Anti-Virus Comparative No.14

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

contains also
False positive test
&
Scanning speed test

Date: May 2007 (2007-05)

Last revision: 1st June 2007

Author: Andreas Clementi

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

1. Introduction

This test report is the second part of the February 2007 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 this tests. For this test we used new samples[1] received between 2nd February and 2nd May 2007, which were all new to any tested product. The following 17 products were tested in this comparative (last signature updates and versions are from 2nd February 2007):

- 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

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

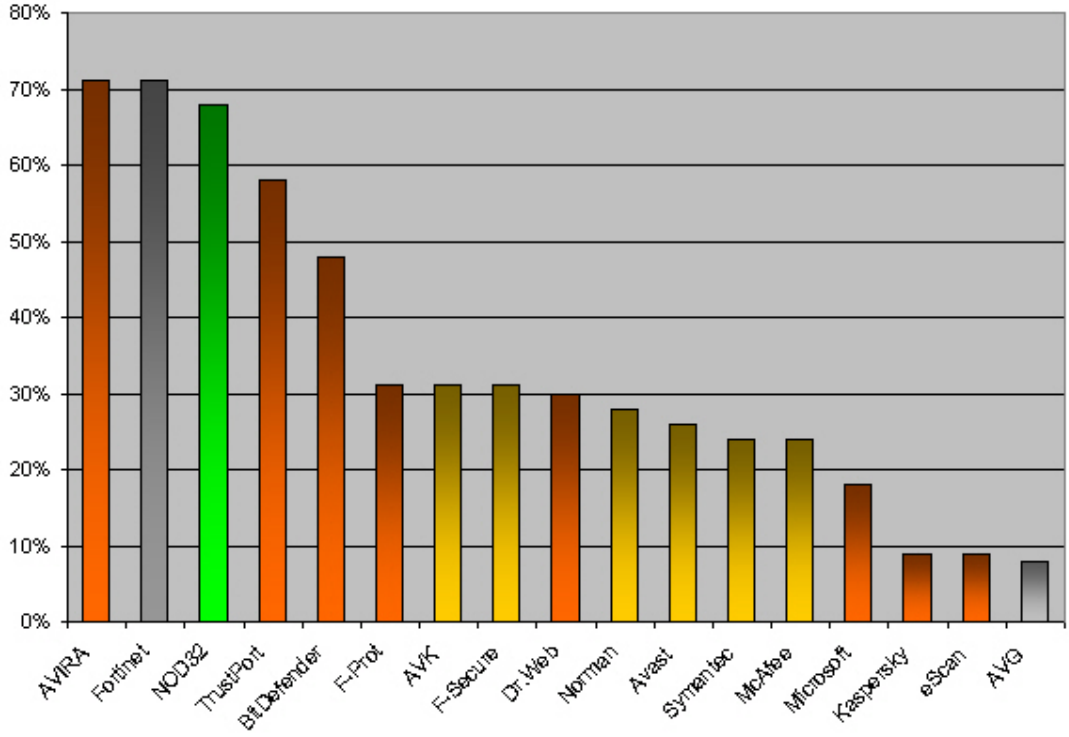
Below the detailed test result tables of all tested products:

Company		AVIRA		G DATA Security		Alwil Software		GriSoft	
Product		**AntiVir PE Premium**		**AntiVirusKit (AVK)**		**Avast! Professional**		**AVG 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*	
Certification level reached*		**STANDARD**		**ADVANCED**		**ADVANCED**			
Number of false positives*		*many*		*few*		*few*		*many*	
On-demand scanning speed*		*fast*		*slow*		*average*		*slow*	
ProActive detection of "NEW" samples**									
Windows viruses	255	162	64%	102	40%	84	33%	0	0%
Script malware	80	17	21%	6	8%	0	0%	0	0%
Worms	4.075	992	24%	295	7%	291	7%	0	0%
Backdoors	3.873	3.361	87%	2.876	74%	2.029	52%	878	23%
Trojans	11.966	9.967	83%	3.097	26%	2.990	25%	697	6%
other malware	260	129	50%	40	15%	39	15%	2	1%
OtherOS malware	13	0	0%	0	0%	0	0%	0	0%
TOTAL	**20.522**	14.628	**71%**	6.416	**31%**	5.433	**26%**	1.577	**8%**

