



Anti-Virus Comparative No.16

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

contains also
False positive test
&
Scanning speed test

Date: November 2007 (2007-11)

Last revision: 27th November 2007

Author: Andreas Clementi

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

1. Introduction

This test report is the second part of the August 2007 test. The same products were used and the results show the proactive detection capabilities that the products had in August. 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 all new samples¹ received between 5th August and 31th August 2007. The following 17 products were tested in this comparative (last signature updates and versions are from 5th August 2007 [exception: Dr.Web, which engine is from October/November]):

- ❖ Avast! 4.7.1029 Professional Edition
- ❖ AVG Anti-Malware 7.5.476
- ❖ AVIRA AntiVir Personal Edition Premium 7.04.00.57
- ❖ BitDefender Anti-Virus 10 Professional Plus
- ❖ Dr.Web Anti-Virus for Windows 95-XP 4.44.1 (final)
- ❖ eScan Anti-Virus 9.0.722.1
- ❖ ESET NOD32 Anti-Virus 2.70.39
- ❖ Fortinet FortiClient 3.0.459
- ❖ F-Prot Anti-Virus for Windows 6.0.7.1
- ❖ F-Secure Anti-Virus 2007 7.01.128
- ❖ GDATA AntiVirusKit (AVK) 17.0.6353
- ❖ Kaspersky Anti-Virus 7.0.0.125
- ❖ McAfee VirusScan 11.2.121
- ❖ Microsoft Live OneCare 1.6.2111.30
- ❖ Norman Virus Control 5.91
- ❖ Symantec Norton Anti-Virus 14.0.3.3
- ❖ TrustPort Antivirus Workstation 1.4.2.428

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 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 more 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

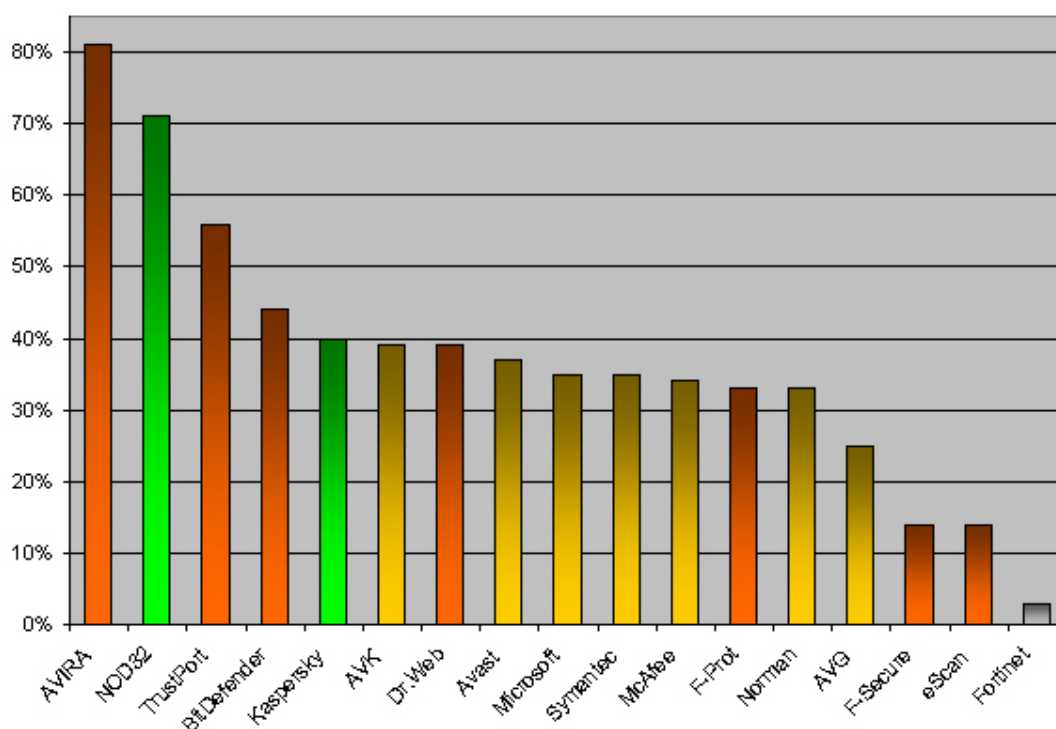
On request of various AV vendors, we changed a bit the test and sample selection methods. The time-frame used is this time only about one month instead of three months. This is more real-world like, but due the new sample selection method (based on appearance in our/other labs and not on signature detections) this test may be now a mixture of proactive and also a bit of retroactive detection.

