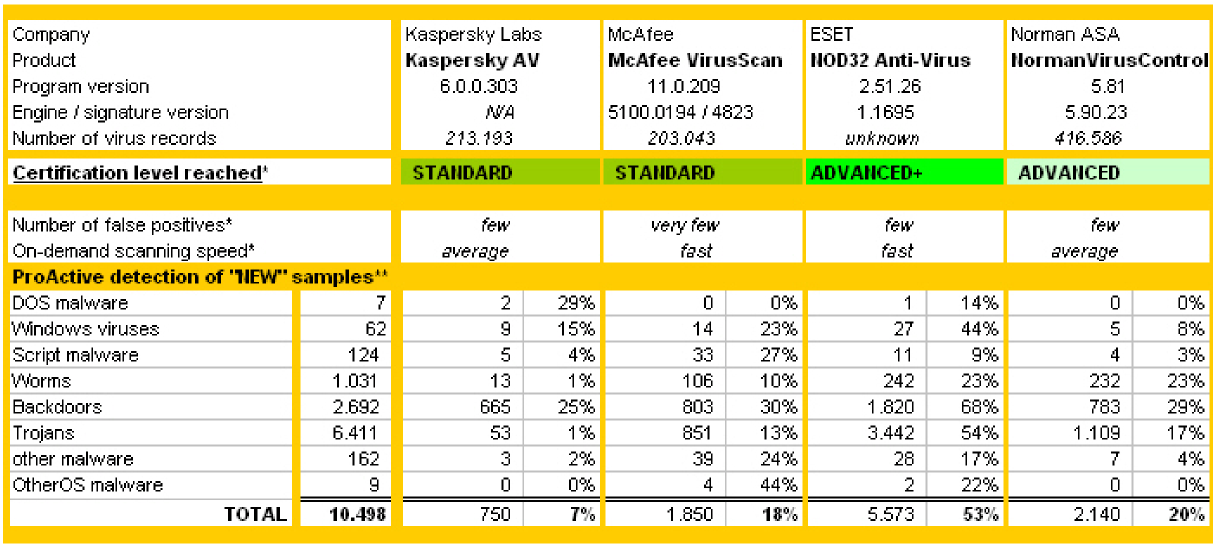
Below the detailed test result tables of all tested products:



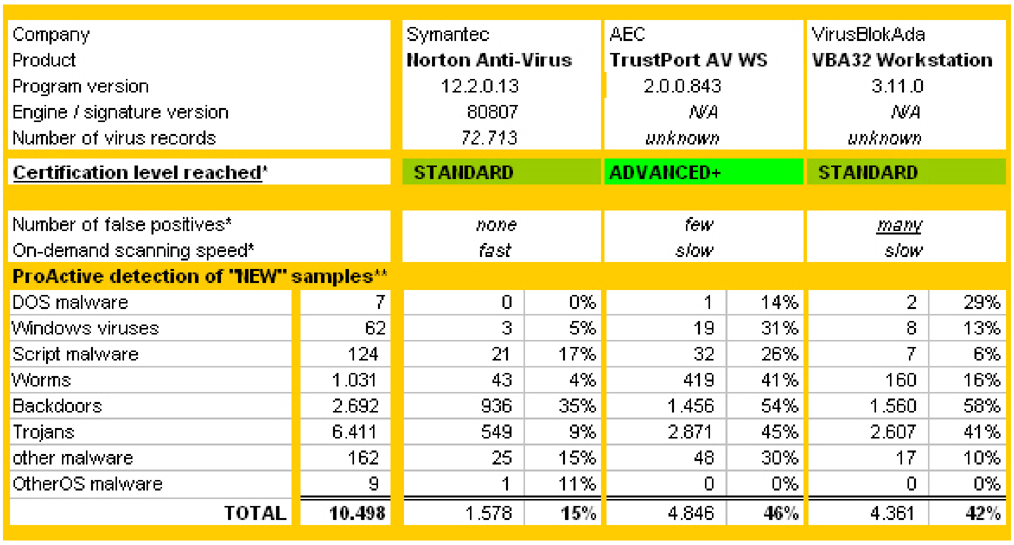
Company		AVIRA		G DATA Security		Alwil Software		GriSoft	
Product		**AntiVir PE Premium**		**AntiVirusKit (AVK)**		**Avast! Professional**		**AVG Professional**	
Program version		7.01.01.02		16.0.7 (2006)		4.7.869		7.1.405	
Engine / signature version		6.35.01.60		16.8976 / 16.5352		0631-3		268.10.7 / 411	
Number of virus records		*477.718*		*unknown*		*unknown*		*unknown*	
Certification level reached*		**ADVANCED+**		**ADVANCED+**		**STANDARD**			
Number of false positives*		*few*		*few*		*few*		*very few*	
On-demand scanning speed*		*fast*		*slow*		*average*		*fast*	
ProActive detection of "NEW" samples**									
DOS malware	7	0	0%	3	43%	0	0%	0	0%
Windows viruses	62	14	23%	20	32%	3	5%	0	0%
Script malware	124	7	6%	35	28%	0	0%	7	6%
Worms	1.031	317	31%	376	36%	54	5%	23	2%
Backdoors	2.692	1.781	66%	1.406	52%	1.029	38%	204	8%
Trojans	6.411	3.438	54%	2.603	41%	827	13%	74	1%
other malware	162	56	35%	47	29%	10	6%	2	1%
OtherOS malware	9	2	22%	0	0%	1	11%	0	0%
TOTAL	**10.498**	5.615	**53%**	4.490	**43%**	1.924	**18%**	310	**3%**