Company		Softwin		Doctor Web		Fortinet		Frisk Software	
Product		**BitDefender Prof.+**		**Dr. Web**		**FortiClient**		**F-Prot Anti-Virus**	
Program version		10		4.33.5.10110		3.0.308		6.0.5.1	
Engine / signature version		7.11190		4.33.2.10060		2.86 / 7.111		4.3.1	
Number of virus records		*453.630*		*173.398*		*unknown*		*491.050*	
Certification level reached*		**STANDARD**		**STANDARD**				**STANDARD**	
Number of false positives*		*many*		*many*		*very many*		*many*	
On-demand scanning speed*		*slow*		*slow*		*fast*		*average*	
ProActive detection of "NEW" samples**									
Windows viruses	255	129	51%	40	16%	206	81%	104	41%
Script malware	80	7	9%	16	20%	0	0%	0	0%
Worms	4.075	401	10%	150	4%	3.478	85%	672	16%
Backdoors	3.873	2.492	64%	2.313	60%	2.715	70%	1.577	41%
Trojans	11.966	6.786	57%	3.610	30%	8.063	67%	3.868	32%
other malware	260	46	18%	28	11%	126	48%	81	31%
OtherOS malware	13	0	0%	0	0%	0	0%	0	0%
TOTAL	**20.522**	9.861	**48%**	6.157	**30%**	14.588	**71%**	6.302	**31%**

Company		F-Secure		Kaspersky Labs		McAfee		Microsoft	
Product		**F-Secure Anti-Virus**		**Kaspersky AV**		**McAfee VirusScan**		**Microsoft OneCare**	
Program version		7.01.128		6.0.2.614		11.1.124		1.5.1890.18	
Engine / signature version		7.00.12371		*N/A*		5100.0194 / 4955		1.15.2227.7	
Number of virus records		*unknown*		*264.410*		*225.413*		367.307	
Certification level reached*		**ADVANCED**		**STANDARD**		**ADVANCED**		**STANDARD**	
Number of false positives*		*very few*		*very few*		*few*		*very few*	
On-demand scanning speed*		*slow*		*average*		*fast*		*fast*	
ProActive detection of "NEW" samples**									
Windows viruses	255	66	26%	56	22%	132	52%	67	26%
Script malware	80	30	38%	6	8%	14	18%	1	1%
Worms	4.075	195	5%	16	0%	357	9%	253	6%
Backdoors	3.873	2.003	52%	1.356	35%	1.796	46%	1.375	36%
Trojans	11.966	4.011	34%	345	3%	2.616	22%	1.898	16%
other malware	260	20	8%	3	1%	60	23%	50	19%
OtherOS malware	13	0	0%	0	0%	0	0%	0	0%
TOTAL	**20.522**	6.325	**31%**	1.782	**9%**	4.975	**24%**	3.644	**18%**

Company		MicroWorld		ESET		Norman ASA		Symantec		AEC	
Product		**eScan Anti-Virus**		**NOD32 Anti-Virus**		**NormanVirusControl**		**Norton Anti-Virus**		**TrustPort AV WS**	
Program version		8.0.671.1		2.70.23		5.82		14.0.0.89		2.5.0.957	
Engine / signature version		*N/A*		2.031		5.90.30		90202ai		*N/A*	
Number of virus records		*unknown*		*unknown*		*654.451*		*73.132*		*unknown*	
Certification level reached[1]		**STANDARD**		**ADVANCED+**		**ADVANCED**		**ADVANCED**		**STANDARD**	
Number of false positives*		*very few*		*very few*		*few*		*none*		*many*	
On-demand scanning speed*		*average*		*fast*		*average*		*fast*		*slow*	
ProActive detection of "NEW" samples[2]											
Windows viruses	255	56	22%	134	53%	45	18%	71	28%	136	53%
Script malware	80	6	8%	6	8%	27	34%	4	5%	28	35%
Worms	4.075	16	0%	2.687	66%	193	5%	234	6%	498	12%
Backdoors	3.873	1.356	35%	2.884	74%	1.380	36%	3.160	82%	2.755	71%
Trojans	11.966	345	3%	8.210	69%	3.996	33%	1.432	12%	8.486	71%
other malware	260	3	1%	117	45%	18	7%	82	32%	57	22%
OtherOS malware	13	0	0%	0	0%	0	0%	0	0%	0	0%
TOTAL	**20.522**	1.782	**9%**	14.038	**68%**	5.659	**28%**	4.983	**24%**	11.960	**58%**



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 2007 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.	AVIRA	84%
2.	NOD32, TrustPort	70%
3.	Fortinet	68%
4.	BitDefender	58%
5.	Dr.Web, AVK, F-Secure	37%
6.	Norman, F-Prot	34%
7.	Avast	31%
8.	Symantec	29%
9.	McAfee	28%
10.	Microsoft	21%
11.	eScan, Kaspersky	11%
12.	AVG	10%

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

1.	Fortinet	84%
2.	NOD32	64%
3.	AVIRA	27%
4.	F-Prot	18%
5.	TrustPort	15%
6.	BitDefender	12%
7.	McAfee	11%
8.	Avast, AVK	9%
9.	Microsoft, Symantec, F-Secure	7%
10.	Norman	6%
11.	Dr.Web	5%
12.	eScan, Kaspersky	2%
13.	AVG	0%

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

1.	AVIRA, Fortinet	71%
2.	NOD32	68%
3.	TrustPort	58%
4.	BitDefender	48%
5.	F-Prot, AVK, F-Secure	31%
6.	Dr.Web	30%
7.	Norman	28%
8.	Avast	26%
9.	Symantec, McAfee	24%
10.	Microsoft	18%
11.	Kaspersky, eScan	9%
12.	AVG	8%

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, eScan, F-Secure and TrustPort are multi-engine AV's.