Company	AVIRA		G DATA Security		Alwil Software		GriSoft		
Product	AntiVir PE Premium		AntiVirusKit (AVK)		Avast! Professional		AVG Anti-Malware		
Program version	7.04.00.57		17.0.6353		4.7.1029		7.5.476		
Engine / signature version	6.39.00.213		17.6648 / 17.326		0763-5		269.11.6 / 938		
Number of virus records	1.000.742		unknown		unknown		unknown		
Certification level reached'	STANDARD		ADVANCED		ADVANCED		ADVANCED		
Number of false positives'	many		few		few		few		
On-demand scanning speed*	<i>fast</i>		<i>slow</i>		<i>average</i>		<i>average</i>		
ProActive detection of 'NIEW' samples''									
Windows viruses	1.773	1.518	86%	1.127	64%	1.087	61%	411	23%
Macro	2	0	0%	0	0%	0	0%	0	0%
Script malware	333	142	43%	15	5%	11	3%	45	14%
Worms	4.322	4.076	94%	221	5%	217	5%	190	4%
Backdoors	5.532	4.759	86%	3.569	65%	3.434	62%	2.049	37%
Trojans	12.754	9.693	76%	4.878	38%	4.549	36%	3.462	27%
other malware	314	188	60%	47	15%	44	14%	92	29%
OtherOS malware	6	2	33%	0	0%	4	67%	0	0%
TOTAL	25.036	20.378	81%	9.857	39%	9.346	37%	6.249	25%

Company	Softwin		Doctor Web		MicroWorld		Fortinet		
Product	BitDefender Prof.+		Dr. Web		eScan Anti-Virus		FortiClient		
Program version	10.247		4.44.0.11070		9.0.722.1		3.0.459		
Engine / signature version	7.14211		4.44.1.10260		N/A		3.11 / 7.923		
Number of virus records	752.905		227.123		unknown		unknown		
Certification level reached'	STANDARD		STANDARD		STANDARD				
Number of false positives'	many		many		very few		few (w/o heuristic)		
On-demand scanning speed*	<i>average</i>		<i>slow</i>		<i>slow</i>		<i>fast</i>		
ProActive detection of 'NIEW' samples''									
Windows viruses	1.773	724	41%	961	54%	311	18%	35	2%
Macro	2	0	0%	0	0%	0	0%	0	0%
Script malware	333	25	8%	10	3%	5	2%	3	1%
Worms	4.322	570	13%	220	5%	113	3%	31	1%
Backdoors	5.532	3.281	59%	3.555	64%	1.131	20%	311	6%
Trojans	12.754	6.383	50%	4.913	39%	1.895	15%	401	3%
other malware	314	85	27%	36	11%	7	2%	11	4%
OtherOS malware	6	3	50%	0	0%	0	0%	0	0%
TOTAL	25.036	11.071	44%	9.695	39%	3.462	14%	792	3%

Company	Frisk Software		F-Secure		Kaspersky Labs		McAfee		
Product	F-Prot Anti-Virus		F-Secure Anti-Virus		Kaspersky AV		McAfee VirusScan		
Program version	6.0.7.1		7.01.128		7.0.0.125		11.2.121		
Engine / signature version	4.3.3		7.00.12371		N/A		5200 / 5090		
Number of virus records	685.078		unknown		373.197		303.739		
Certification level reached'	STANDARD		STANDARD		ADVANCED+		ADVANCED		
Number of false positives'	many		very few		few		few		
On-demand scanning speed*	<i>fast</i>		<i>slow</i>		<i>slow</i>		<i>average</i>		
ProActive detection of 'NIEW' samples''									
Windows viruses	1.773	575	32%	311	18%	971	55%	1.072	60%
Macro	2	0	0%	0	0%	0	0%	2	100%
Script malware	333	11	3%	11	3%	5	2%	14	4%
Worms	4.322	395	9%	113	3%	446	10%	365	8%
Backdoors	5.532	2.887	52%	1.131	20%	3.315	60%	3.162	57%
Trojans	12.754	4.433	35%	1.897	15%	5.354	42%	3.780	30%
other malware	314	45	14%	10	3%	34	11%	89	28%
OtherOS malware	6	0	0%	0	0%	0	0%	4	67%
TOTAL	25.036	8.346	33%	3.473	14%	10.125	40%	8.488	34%