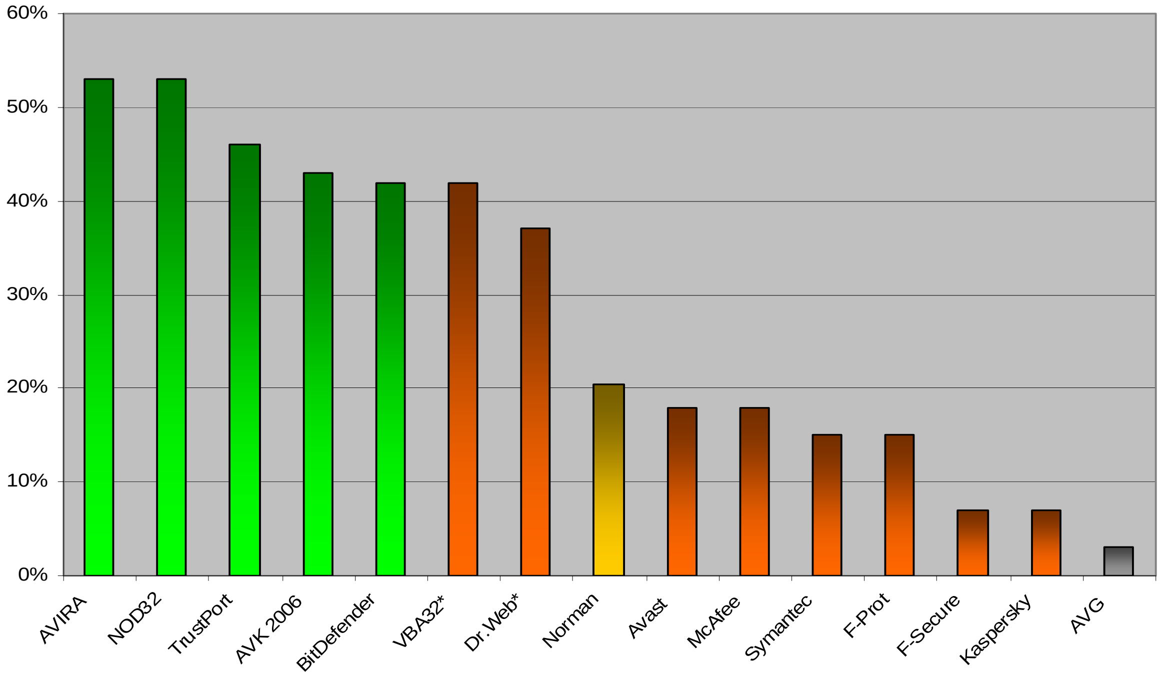
Company		Softwin		Doctor Web		Frisk Software		F-Secure	
Product		**BitDefender Prof.+**		**Dr. Web**		**F-Prot Anti-Virus**		**F-Secure Anti-Virus**	
Program version		9.5		4.33.4.07270		3.16f		6.12.90	
Engine / signature version		7.08453		4.33.2.06080		3.16.13		6.11.11450	
Number of virus records		*458.019*		*134.337*		*313.508*		*unknown*	
Certification level reached*		**ADVANCED+**		**STANDARD**		**STANDARD**		**STANDARD**	
Number of false positives*		*few*		*many*		*few*		*few*	
On-demand scanning speed*		*slow*		*slow*		*average*		*slow*	
ProActive detection of "NEW" samples**									
DOS malware	7	1	14%	0	0%	1	14%	2	29%
Windows viruses	62	17	27%	15	24%	9	15%	9	15%
Script malware	124	29	23%	31	25%	3	2%	5	4%
Worms	1.031	371	36%	98	10%	56	5%	14	1%
Backdoors	2.692	1.329	49%	1.349	50%	671	25%	665	25%
Trojans	6.411	2.585	40%	2.061	32%	824	13%	53	1%
other malware	162	46	28%	30	19%	4	2%	3	2%
OtherOS malware	9	0	0%	0	0%	0	0%	0	0%
TOTAL	**10.498**	4.378	**42%**	3.584	**34%**	1.568	**15%**	751	**7%**