5. False positive/alarm test

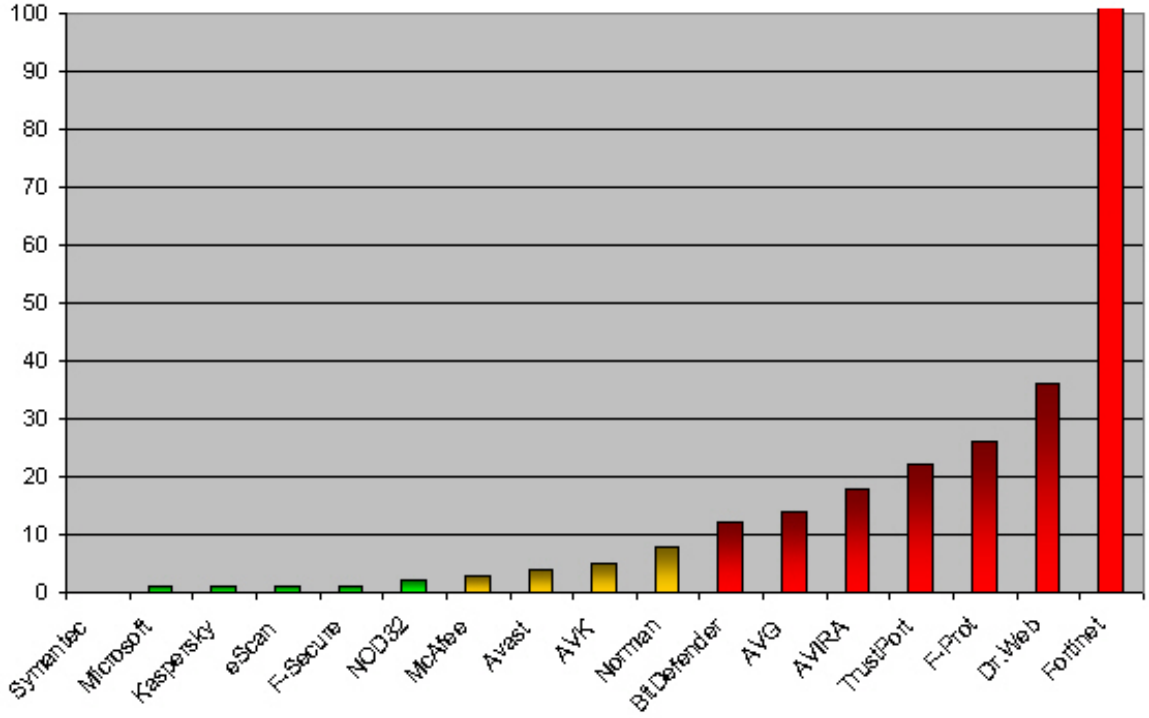
We provide in our retrospective test reports also a false alarm test, in order to better evaluate the quality of the proactive detection capabilities. This test also demonstrates that also with deactivated heuristics false alarms can occur.
A false alarm (false positive) is when an Anti-Virus product 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[3]:

1.	Symantec	0	none or very few FP's
2.	Microsoft, Kaspersky, eScan, F-Secure	1	
3.	NOD32	2	
4.	McAfee	3	few FP's
5.	Avast	4	
6.	AVK	5	
7.	Norman	8	
8.	BitDefender	12	many FP's
9.	AVG	14	
10.	AVIRA	18	
11.	TrustPort	22	
12.	F-Prot	26	
13.	Dr.Web	36	
14.	Fortinet	>1000+	very many FP's

Products which have many FP's (false positives) can not gain the 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. Fortinet does not even deserve the STANDARD award due its very high number of false positives.

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 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.