Company	Microsoft	ESET	Norman ASA	Symantec	AEC	
Product	Microsoft OneCare	HOD32 Anti-Virus	NormanVirusControl	Horton Anti-Virus	TrustPort AV WS	
Program version	1.6.2111.30	2.70.39	5.91	14.0.3.3	1.4.2.428	
Engine / signature version	1.20.2827.3	2.438	5.91.02	90804t	2.6.0.1237	
Number of virus records	578.378	unknown	840.675	73.620	unknown	
Certification level reached*	ADVANCED	ADVANCED+	ADVANCED	ADVANCED	STANDARD	
Number of false positives*	<i>few</i>	<i>none</i>	<i>few</i>	<i>very few</i>	<i>many</i>	
On-demand scanning speed*	<i>average</i>	<i>fast</i>	<i>average</i>	<i>fast</i>	<i>slow</i>	
ProActive detection of "NEW" samples**						
Windows viruses	1.773	505	1.264	351	621	931
Macro	2	0	2	0	0	0
Script malware	333	24	7	11	12	65
Worms	4.322	1.226	4.163	1.449	3.880	1.461
Backdoors	5.532	1.806	3.889	2.743	1.197	4.226
Trojans	12.754	5.108	8.238	3.662	2.904	7.255
other malware	314	138	124	18	117	103
OtherOS malware	6	0	0	0	2	3
TOTAL	25.036	8.807	17.687	8.234	8.733	14.044



4. Summary results

The results show the proactive on-demand² 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 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 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	79%
2.	NOD32	66%
3.	TrustPort	62%
4.	BitDefender	52%
5.	Kaspersky	47%
6.	Dr.Web, AVK	46%
7.	Avast	43%
8.	F-Prot	40%
9.	Microsoft, McAfee	38%
10.	Norman	35%
11.	AVG	30%
12.	Symantec	23%
13.	F-Secure, eScan	16%
14.	Fortinet	4%

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

1.	AVIRA	89%
2.	NOD32	84%
3.	Symantec	70%
4.	TrustPort	38%
5.	Norman, Microsoft	28%
6.	McAfee	23%
7.	Kaspersky	22%
8.	AVK, BitDefender	21%
9.	Avast	20%
10.	Dr.Web	19%
11.	F-Prot	15%
12.	AVG	10%
13.	F-Secure, eScan	7%
14.	Fortinet	1%

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

1.	AVIRA	81%
2.	NOD32	71%
3.	TrustPort	56%
4.	BitDefender	44%
5.	Kaspersky	40%
6.	AVK, Dr.Web	39%
7.	Avast	37%
8.	Microsoft, Symantec	35%
9.	McAfee	34%
10.	F-Prot, Norman	33%
11.	AVG	25%
12.	F-Secure, eScan	14%
13.	Fortinet	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, eScan, AVG, 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.

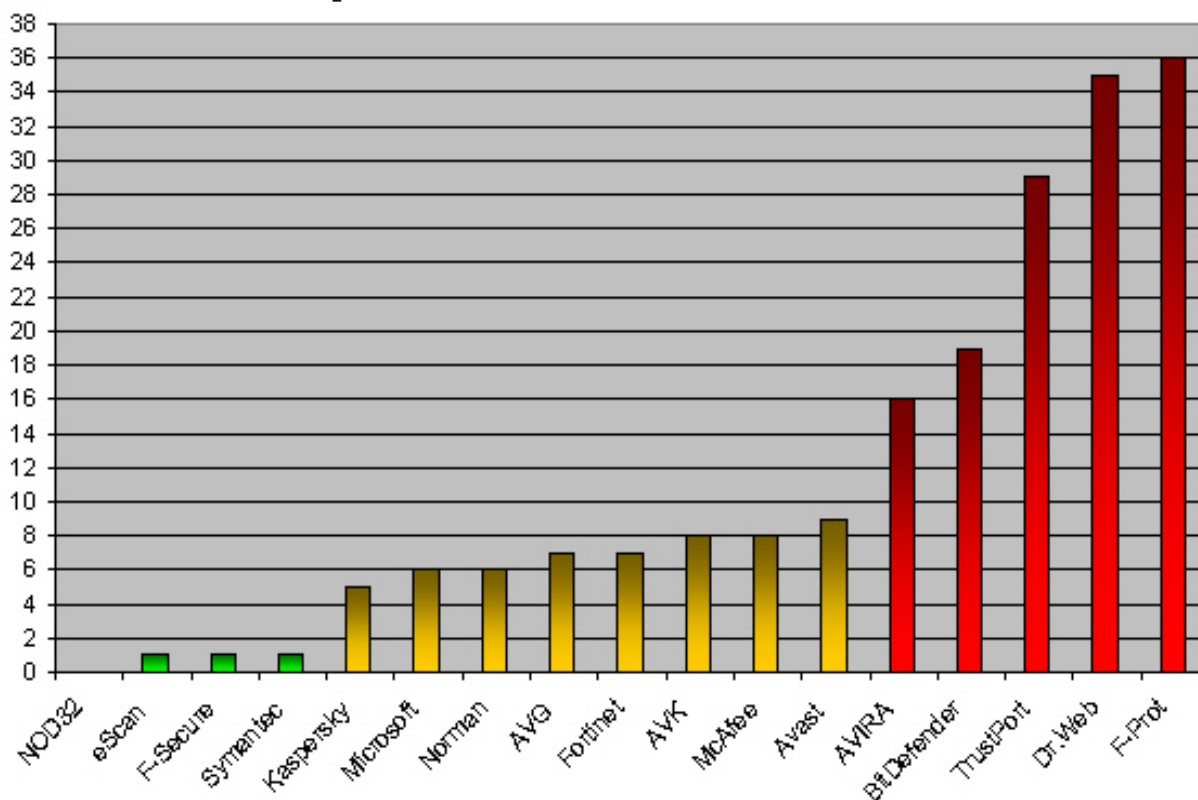
A false alarm (or false positive) is when an Anti-Virus product flags an innocent file to be infected when it is not. False alarms can sometimes cause as much troubles like a real infection.