Company		Kaspersky Labs		McAfee		ESET		Norman ASA	
Product		**Kaspersky AV**		**McAfee VirusScan**		**NOD32 Anti-Virus**		**NormanVirusControl**	
Program version		6.0.0.303		11.0.209		2.51.26		5.81	
Engine / signature version		N/A		5100.0194 / 4823		1.1695		5.90.23	
Number of virus records		*213.193*		*203.043*		*unknown*		*416.586*	
Certification level reached*		**STANDARD**		**STANDARD**		**ADVANCED+**		**ADVANCED**	
Number of false positives*		*few*		*very few*		*few*		*few*	
On-demand scanning speed*		*average*		*fast*		*fast*		*average*	
ProActive detection of "NEW" samples**									
DOS malware	7	2	29%	0	0%	1	14%	0	0%
Windows viruses	62	9	15%	14	23%	27	44%	5	8%
Script malware	124	5	4%	33	27%	11	9%	4	3%
Worms	1.031	13	1%	106	10%	242	23%	232	23%
Backdoors	2.692	665	25%	803	30%	1.820	68%	783	29%
Trojans	6.411	53	1%	851	13%	3.442	54%	1.109	17%
other malware	162	3	2%	39	24%	28	17%	7	4%
OtherOS malware	9	0	0%	4	44%	2	22%	0	0%
TOTAL	**10.498**	750	**7%**	1.850	**18%**	5.573	**53%**	2.140	**20%**



Company Product Program version Engine / signature version Number of virus records		Symantec **Norton Anti-Virus** 12.2.0.13 80807 *72.713*		AEC **TrustPort AV WS** 2.0.0.843 *N/A* *unknown*		VirusBlokAda **VBA32 Workstation** 3.11.0 *N/A* *unknown*	
Certification level reached*		**STANDARD**		**ADVANCED+**		**STANDARD**	
Number of false positives* On-demand scanning speed*		*none* *fast*		*few* *slow*		*many* *slow*	
ProActive detection of "NEW" samples**							
DOS malware	7	0	0%	1	14%	2	29%
Windows viruses	62	3	5%	19	31%	8	13%
Script malware	124	21	17%	32	26%	7	6%
Worms	1.031	43	4%	419	41%	160	16%
Backdoors	2.692	936	35%	1.456	54%	1.560	58%
Trojans	6.411	549	9%	2.871	45%	2.607	41%
other malware	162	25	15%	48	30%	17	10%
OtherOS malware	9	1	11%	0	0%	0	0%
TOTAL	**10.498**	1.578	**15%**	4.846	**46%**	4.361	**42%**



4. Summary results

The results show the pure proactive on-demand[3] 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 August 2006 comparative.

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

[3] 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.	NOD32, AVIRA	57%
2.	TrustPort	47%
3.	VBA32	45%
4.	AVK 2006	44%
5.	BitDefender	43%
6.	Dr.Web	37%
7.	Norman, Avast	20%
8.	McAfee	18%
9.	Symantec, F-Prot	16%
10.	Kaspersky, F-Secure	8%
11.	AVG	3%

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

1.	TrustPort	38%
2.	AVK 2006	35%
3.	BitDefender	34%
4.	AVIRA	28%
5.	NOD32	23%
6.	Norman	20%
7.	VBA32	14%
8.	McAfee	13%
9.	Dr.Web	12%
10.	F-Prot, Symantec	6%
11.	Avast	5%
12.	F-Secure, KAV, AVG	2%

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

1.	AVIRA, NOD32	53%
2.	TrustPort	46%
3.	AVK 2006[4]	43%
4.	BitDefender, VBA32	42%
5.	Dr.Web	37%
6.	Norman	20%
7.	Avast, McAfee	18%
8.	Symantec, F-Prot	15%
9.	F-Secure, Kaspersky	7%
10.	AVG	3%

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.

[4] AVK 2007 uses now the Avast engine instead of the Bitdefender engine along with the Kaspersky engine; therefore AVK2007 would in this test not have reached only the STANDARD award.