Avast

False alarm found in some part(s) of	Detected as
Cubase package	Win32:Trojan-gen. {Other}
PDF Converter package	Win32:Trojan-gen. {VC}
StegHide package	Win32:Iroffer-055 [Trj]
TransMac package	Win32:Trojan-gen. {VC}

AVG

False alarm found in some part(s) of	Detected as
1Net4You package	Heuristic.Win32.Dialer
0190Warner package	Heuristic.Win32.Dialer
BIOS Kompendium package	Logger.Ransom.a
Cubase package	IRC/Backdoor.SdBot.183.BE
Datawest Support package	I-Worm/VB.NC
DrWeb package	Trojan.QQShou.gq
Hide In Picture package	Downloader.Adload.do
Kindersicherung package	Dropper.Agent.BBF
MB-Ruler package	Backdoor.Delf.eg
Outlook Express DB Converter package	Trojan.CuteSpy
SenseConnect package	Heuristic.Win32.Dialer
TiscaliProtect package	Heuristic.Win32.Dialer
Topologilinux package	Linux/Brundle.a
USB-Tray package	Heuristic.Win32.Dialer

Norman

False alarm found in some part(s) of	Detected as
3D Screensaver package	Agent.AQJM
Bathc2Exe Converter package	W32/Zacryxof.A.dropper
Cubase package	W32/SDBot.ABGE
IntelliHyperSpeed package	Agent.AQJN
iPod eBookMaker package	QQRob.UV
JAP package	W32/Hupigon.RPZ
Miranda package	Zlob.UFS
MS WindowsXP Patch package	W32/Malware

Microsoft

False alarm found in some part(s) of	Detected as
Reatogo package	TrojanDropper:Win32/Small.G

F-Secure

False alarm found in some part(s) of	Detected as
Bitdefender package	Monitor.Win32.PCAcme.61

AntiVir (AVIRA)

False alarm found in some part(s) of	Detected as
Advanced Process Termination package	HEUR/Crypted
Cubase package	WORM/SdBot.3478016
eBay Starter Kit package	HEUR/Exploit.HTML
Hauppage package	DR/VirtualBouncer.R.3
IPCop package	HEUR/Exploit.HTML
IViewPCW package	HEUR/Exploit.HTML
Kleptomania package	HEUR/Malware
MP3TAG package	HEUR/Exploit.HTML
Norton Ghost package	HEUR/Malware
NVHardPage package	HEUR/Malware
PrestoDVD package	HEUR/Exploit.HTML
Search & Replace package	HEUR/Crypted
Simple File Shredder package	HEUR/Malware
SQLiteJournal package	PHISH/EbayFraud.CS
SystemVirginityVerifier package	SPR/RootKit.G program
TIFLoesch package	HEUR/Exploit.HTML
USB Mouserate Switcher package	HEUR/Crypted
VS2000GUI package	HEUR/Malware

BitDefender

False alarm found in some part(s) of	Detected as
Audio Maestro package	Trojan.Spy.Keylogger.JB
Batch2Exe Converter package	Dropped:Trojan.Zacryxof.A
Cubase package	Win32.Worm.Sdbot.CS
Datawest Support package	Win32.Vimover.B@mm
Datei Commander package	Trojan.Spy.Keylogger.JB
eScan package	BehavesLike:Win32.FileInfector
Outlook package	Trojan.Cutespy.E
RocketLife package	BehavesLike:Trojan.Downloader
ShipSimulator package	BehavesLike:Win32.FileInfector
TippGenerator package	Generic.Malware.dld!!.F623A0BA
USB Drive package	Dialer.1000.I
WormRadar package	Generic.XPL.IIS.0D4AAD53

NOD32 (ESET)

False alarm found in some part(s) of	Detected as
AOL2POP3 package	probably unknown NewHeur_PE virus [7]
EMIS package	probably unknown NewHeur_PE virus [7]

Symantec (NAV)

Symantec Norton Anti-Virus was again (for the third time) 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.

Kaspersky

False alarm found in some part(s) of	Detected as
Bitdefender package	Monitor.Win32.PCAcme.61

McAfee

False alarm found in some part(s) of	Detected as
Kaspersky Anti-Virus package	Generic.du
Miranda package	Puper.dr
ProtectEXE package	MultiDropper-JN

F-Prot

False alarm found in some part(s) of	Detected as
Airsnare package	{no name}
Babyflash package	W32/Backdoor.VYJ (exact)
CidSaver package	W32/new_malware!Maximus
Datawest Support package	{no name}
EMS Manager package	{no name}
FireTune package	{no name}
F-Secure AV package	{no name}
GameXP package	{no name}
IntelliHyperSpeed package	{no name}
Kaspersky AV package	{no name}
Kazaa package	{no name}
Leserbefragung package	{no name}
Miranda package	{no name}
MS Windows ME package	{no name}
MusicMatch package	{no name}
NeroDigital package	{no name}
PDF Annotator package	{no name}
PE Builder package	{no name}
Powerstrip package	{no name}
Proactive Security Auditor package	{no name}
QuickTime package	{no name}
Recorder package	{no name}
SafeXP package	{no name}
Schwarzbuch package	{no name}
SpywareFighter package	{no name}
WinRAR package	{no name}