Number of false positives found³:

1. NOD32	0	none or
2. eScan, F-Secure, Symantec	1	very few FP's
3. Kaspersky	5	
4. Microsoft, Norman	6	
5. AVG, Fortinet (<i>without heuristic</i>)	7	few FP's
6. AVK, McAfee	8	
7. Avast	9	
8. AVIRA	16	
9. BitDefender	19	
10. TrustPort	29	many FP's
11. Dr.Web	35	
12. F-Prot	36	

Products which have many FP's (false positives) can not gain the certification/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:



³ Lower is better

5.1 Details of the false positives detected

All listed false alarms were reported and sent (in October 2007) to the Anti-Virus vendors for verification and are now already fixed. False alarms caused by unencrypted data blocks in Anti-Virus related files are not counted in this test. If a product caused several false alarms in the same package, it is counted here as only 1 false alarm. If a false alarm is marked as "by signature", it means that the false alarm occurred also with disabled heuristics.

Avast

False alarm found in some part(s) of	Detected as	By
ANDRoute package	Win32:Trojan-gen	Signature (Quick)
CDL package	ELF:Agent	Signature (Normal)
Cubase VST32 package	Win32:SdBot-4468	Signature (Quick)
ICQ package	Win32:Trojan-gen	Signature (Quick)
PEINFO package	Win32:Simile	Signature (Normal)
PestPatrol package	Win32:Trojan-gen	Signature (Quick)
TransMac package	Win32:Gaobot-2134	Signature (Quick)
WineBook package	Win32:Orez-K	Signature (Quick)
Zoner Draw package	Win32:Trojan-gen	Signature (Quick)

Avast had 9 false positives. In parenthesis the minimum scan mode in which they occurred.

AVG

False alarm found in some part(s) of	Detected as	By
AudioVideoToExe package	Generic5.JXF	Signature
ClamWin package	Downloader.QQHelper.gt	Signature (Ewido)
Gothic 2 package	PSW.Generic4.MUZ	Signature
Joshuas PreShell package	Generic5.IVD	Signature
PHP-Nuke package	Hijacker.Iframe.1	Signature (Ewido)
VirtualDub package	Trojan.LdPinch	Signature (Ewido)
XP Tweaker package	Downloader.Generic3.RUR	Signature

AVG Anti-Malware had 7 false positives.

Norman

False alarm found in some part(s) of	Detected as	By
AudioVideoToExe package	W32/Suspicious_U.gen	Signature
BatchToExe Converter package	W32/Zacryxof.A.dropper	Signature
NvHardPage package	W32/Adclicker.AJY	Signature
RunWithParameters package	W32/Suspicious_U.gen	Signature
UPACK compression tool package	W32/Suspicious_U.gen	Signature
Vispa package	W32/Suspicious_U.gen	Signature

Norman had 6 false positives.

eScan

False alarm found in some part(s) of	Detected as	By
ClamWin package	FraudTool.Win32.AntiVirusSolution.a	Signature

eScan had 1 false positive.