5. False positive/alarm test

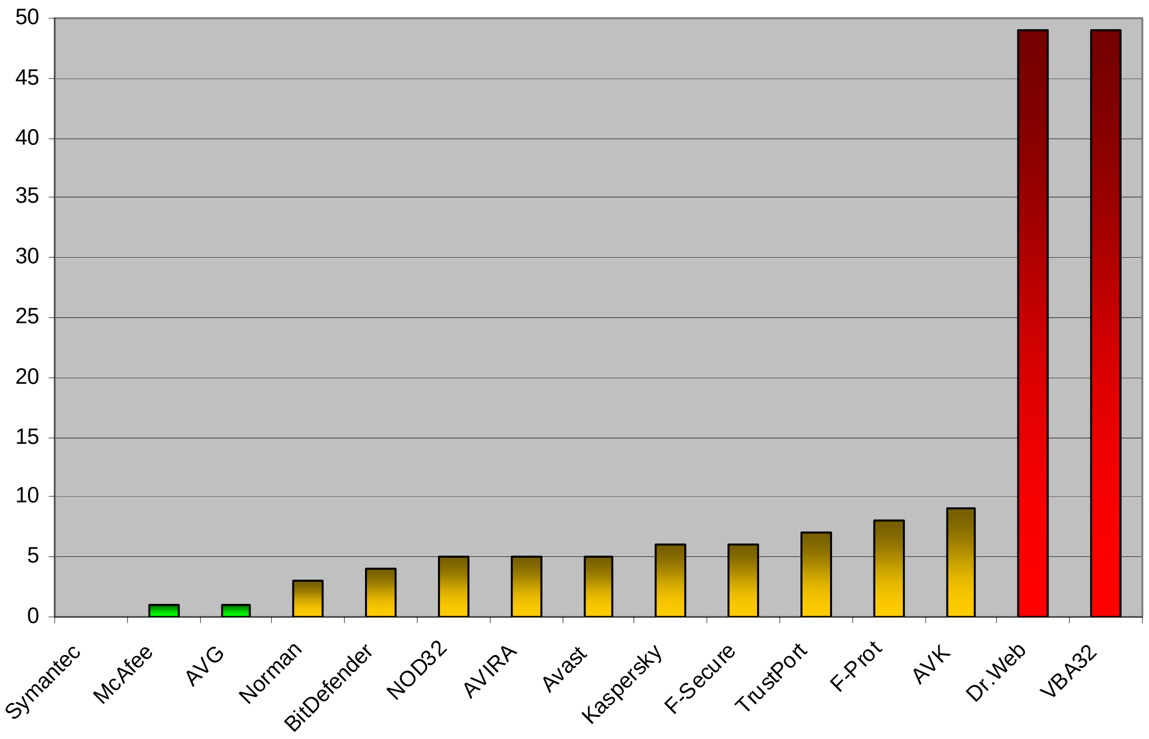
We provide in our retrospective test reports also a false alarm test, in order to better evaluate the quality of the proactive detection capabilities. This test also demonstrates that also with deactivated heuristics false alarms can occur.
A false alarm (false positive) is when an Anti-Virus product 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[5]:

1. Symantec	0	none or very few FP's
2. McAfee, AVG	1	
3. Norman	3	few FP's
4. BitDefender	4	
5. Avast, AVIRA, NOD32	5	
6. Kaspersky, F-Secure	6	
7. TrustPort	7	
8. F-Prot	8	
9. AVK	9	
10. Dr.Web, VBA32	49	many FP's

Products which have many FP's (false positives) can not gain level award they would fall in, and will only receive the STANDARD award, as users can not rely on a heuristic that causes too many false alarms.

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



[5] 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 already fixed. False alarms caused by unencrypted data blocks in Anti-Virus related files are not counted in this test. If a product caused severel false alarms in the same package, it is counted here as only 1 false alarm. Please read also the comments under the tables to know what is meant with “heuristic” and “signature” – usually it simply means the false alarm occurred with heuristics turned off and due that it was counted as signature.

Avast

False alarm found in some part(s) of	Detected as	By
Actual Shut Down package	Win32:Delf-YQ [Trj]	Signature (Standard)
DaviDeo package	Flood-B [Wrm]	Signature (QuickScan)
Outlook Express Database Manager package	Win32:Trojan-gen {Other}	Signature (QuickScan)
TrendMicro ScanMail package	Win32:Small-WE [Trj]	Signature (QuickScan)
Ultimate Windows Boot CD package	VBS:Davinia	Signature (Thorough)

In parenthesis the scan mode in which the false alarms occur.

AVG

False alarm found in some part(s) of	Detected as	By
Kindersicherung package	Trojan Horse Dropper.Agent.BBF	Signature

AVG had only one false alarm.