G DATA AVK 2007

False alarm found in some part(s) of	Detected as
Bitdefender package	Monitor.Win32.PCAcme.61
Cubase package	Win32:Trojan-gen. {Other}
PDF Converter package	Win32:Trojan-gen. {VC}
StegHide package	Win32:Iroffer-055 [Trj]
TransMac package	Win32:Trojan-gen. {VC}

TrustPort

False alarm found in some part(s) of	Detected as
3D Screensaver package	Agent.AQJM
Audio Maestro package	Trojan.Spy.Keylogger.JB
Batch2Exe Converter package	Dropped:Trojan.Zacryxof.A
BIOS Kompendium package	Logger.Ransom.a
Cubase package	IRC/BackDoor.SdBot.183.BA
Datawest Support package	I-Worm/VB.NC
Datei Commander package	Trojan.Spy.Keylogger.JB
eScan package	BehavesLike:Win32.FileInfector

Hide In Picture package	Downloader.Adload.do
IntelliHyperSpeed package	Agent.AQJN
iPod eBookMaker package	QQRob.UV
JAP package	W32/Hupigon.RPZ
Kindersicherung package	Dropper.Agent.BBF
MB-Ruler package	Backdoor.Delf.ag
Miranda package	Zlob.UFS
MS WindowsXP Patch package	W32/Malware
Outlook package	Trojan.Cutespy
RocketLife package	BehavesLike:Trojan.Downloader
ShipSimulator package	BehavesLike:Win32.FileInfector
TippGenerator package	Generic.Malware.dld!!.F623A0BA
Topologilinux package	Linux/Brundle.A
WormRadar package	Generic.XPL.IIS.0D4AAD53

Dr.Web

False alarm found in some part(s) of	**Detected as**
2020 package	BACKDOOR.Trojan
ADVGrid package	W32.Swaduk.6891
ASAP Utilities package	W97M.Iseng
AuktionBE package	BACKDOOR.Trojan
Auktionskalender package	BACKDOOR.Trojan
Bitdefender package	DLOADER.Trojan
CookeCooker package	DLOADER.Trojan
DiManager package	DLOADER.Trojan
eScan package	WIN.WORM.Virus
FireMonitor package	Virus
FixFoto package	SCRIPT.Virus
FreeDos package	BATCH.Virus
GoldMine package	DLOADER.Trojan
GPU package	DLOADER.Trojan
HDDVDJump package	Win32.HLLW.Dbot
InstantCopy package	DLOADER.Trojan
Kaspersky package	BINARYRES
Kindersicherung package	BACKDOOR.Trojan
LANTool package	Trojan.DownLoader.10130
MBSWinExpander package	WIN.WORM.Virus
MS PowerPoint package	SCRIPT.Virus
NetIntelligence package	WIN.WORM.Virus
OutlookHelpDesk package	WIN.WORM.Virus
OutlookTools package	WORM.Virus
ParentsFriend package	BACKDOOR.Trojan
PC SecurityTest package	STPAGE.Trojan
PDF Machine package	BACKDOOR.Trojan
PowerTuningXP package	BackDoor.Generic.957
Registry Bearbeitung package	SCRIPT.BATCH.Virus
Registry System Wizard package	SCRIPT.BATCH.Virus
Samurize package	DLOADER.Trojan
Soviewim package	DLOADER.Trojan
Sygate package	BACKDOOR.Trojan
TrendMicro package	Trojan.DelSys.191
Wintuning Kit package	STPAGE.Trojan
YabeOffice package	BACKDOOR.Trojan

Fortinet

False alarm found in some part(s) of	Detected as
0190Warner package	Suspicious
12erSudoku package	Suspicious
1by1 package	Suspicious
1PASSWORD package	Suspicious
234-Gleiche package	Suspicious
3Com Driver package	Suspicious
3D FontTwister package	Suspicious
3D Mark package	Suspicious
3D UP15 package	PossibleThreat!06131
3DEigenheimplaner package	Suspicious
3D Muehle package	Suspicious
ACER RecoveryCD package	Suspicious
Acronis DiskDirector package	Suspicious
Acronis PartitionExpert package	Suspicious
Acronis TrueImage package	Suspicious
ActivAId package	Suspicious
Adobe Acrobat Reader package	JS/Feebs.A@mm
Adobe Photoshop package	Suspicious
Adorage package	Suspicious
AKarten package	Suspicious
Alarm für Cobra 11 package	Suspicious
alcohol120 package	Suspicious
alignit package	Suspicious
Allesšber package	Suspicious
AlligatorSQL package	Suspicious
AntiVirPEClassic7 package	Suspicious
anymate package	Suspicious
AOL Banking package	Suspicious
AOL9 package	Suspicious
APT package	Suspicious
AquaScreen package	Suspicious
Arbeitszeit package	Suspicious
Armobiles package	Suspicious
AstaroSecurityLinux6 package	Suspicious
ASUS A8V Driver package	Suspicious
ASUS DVD2000 package	Suspicious
ASUS V7700 Driver package	Suspicious
ASUS ViaChipset Driver package	Suspicious
ATI Catalyst Driver package	Suspicious
Auction Studio package	Suspicious
audacity package	Suspicious
Avast package	Suspicious
AVG package	Suspicious
Backvoll package	Suspicious
Batch2Exe_Converter package	Suspicious
Beacon package	Suspicious
Bietassistent package	Suspicious
Bitdefender package	Suspicious
BlueFish Media package	Suspicious
buchdruck package	Suspicious
Bulk Rename package	Suspicious
Call of Duty Patch package	Suspicious
Canon Printer Driver package	Suspicious