Microsoft

False alarm found in some part(s) of	Detected as	By
AutoHotKey package	TrojanDownloader:Win32/Istbar!2C6D	Signature
Miranda package	VirTool:Win32/Obfuscator.C	Signature
NeoPlanet package	BrowserModifier:Win32/Flyswat	Signature
RemoveWGA package	TrojanDropper:Win32/Small!DEDA	Signature
RoseUtilities package	Trojan:Win32/Anomaly.gen!A	Signature
Winfingerprint package	SoftwareBundler:Win32/KaZaA	Signature

Microsoft OneCare had 6 false positives.

F-Secure

False alarm found in some part(s) of	Detected as	By
ClamWin package	FraudTool.Win32.AntiVirusSolution.a	Signature

F-Secure had 1 false positive.

AntiVir (AVIRA)

False alarm found in some part(s) of	Detected as	By
ASTdown package	W32/Gnil.a	Signature
ColorPK package	TR/Drop.Booty	Signature
Convert package	ADSPY/Dm.I.55	Signature
Cubase VST32 package	WORM/SdBOT.3478016	Signature
FritzBox Tools package	HEUR/Crypted	Heuristic (high)
F-Secure AV package	HEUR/Exploit.HTML	Heuristic (high)
KiX package	SPR/Tool.R	Signature
LANTool package	TR/Dldr.ARO	Signature
Nikto package	HEUR/Exploit.HTML	Heuristic (high)
Outlook package	TR/Cutespy.E	Signature
Radio Ripper package	HEUR/Malware	Heuristic (high)
Trend Micro AV package	HEUR/Exploit.HTML	Heuristic (high)
VBS Listings package	HEUR/Exploit.HTML	Heuristic (medium)
VP3 package	TR/Drop.Booty	Signature
VS2000GUI package	HEUR/Malware	Heuristic (low)
XpTweaker package	PCK/Packman	Signature (packer)

AVIRA had 16 false alarms.

NOD32 (ESET)

ESET NOD32 had no false alarms in our set of clean files.

Symantec (NAV)

False alarm found in some part(s) of	Detected as	By
Logitech G15 Gaming Keyboard package	Trojan.Zlob	Signature

Symantec Norton Anti-Virus had 1 false positive. The false alarm was fixed by Symantec few days after release, before we reported it to Symantec.

BitDefender

False alarm found in some part(s) of	Detected as	By
Acer_USB Driver package	Dialer.1000.I	Signature (PUP)
BatchToExe Converter package	Dropped:Trojan.Zacryxof.A	Signature
Bullet Proof FTP package	Trojan.Agent.BGY	Signature
CD DVD Burning package	Backdoor.Pcclient.GV	Signature
Desktop Notes package	Generic.Malware.M!H@mm.62540566	Signature
ExeCrypt package	Trojan.Multidropper.JN	Signature
File Securer package	Trojan.Click.Delf.GT	Signature
ICQ package	Backdoor.Ip.Protect.A	Signature
KidKey package	Trojan.Horse.BNM	Signature
LANTool package	Trojan.Downloader.ARO	Signature
MassDownloader package	Trojan.Downloader.BEC	Signature
MP3 DirectCut package	Trojan.Dropper.Agent.G	Signature
NetControl package	Generic.Malware.SL!g.EAEAF616	Signature
NetMeter package	Trojan.Downloader.Q.TR	Signature
Parents Friend package	Trojan.Vb.JI	Signature
RunWithParameters package	Trojan.Downloader.Zlob.NI	Signature
TopDesk package	Trojan.Favadd.BB	Signature
TweakXP package	Spyware.Hideagentdll.A	Signature (PUP)
VicMan PhotoEditor package	Trojan.Peed.Gen	Signature

Bitdefender had 19 false positives.

Kaspersky

False alarm found in some parts of	Detected as	By
ClamWin package	FraudTool.Win32.AntiVirusSolution.a	Signature
eScan package	Heur.Trojan.Generic	Heuristic (Medium)
F-Secure AV package	Heur.Trojan.Generic	Heuristic (Shallow)
PostScript Converter package	Heur.Worm.Generic	Heuristic (Shallow)
SetPoint Bluetooth package	Heur.Trojan.Generic	Heuristic (Detail)

Kaspersky had 5 false positives.

G DATA AVK

False alarm found in some part(s) of	Detected as	By
ANDRoute package	Win32:Trojan-gen	Signature
CDL package	ELF:Agent	Signature
ClamWin package	FraudTool.Win32.AntiVirusSolution.a	Signature
Cubase VST32 package	Win32:SdBot-4468	Signature
PEINFO package	Win32:Simile	Signature
PestPatrol package	Win32:Trojan-gen	Signature
WineBook package	Win32:Orez-K	Signature
Zoner Draw package	Win32:Trojan-gen	Signature

GDATA AVK had 8 false positives (1 caused by the KAV engine and 7 by the Avast engine it uses).