AntiVir (AVIRA)

False alarm found in some part(s) of	Detected as	By
BersIRC package	HEUR/Backdoor.IRCBot	Heuristic (L)
PreShell package	PCK/Expressor	Signature
Search and Replace package	HEUR/Crypted.DNFLR	Heuristic (H)
Skype package	HEUR/Trojan.Downloader	Heuristic (L)
XPE Plugin package	HEUR/Hijacker	Heuristic (H)

AVIRA had this time only 5 false alarms. (L) means heuristics set to low, (H) means heuristics set to high.

BitDefender

False alarm found in some part(s) of	Detected as	By
aReakerWater package	Win32.Worm.Franvir.A	Signature
Google DesktopSearch package	Trojan.Dloader.NY	Signature
Net Control package	Generic.Malware.SLg.EAEAF616	Signature
Portable OpenOffice package	Trojan.Zlob.Gen	Signature

All the false alarms occurred also with heuristic turned off.

Norman

False alarm found in some part(s) of	Detected as	By
7-Zip package	Trojan Adclicker.FJ	Signature
Runwithparameters package	Trojan W32/Suspicious_U.gen	Signature
XPY package	Trojan W32/Suspicious_U.gen	Signature

Norman had few false positives in our test.

NOD32 (ESET)

False alarm found in some part(s) of	Detected as	By
JSSplit package	probably unknown NewHeur_PE virus	Heuristic (AH)
Marusoft Plugin for Excel package	probably unknown MACRO virus	Heuristic
NetIntelligence package	probably unknown NewHeur_PE virus	Heuristic (AH)
OutlookHelpDesk package	probably unknown NewHeur_PE virus	Heuristic (AH)
PlacemarkManager package	probably unknown NewHeur_PE virus	Heuristic (AH)

The false alarms marked with (AH) occur only if NOD32’s Advanced Heuristic is turned on.

F-Prot

False alarm found in some parts of	Detected as	By
BersIRC package	W32/IRCBot-based!Maximus	Signature
Datawest Support package	W32/Vimover.A (exact)	Signature
Geexbox package	archive bomb	Heuristic
Hauppage WinTV Driver package	W32/VB-EMU:VB-Dropper-based!Maximus	Signature
Internet Sammler package	W32/Threat-SysAdderSml-based!Maximus	Signature
PC Analyser package	W32/Rootkit-Backdoor-based!Maximus	Signature
Safe2Bid package	W32/VB-EMU:VB-Backdoor-HRS-based!Maximus	Signature
TrafficMonitor package	W32/SecRisk-ProcessPatcher-based!Maximus	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.

Kaspersky

False alarm found in some parts of	Detected as	By
Audio Maestro package	Trojan-Spy.Win32.KeyLogger.jb	Signature
Autographics package	Type_Win32 (modification)	Signature
Datawest Support package	Email-Worm.Win32.Vimover (modification)	Signature
Datei CommanderLE package	Trojan-Spy.Win32.KeyLogger.jb	Signature
EraserPro package	Trojan.Win32.Pakes	Signature
TransMac package	Backdoor.Win32.Agobot.afz	Signature

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

McAfee

False alarm found in some part(s) of	Detected as	By
Webzip package	BackDoor-AWQ.b	Signature

McAfee had only one false alarm.

Symantec (NAV)

Symantec Norton Anti-Virus was again 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.

F-Secure

False alarm found in some part(s) of	Detected as	By
Audio Maestro package	Trojan-Spy.Win32.KeyLogger.jb	Signature
Autographics package	Type_Win32	Signature
Datawest Support package	Email-Worm.Win32.Vimover	Signature
Datei CommanderLE package	Trojan-Spy.Win32.KeyLogger.jb	Signature
EraserPro package	Trojan.Win32.Pakes	Signature
TransMac package	Backdoor.Win32.Agobot.afz	Signature

In F-Secure it is not possible to turn off the heuristics.

TrustPort

False alarm found in some part(s) of	Detected as	By
7-Zip package	Trojan Adclicker.FJ	Signature
aReakerWater package	Win32.Worm.Franvir.A	Signature
Google DesktopSearch package	Trojan.Dloader.NY	Signature
Net Control package	Generic.Malware.SLg.EAEAF616	Signature
Portable OpenOffice package	Trojan.Zlob.Gen	Signature
Runwithparameters package	Trojan W32/Suspicious_U.gen	Signature
XPY package	Trojan W32/Suspicious_U.gen	Signature

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

G DATA AVK (2006)