CDDVDBurning package	PossibleThreat!018918
CDex package	Suspicious
CDSearch package	Suspicious
CDStartUp package	Suspicious
ClipBoardManager package	Suspicious
CloneDVD2 package	Suspicious
CMOS Password package	PossibleThreat
ColorPilot package	Suspicious
Computec Media package	Suspicious
COMWIN package	Suspicious
ConWat package	Suspicious
cPicture package	Suspicious
CPU-Z package	Suspicious
CreateMovie package	Suspicious
Creative SB Driver package	Suspicious
Crystal Player package	Suspicious
DAEMON Tools package	Suspicious
DarkDesktop package	Suspicious
Datawest Support package	W32/Vimover@mm
DaViDeo package	Suspicious
DCOM98 package	Suspicious
Depotverwalter package	Suspicious
DIGICAMPRAXIS package	Suspicious
DirectX package	Suspicious
DNet Kit package	Suspicious
DriveSitter package	Suspicious
DrWeb CureIT package	Suspicious
Duden package	Suspicious
DVTool package	Suspicious
EMIS package	Spy/Bancos
eScan package	Suspicious
F-Secure AV package	Suspicious
F-Secure IS package	Suspicious
F.E.A.R package	Suspicious
Fallobst_Arcade package	Suspicious
FFDShow package	Suspicious
FileZilla package	Suspicious
Flash Player package	Suspicious
FlasKMPEG package	Suspicious
FLV Player package	Spy/Zlob
FotoMatchAll package	Suspicious
FreePhone package	Suspicious
FreeRAM package	Suspicious
FTCheck package	Suspicious
GDATA AVK package	Suspicious
GMER package	PossibleThreat!021393
Google package	PossibleThreat!02931
Gigabyte Driver package	Suspicious
Gothic 2 Add-on package	Suspicious
Haushaltsbuch package	Suspicious
HDiskDefrag package	Suspicious
Heimwerkerlexikon package	Suspicious
Heroglyph package	Suspicious
HiJackThis package	Suspicious
HP ScanJet Driver package	Suspicious

HyperCam package	Suspicious
IceSword package	Stealth!tr
Ice Age2 Drumkit package	Suspicious
Ice Storm Fighters package	Suspicious
IDA Pro package	Suspicious
Image Optimizer package	Suspicious
Jokemaker package	Suspicious
JustCause package	Suspicious
Kampf dem Terror package	Suspicious
Kaspersky AV package	Suspicious
Kaspersky IS package	Suspicious
Kassenbuch package	Suspicious
Kensington Driver package	Suspicious
Kugeln2D package	Suspicious
LottoFee package	Suspicious
MagicGames package	Suspicious
Matrox Driver package	Suspicious
MaxMixFoto package	Suspicious
McAfee Antispy package	Suspicious
McAfee Firewall package	Suspicious
McAfee Spamkiller package	Suspicious
MediaPlayerClassic package	Suspicious
Messenger package	Suspicious
Microsoft ActiveSync package	Suspicious
Microsoft Internet Explorer package	Suspicious
Money 2000 package	Suspicious
Mozilla Firefox package	Suspicious
Mozilla Thunderbird package	Suspicious
MS DigitalPersona Driver package	Suspicious
MS Links package	Suspicious
MS Windows 2000 Patches package	Suspicious
MS Windows 2000 SP2 package	Suspicious
MS Windows 95 package	Suspicious
MS Windows 98 package	Suspicious
MS Windows ME package	Suspicious
MS Windows NT4 Patches package	Suspicious
MS Windows XP Patches package	Suspicious
MS Windows XP package	PossibleThreat
MS BusinessContactManager package	Suspicious
MS Encarta 2001 EnzyklopädiePlus package	Suspicious
MS OfficeProfessional2001 package	Suspicious
MS OfficeXP package	Suspicious
MS Office Standard2003 package	Suspicious
MS ServicesCD2003 package	Suspicious
MS SicherheitsupdateCD2005 package	Suspicious
MS VirtualPC5 package	Suspicious
MS Windows2000 package	Suspicious
MS WindowsXP Pro SP1 package	Suspicious
MWTI AV package	Suspicious
Nero Burning Rom package	Suspicious
NewsBin package	PossibleThreat
NOD32 package	Suspicious
Norton Anti-Virus package	Suspicious
Norton Internet Security package	Suspicious
Norton Personal Firewall 2003 package	Suspicious