McAfee

False alarm found in some part(s) of	Detected as	By
AudioVideoToExe package	New Malware.aj variant	Heuristic
CableMonitor package	New Malware.dq variant	Signature
CD DVD Burning package	New Malware.bj variant	Heuristic
Cubase VST32 package	Generic.ea variant	Heuristic
Joshuas Preshell package	New Malware.dq variant	Signature
PocketDivXEncoder package	Generic.ea variant	Heuristic
RunWithParameters package	New Malware.j variant	Heuristic
Vispa package	New Malware.aj variant	Heuristic

McAfee had 8 false positives.

F-Prot

False alarm found in some parts of	Detected as	By
Artofillusion package	ZIP Bomb	Normal scan
AudioVideoToExe package	{no name}	Thorough scan
Bitdefender package	W32/NewMalware-LSU-based!Maximus	Quick scan
BORG package	ZIP Bomb	Normal scan
Bullfrog package	{no name}	Thorough scan
Capivara package	ZIP Bomb	Normal scan
CFOSSpeed package	ANI-exploit(1)	Quick scan
ClamWin Portable package	W32/Downloader!7b84	Quick scan
Das Telefonbuch package	{no name}	Quick scan
DreamMail package	{no name}	Thorough scan
EnvelopePrinter package	ZIP Bomb	Thorough scan
FileAnalyser package	W32/Backdoor.AJKH	Quick scan
FTCheck package	W32/Blocker-based!Maximus	Quick scan
Gothic 2 package	W32/Trojan.BHOT	Quick scan
iN@tControl package	W32/NewMalware-Rootkit-I-based!Maximus	Quick scan
Memtest86 package	{no name}	Quick scan
Microsoft Office 2007 package	W32/NewMalware-LSU-based!Maximus	Quick scan
Miranda package	{no name}	Thorough scan
Mobimb package	{no name}	Thorough scan
Nero package	{no name}	Thorough scan
No23Recorder package	{no name}	Quick scan
Powerstrip package	{no name}	Thorough scan
RCS package	W32/VB-Backdoor-PSVR-based!Maximus	Quick scan
Rootkit Unhooker package	{no name}	Thorough scan
Router Syslog package	{no name}	Thorough scan
RunWithParameters package	{no name}	Thorough scan
SafeXP package	{no name}	Thorough scan
SecurityTaskManager package	{no name}	Thorough scan
SpamTerrier package	W32/Malware!2laf	Quick scan
SplitFMan package	W32/Trojan.AOCU	Quick scan
Splitting package	{no name}	Thorough scan
TaskSwitchXP package	W32/Malware!f0bb	Quick scan
UPACK compression tool package	{no name}	Thorough scan
USBAgent package	W32/Blocker-based!Maximus	Quick scan
Vispa package	{no name}	Thorough scan
Webscara package	ZIP Bomb	Normal scan

F-Prot had 36 false positives.

TrustPort

False alarm found in some part(s) of	Detected as	By
Acer USB Driver package	Dialer.1000.I	Signature
AudioVideoToExe package	Generic5.JXF	Signature
BatchToExe Converter package	Dropped:Trojan.Zacryxof.A	Signature
BulletProof FTP package	Trojan.Agent.BGY	Signature
CD DVD Burning package	Backdoor.Pcclient.GV	Signature
ClamWin package	Downloader.QQHelper.gt	Signature
DesktopNotes package	Generic.Malware.M!H@mm.62540566	Signature
ExeCrypt package	Trojan.Multidropper.JN	Signature
File Securer package	Trojan.Click.Delf.GT	Signature
Gothic 2 package	PSW.Generic4.MUZ	Signature
ICQ package	Backdoor.Ip.Protect.A	Signature
Joshuas Preshell package	Generic5.IVD	Signature
KidKey package	Trojan.Horse.BNM	Signature
LANTool package	Trojan.Downloader.ARO	Signature
MassDownloader package	Trojan.Downloader.BEC	Signature
MP3 DirectCut package	Trojan.Dropper.Agent.G	Signature
NetControl package	Generic.Malware.SL!g.EAEAF616	Signature
NetMeter package	Trojan.Downloader.Q.TR	Signature
NvHardpage package	W32/Adclicker.AJY	Signature
ParentsFriend package	Trojan.Vb.JI	Signature
PHP-Nuke package	Hijacker.Iframe.1	Signature
RunWithParameters package	Trojan.Downloader.Zlob.NI	Signature
TopDesk package	Trojan.Favadd.BB	Signature
TweakXP package	Spyware.Hideagentdll.A	Signature
UPACK compression tool package	W32/Suspicious_U.gen	Signature
VicMan PhotoEditor package	Trojan.Peed.Gen	Signature
VirtualDub package	Trojan.LdPinch	Signature
Vispa package	W32/Suspicious_U.gen	Signature
XPTweaker package	Downloader.Generic3.RUR	Signature