False alarm found in some parts of	Detected as	By
aReakerWater package	Win32.Worm.Franvir.A	Signature
Audio Maestro package	Trojan-Spy.Win32.KeyLogger.jb	Signature
Autographics package	Type_Win32	Heuristic
Datei CommanderLE package	Trojan-Spy.Win32.KeyLogger.jb	Signature
EraserPro package	Trojan.Win32.Pakes	Signature
Google DesktopSearch package	Trojan.Dloader.NY	Signature
Net Control package	Generic.Malware.SLg.EAEAF616	Signature
Portable OpenOffice package	Trojan.Zlob.Gen	Signature
TransMac package	Backdoor.Win32.Agobot.afz	Signature

If the heuristic in AVK is turned off, the false alarm caused by the heuristic will not occur. Please note that new AVK 2007 uses now the Kaspersky engine and the Avast engine (instead of the Kaspersky engine and BitDefender engine).

Dr.Web

False alarm found in some part(s) of	Detected as	By
AccessServer package	modification of BackDoor.Generic.1261	Signature
AdvStringGrid package	modification of Win32.Swaduk.6891	Signature
AntiVir update package	probably infected with WIN.WORM.Virus	Heuristic
AOL Toolbar package	probably infected with BACKDOOR.Trojan	Heuristic
Arcor OnlineButler package	probably infected with BACKDOOR.Trojan	Heuristic
ASAP Utilities package	W97M.Iseng	Signature
CDN WinTool package	probably infected with BACKDOOR.Trojan	Heuristic
ChipChap package	probably infected with DLOADER.Trojan	Heuristic
Conpresso package	probably infected with SCRIPT.Virus	Heuristic
CS FireMonitor package	probably infected with BACKDOOR.Trojan	Heuristic

DateiCommander package	probably infected with BACKDOOR.Trojan	Heuristic
DigitalPatrol package	probably infected with BACKDOOR.Trojan	Heuristic
DIManager package	probably infected with DLOADER.Trojan	Heuristic
Ebay package	probably infected with BACKDOOR.Trojan	Heuristic
FavoriteStartpage package	probably infected with SCRIPT.Virus	Heuristic
FixFoto package	probably infected with SCRIPT.Virus	Heuristic
GPU package	probably infected with DLOADER.Trojan	Heuristic
IEPopStop package	probably infected with BACKDOOR.Trojan	Heuristic
Image Page Wizard package	Tool.GabanBus.20	Signature
InstantCopy package	probably infected with DLOADER.Trojan	Heuristic
KidKey package	probably infected with BACKDOOR.Trojan	Heuristic
Kindersicherung 2002 package	probably infected with BACKDOOR.Trojan	Heuristic
Kindersicherung 2006 package	Trojan.Watchdog	Signature
Mail2View package	probably infected with BACKDOOR.Trojan	Heuristic
MailBag package	probably infected w WIN.PWS.WORM.Virus	Heuristic
Microsoft Netmeeting package	modification of Win32.Bumblebee.3649	Signature
MiniMail package	Trojan.PWS.Bancos.142	Signature
MS PowerPoint 2002 Producer package	probably infected with SCRIPT.Virus	Heuristic
NetIntelligence package	probably infected with WIN.WORM.Virus	Heuristic
NeXX Pro package	probably infected with DLOADER.Trojan	Heuristic
Outlook Express Database Manager package	Trojan.CuteSpy	Signature
OutlookTools package	probably infected with WIN.WORM.Virus	Heuristic
PDF Experte package	probably infected with BACKDOOR.Trojan	Heuristic
PDF Machine package	probably infected with BACKDOOR.Trojan	Heuristic
Pit's WinToys package	probably WIN.SCRIPT.BATCH.Virus	Heuristic
PowerTuningXP package	modification of BackDoor.Generic.957	Signature
PrestoDVD package	probably infected with DLOADER.Trojan	Heuristic
Registry System Wizard package	probably infected w SCRIPT.BATCH.Virus	Heuristic
RemoteKeys package	probably infected with BACKDOOR.Trojan	Heuristic
Sudoku package	Trojan.MulDrop.3404	Signature
Sygate Personal Firewall package	probably infected with BACKDOOR.Trojan	Heuristic
TaskMatePro package	probably infected with BACKDOOR.Trojan	Heuristic
TrendMicro OfficeScan package	probably infected with BACKDOOR.Trojan	Heuristic
Windows Washer package	probably infected with DLOADER.Trojan	Heuristic
WinExpander package	probably infected with WIN.WORM.Virus	Heuristic
WinGuruXP package	probably infected with BACKDOOR.Trojan	Heuristic
WinTuningKit package	probably infected with DLOADER.Trojan	Heuristic
XP RegTune package	probably infected with 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 many false positives, so it gets penalized and gets only the STANDARD award, as users can not rely on a heuristic that causes too many false alarms.