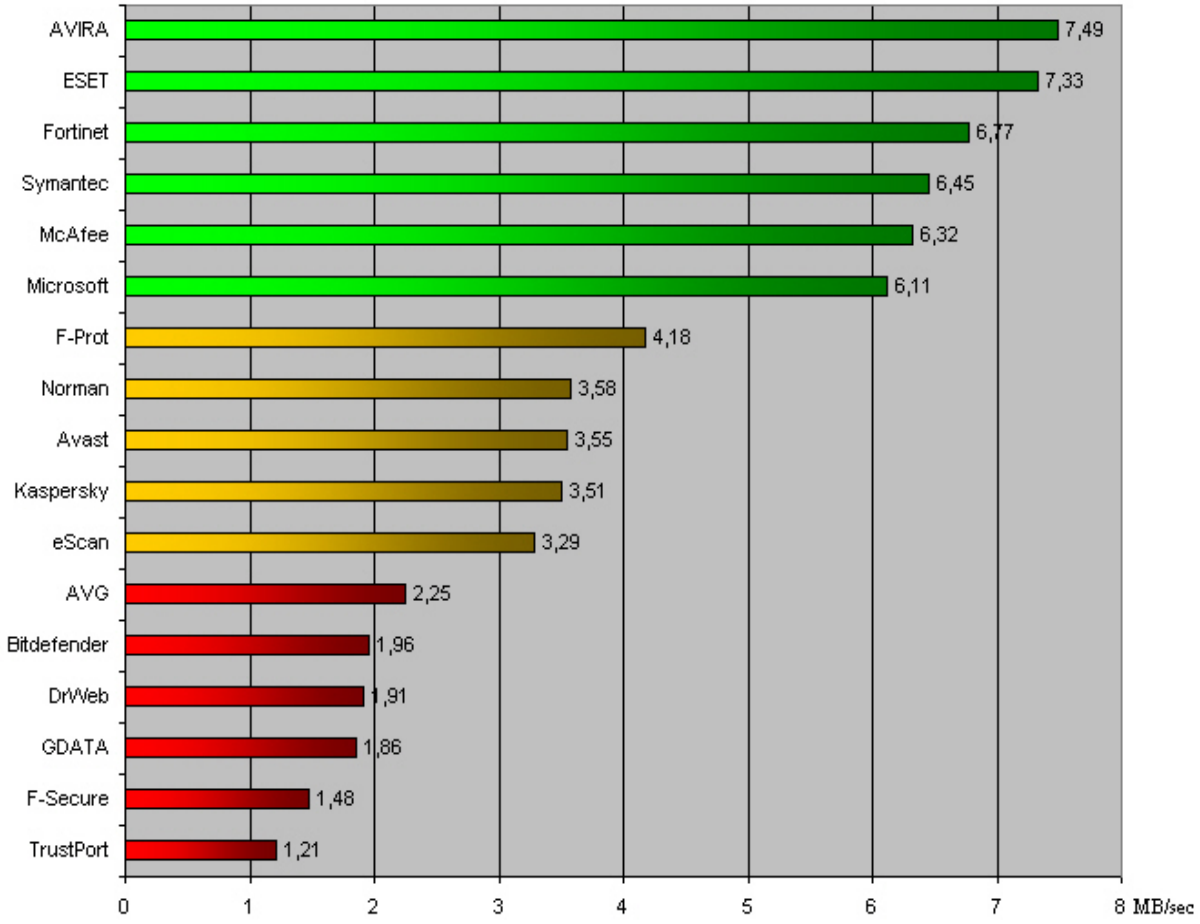
Norton System Works package	Suspicious
Norton Utilities 3 package	Suspicious
Notebook Hardware Control package	Suspicious
NVIDIA Driver package	Suspicious
O&O Defrag package	Suspicious
OilTycoon package	Suspicious
OmniPage package	Suspicious
OpenOffice package	Suspicious
OpenSourceGames 2 package	Suspicious
Opera package	Suspicious
Outpost Pro package	Suspicious
Paint Shop Pro package	Suspicious
PDF-Fotoalbum package	Suspicious
PDFCreator package	Suspicious
PE Builder package	Suspicious
PerfWatch package	Suspicious
Phoner package	Suspicious
PhotoFlash package	Suspicious
Picasa package	Suspicious
Planet-Interkom package	Suspicious
PodTools package	Suspicious
Poker package	Suspicious
Pop-Up Stopper package	Suspicious
Portable Apps package	W32/VB.AQS!tr.dldr
PortRoyaleGold package	Suspicious
PowerArchiver2000 package	Suspicious
PowerClick package	Suspicious
Profan package	Suspicious
Quake 4 Patch package	Suspicious
QuickDic package	Demo1.1698
QuickTime package	Suspicious
Quiztime package	Suspicious
QuoteFix package	Suspicious
Raetsel package	Suspicious
RAMster package	Suspicious
RegCool package	Suspicious
Registry Cleaner package	Suspicious
Rizzoli Larousse 2002 package	Suspicious
RootKit Revealer package	Suspicious
Roter Baron3 package	Suspicious
S.T.A.L.K.E.R. package	Suspicious
SAD-Vorlagen package	Suspicious
Samsung Driver package	Suspicious
Samurai package	Suspicious
Serious Sam Patch package	Suspicious
Sicherheitscheck-CD package	Suspicious
Simply Zip package	Suspicious
Sleepy package	Suspicious
SMS SUS package	Suspicious
Sophos Anti-Rootkit package	Suspicious
SpamPal package	SPY/LdPinch
SpeedCommander package	Suspicious
Spiegel Spezial package	Suspicious
Splinter Cell Patch package	Suspicious
SPSS10 package	Suspicious