TrustPort had 29 false positives (caused by the engines it uses: Bitdefender, AVG, Ewido, Norman).

Dr.Web

False alarm found in some part(s) of	Detected as	By
ACER_RecoveryCD package	Win32.HLLM.Graz	Signature
ADVGrid package	modification of Win32.Swaduk.6891	Signature
AntiSpamBoy package	Trojan.MulDrop.4566	Signature
Anvil Studio package	modification of BAT.Mtr.1429	Signature
AOL IM package	probably BACKDOOR.Trojan	Heuristic
ASAP Utilities package	W97M.Iseng	Signature
Commander package	probably BACKDOOR.Trojan	Heuristic
Conpresso package	probably SCRIPT.Virus	Heuristic
CopySys package	Probably BACKDOOR.Trojan	Heuristic
Dimanage package	probably DLOADER.Trojan	Heuristic
eScan package	probably WIN.MAIL.WORM.Virus	Heuristic
FlexInfo package	probably BACKDOOR.Trojan	Heuristic
FRITZ!Box package	Trojan.Click.2798	Signature
F-Secure AV package	probably DLOADER.Trojan	Heuristic
GenHTML package	modification of W97M.Gamlet	Signature
HardwareList package	probably SCRIPT.Virus	Heuristic

HDDVDJump package	Win32.HLLW.Dbot	Signature
Kindersicherung package	modification of BackDoor.Generic.1253	Signature
LANTool package	Trojan.DownLoader.10130	Signature
Logincon package	modification of BackDoor.Generic.1200	Signature
MaxiVista package	probably BACKDOOR.Trojan	Heuristic
Metronom package	Win32.HLLW.Gavir.81	Signature
Minimalist GNU package	modification of Eblis.1150	Signature
NetTools package	probably BACKDOOR.Trojan	Heuristic
PCZugriff package	probably DLOADER.Trojan	Heuristic
RegistrySystemWizard package	probably BACKDOOR.Trojan	Heuristic
ServerHound package	modification of BackDoor.Generic.1116	Signature
ShutDownAlone package	probably BACKDOOR.Trojan	Heuristic
Skripte package	modification of VBS.Phereal	Signature
SpamPal package	Trojan.Proxy.1715	Signature
SparSurf package	Trojan.PWS.Wbopen	Signature
Spywall package	probably BACKDOOR.Trojan	Heuristic
TrendMicro AV package	modification of Trojan.DelSys.191	Signature
Wintuning Kit package	probably STPAGE.Trojan	Heuristic
YABE Office package	probably BACKDOOR.Trojan	Heuristic

Dr.Web had 35 false positives.

Fortinet

False alarm found in some part(s) of	Detected as	By
Ascope package	Squisher.338.B	Signature
BartPE package	Misc/BEAV_MS06	Signature
Microsoft Windows ME (CDPlayer) package	W32/Puron@mm	Signature
MZoom package	Spy/Multidr	Signature
Schwarzbuch package	PossibleThreat	Signature
Trend Micro AV package	Keylog/Quick	Signature
XPY package	W32/PE_Patch.Z	Signature