VBA32

False alarm found in some parts of	**Detected as**	**By**
Aquasoft Photoalbum package	suspected of Trojan.Delf.51	Heuristic (E)
BitDefender Professional package	suspected of Unknown.OvrVirus	Heuristic (M)
CDBurnerXP package	suspected of Email-Flooder.VB.3	Heuristic (E)
ConcordF package	suspected of I-Worm.Psw-protected	Heuristic (O)
Corel Linux package	suspected of Unknown.OvrVirus	Heuristic (M)
DebuggingTools package	Trojan.VBS.Ultra#6	Signature

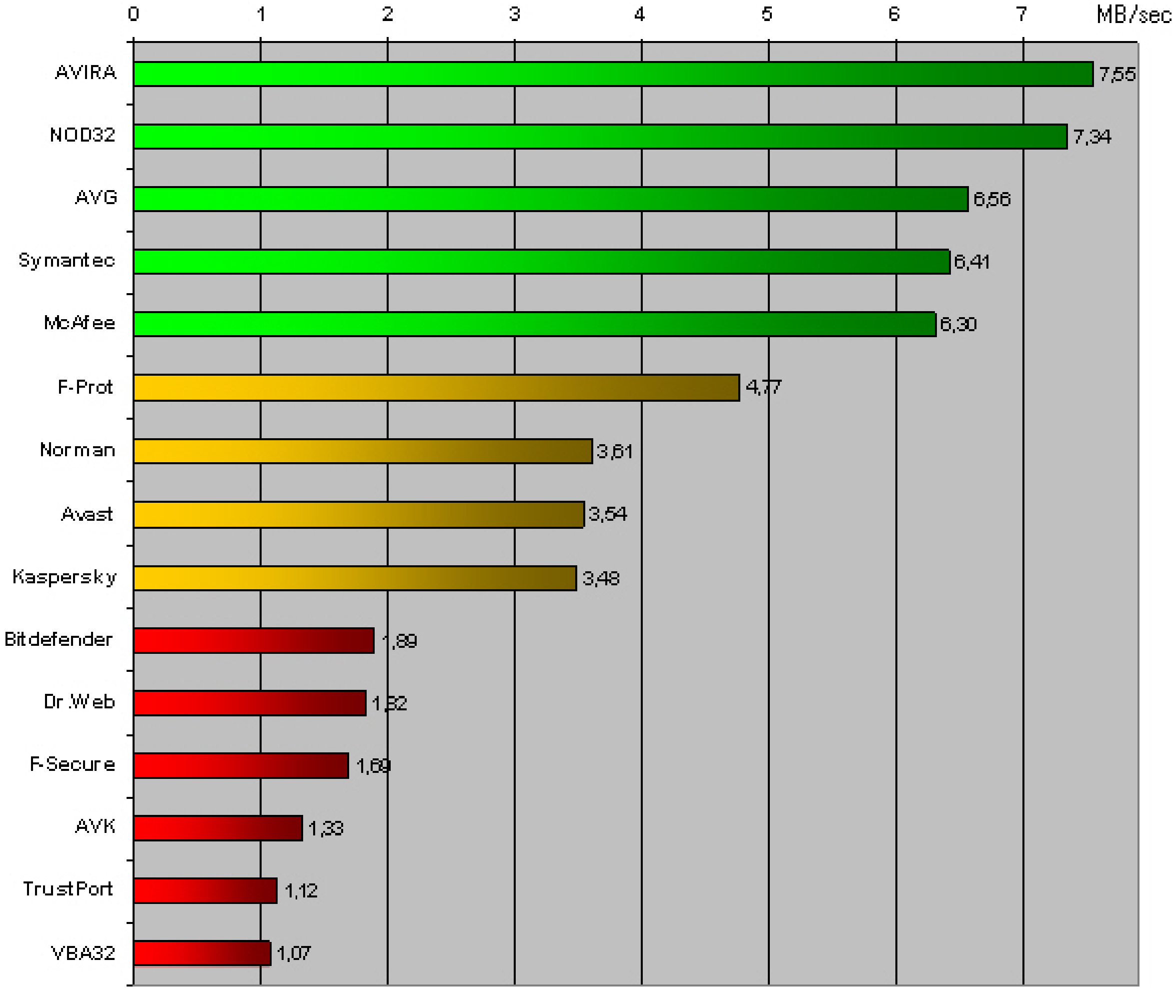
eGames package	Dialer.EMSAT#1	Signature
F-Secure Antivirus package	Trojan.SecretCrush	Signature (T)
Fedora package	suspected of Unknown.OvrVirus	Heuristic (M)
FileLabel package	suspected of Unknown.OvrVirus	Heuristic (M)
FlashGot extension for Firefox package	Virus.BAT.CopyToAll.l#6	Signature
Intel Pro Driver package	Trojan.VBS.Ultra#6	Signature (T)
IPAddress package	suspected of Malware.Delf.14	Heuristic (O)
IPCop package	suspected of Unknown.OvrVirus	Heuristic (M)
JustZIPit package	suspected of Trojan-Spy.Delf.43	Heuristic (O)
Jyve package	suspected of Trojan-PSW.Delf.45	Heuristic (O)
Kaspersky Internet Security package	Trojan.VBS.Ultra#6	Signature (T)
Kindersicherung 2003 package	Trojan.MulDrop.1161	Signature
MobileMaster package	suspected of Trojan-PSW.Lmir.3	Heuristic (E)
MS Office2003 SP2 package	A97M.MiPirat#12	Signature (T)
MS Windows 2000 package	suspected of Unknown.OvrVirus	Heuristic (M)
MS Windows 2000 SP3 package	Trojan.Win32.Dialer.oi	Signature
MS Windows XP package	suspected of Unknown.OvrVirus	Heuristic (M)
MS Windows XP SP1 package	suspected of Unknown.OvrVirus	Heuristic (M)
MS Windows XP SP2 package	suspected of Unknown.OvrVirus	Heuristic (M)
NetMail package	suspected of Backdoor.Hupigon.40	Heuristic (E)
OpenOffice package	suspected of Unknown.OvrVirus	Heuristic (M)
OutlookExpress DatabaseConverter package	Trojan.CuteSpy	Signature
PacSpam package	suspected of Malware.VB.28	Heuristic (O)
PEBuilder package	suspected of Trojan-Spy.Delf.43	Heuristic (O)
PhoCalc package	Trojan-Proxy.Win32.RedBind.a	Signature
PhotoSuite package	suspected of Trojan.Delf.51	Heuristic (O)
Pictures package	suspected of Unknown.OvrVirus	Heuristic (M)
Plugins for Excel package	suspected of Unknown.MacroVirus	Heuristic (M)
PVAStrumento package	suspected of Unknown.OvrVirus	Heuristic (M)