Stinger package	Suspicious
Sygate package	Suspicious
Symantec Business package	Suspicious
T-Mobile Communication Center package	Suspicious
Telefonbuch Deutschland package	Suspicious
The Sims 2 University Patch package	Suspicious
ThrottleWatch package	Suspicious
Tischkicker package	Suspicious
Titan Quest Patch package	Suspicious
ToolBook II package	Suspicious
TrackWinstall package	Suspicious
Traktor Racer package	Suspicious
TransMac package	W32/AgoBot.AFZ!tr.bdr
TrendMicro CD package	Keylog/Quick
TrendMicro IS package	Suspicious
TrendMicro PC-cillin package	Suspicious
TruPrevent package	Suspicious
TuneUp Utilities package	Suspicious
TweakPower package	Suspicious
TweakXP Pro package	W32/Rbot.BRY!tr.bdr
UMRS package	Suspicious
UPACK compression tool package	Suspicious
VirtualCloneDrive package	Suspicious
VirtualDub package	Suspicious
Vokabel package	Suspicious
WaveRecorder package	Suspicious
WBloggar package	Suspicious
WinAAM package	Suspicious
WinAce package	Suspicious
WinAmp package	Suspicious
WinChecker package	Suspicious
WinDVD package	Suspicious
WinHintergrundManager package	Suspicious
WinRAR package	W32/Banload.AMS!tr.dldr
WinZip package	Suspicious
WISO MeinGeld package	Suspicious
WMS Weltreise package	Suspicious
XNote Stopwatch package	Suspicious
XP AntiSpy package	Suspicious
Xpage Internet Studio package	Suspicious
XPizeReloader package	Suspicious
ZoneAlarm package	Suspicious
ZoomPlayer package	Suspicious

Fortinet had thousands of false alarms in our set of clean files. For space reasons, we list here “only” about 250 false alarms.
Due this never seen before amount of false alarms caused by Fortinet heuristic, we decided together with Fortinet to disable the heuristic scanning from Fortinet in future tests until the false alarm rate drops to an acceptable level. Otherwise it will have to be excluded from future testings. Such a heuristic does not make sense in a home user product – AV-Comparatives recommends to Fortinet users to disable the heuristic scanning in FortiClient.

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[4] and the settings in the product[5].



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.

[4] to know how fast the various products would be on your PC at scanning *your* files, try yourself the products
[5] 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+ ★★★ May 07 proactive/retrospective test	**NOD32**
AV comparatives ADVANCED ★★ May 07 proactive/retrospective test	**AVK** **Avast** **F-Secure** **McAfee** **Norman** **Symantec**
AV comparatives STANDARD ★ May 07 proactive/retrospective test	**AVIRA*** **BitDefender*** **Dr.Web*** **eScan** **F-Prot*** **Kaspersky** **Microsoft** **TrustPort***
no certification	**AVG**** **Fortinet****

** : Products with a 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. AVIRA, BitDefender, Dr.Web, F-Prot, TrustPort), as users can not rely on a heuristic that causes too many false alarms.*
*** : In case of Fortinet, the false alarm rate is that high, that it does not even deserve the STANDARD level.*
In case of AVG, the proactive detection is low, while the rate of false alarms is high. Therefore it does not deserve the STANDARD rating.

We are going to make an additional test of Kaspersky Anti-Virus 7.0 (will be released in June 2007).

8. Copyright and Disclaimer

This publication is Copyright (c) 2007 by AV-Comparatives. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of 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 2007)