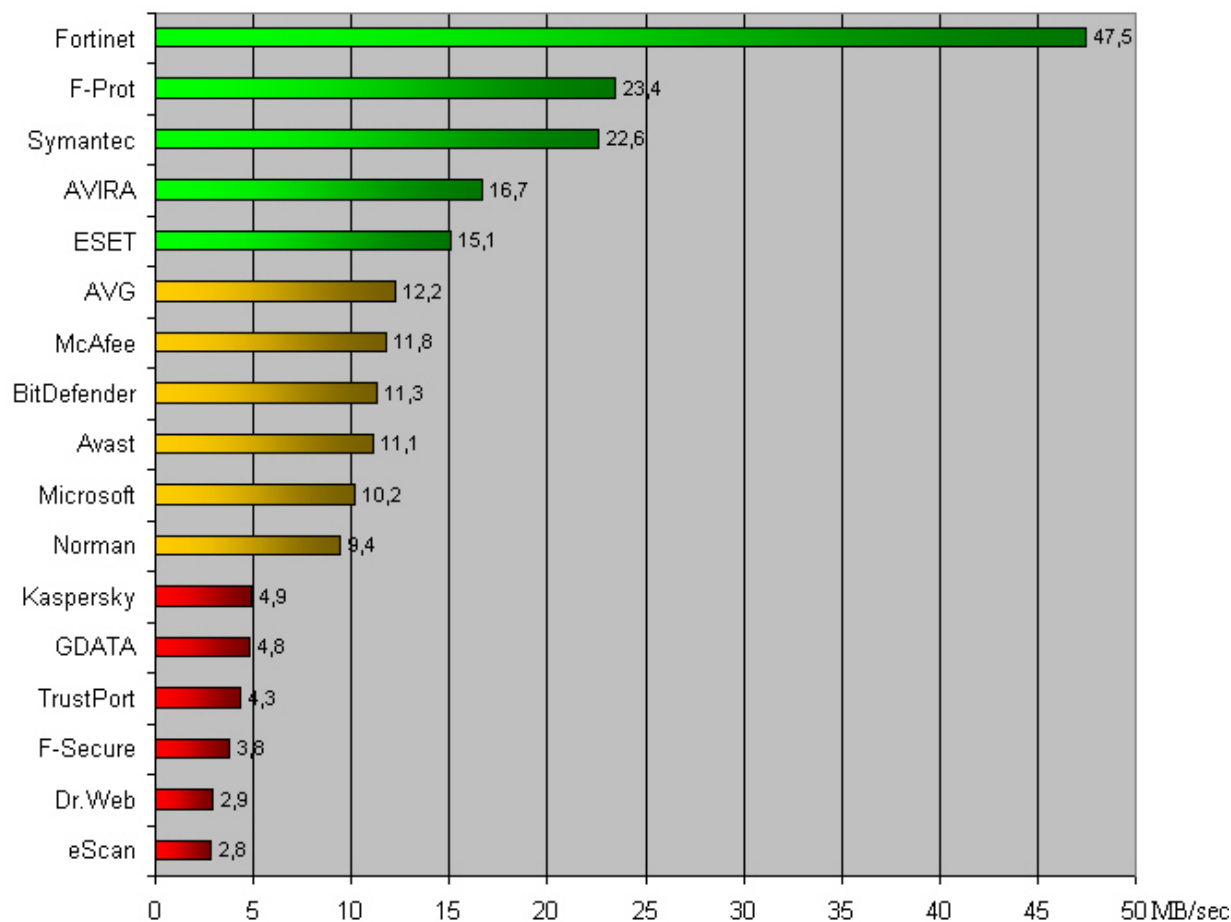
Fortinet was tested with disabled heuristic, because with enabled heuristic the product (still) causes thousands of false alarms (see also report Nr.14) and is therefore of no use in a home user product (we recommend to home users to do not enable the heuristic of FortiClient, due the high amount of false alarms).

Fortinet had 7 false positives with disabled heuristic, including a severe false positive in a file of Microsoft Windows ME.

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 uses code emulation, if it is able to detect difficult polymorphic viruses, if it does a deep heuristic scan analysis, how depth and thoroughful the unpacking and unarchiving support is, 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 files⁴ the settings in the product⁵ and the hardware used.



The average scanning throughput rate (scan speed) is calculated by size of the 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, this time on a PC with Intel Core 2 Extreme QX6800EE 2,66 GHz, ASUS P5W WS Pro, 4096 MB DDR2-1150 RAM, SATA II disks and without network connection.




The following product(s) were unable to scan the whole set of clean files without problems: Dr.Web (copies of all the files where Dr.Web crashed have been sent to the vendor and should now be fixed).

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 highest possible detection settings (also for Fortinet)

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:

<u>CERTIFICATION LEVELS</u>	<u>PRODUCTS</u> (in alphabetical order)
	<p>Kaspersky NOD32</p>
	<p>AVG AVK Avast McAfee Microsoft Norman Symantec</p>
	<p>AVIRA* BitDefender* Dr.Web* eScan F-Prot* F-Secure TrustPort*</p>
no certification	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 product that causes too many false alarms (also because it is much easier to score high in tests [also the ones from February and August] with a heuristic which is more prone to false alarms than other products).*

8. Copyright and Disclaimer

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