Qemu Manager package	suspected of Malware.Delf.76	Heuristic (E)
RegistryScanner package	Backdoor.Win32.Agent.xn	Signature
ScreenshotCaptor package	suspected of Trojan.Delf.51	Heuristic (E)
ShareComputerToolkit package	Trojan.VBS.StartPage.e#12	Heuristic (M)
SpamKiller package	suspected of Trojan-PSW.Agent.12	Heuristic (O)
Special Cell Finder Plus package	suspected of Unknown.MacroVirus	Heuristic (M)
T-Mobile CommunicationCenter package	suspected of Trojan.Agent.55	Heuristic (E)
TrendMicro package	Trojan.Tsup	Signature
Ultimate Windows Boot CD package	suspected of Trojan-Downloader.Agent.75	Heuristic (O)
Vallen JPegger package	suspected of Downloader.Harnig.5	Heuristic (E)
Vallen Zipper package	suspected of Downloader.Harnig.5	Heuristic (E)
VersionBackup package	suspected of Downloader.Small.170	Heuristic (E)
WebArt package	suspected of Unknown.OvrVirus	Heuristic (M)
WinUPACK compression tool package	Net-Worm.Win32.Mytob.bt	Signature

Various scan modes in which the false alarms occurred: (T) Thorough; (O) Optimal; (M) Maximum; (E) Excessive.
VBA32 had many false positives (including on some quite well known applications), so it gets penalized and gets only the STANDARD award, as users can not rely on a heuristic that causes too many false alarms.

6. Scanning speed test

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[6] and the settings in the product[7].



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.

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

[7] we used the best possible detection settings

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+ ★★★ Nov 06 proactive/retrospective test	**AVK 2006** **AVIRA** **BitDefender** **NOD32** **TrustPort**
AV comparatives ADVANCED ★★ Nov 06 proactive/retrospective test	**Norman**
AV comparatives STANDARD ★ Nov 06 proactive/retrospective test	**Avast** **Dr.Web*** **F-Prot** **F-Secure** **Kaspersky** **McAfee** **Symantec** **VBA32***
no certification	**AVG**

** : Products with a very high rate of false alarms do not deserve the proactive detection level they would fall in. They get penalized and receive only the STANDARD award (i.e. Dr.Web, VBA32), as users can not rely on a heuristic that causes too many false alarms.*

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 (November 2006)