



## Anti-Virus Comparative No.18

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

contains also  
False positive test  
&  
Scanning speed test

Date: May 2008 (2008-05)

Last revision: 31<sup>st</sup> May 2008

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

## 1. Introduction

This test report is the second part of the February 2008 test. 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 the 4<sup>th</sup> February, were used for this tests, which shows the proactive detection capabilities that the products had at that time. For this test we used all new samples received between 5<sup>th</sup> and ~12<sup>th</sup> February 2008. The following 16 products were tested in this comparative:

- ❖ avast! Professional Edition 4.7.1098
- ❖ AVG Anti-Malware 7.5.516
- ❖ AVIRA AntiVir Personal Edition Premium 7.06.00.308
- ❖ BitDefender Anti-Virus 2008 11.0.15
- ❖ eScan Anti-Virus 9.0.768.1
- ❖ ESET<sup>1</sup> NOD32 Antivirus 3.0.621.0
- ❖ F-Secure Anti-Virus 2008 8.00.101
- ❖ G DATA AntiVirusKit (AVK) 2008 18.0.7227.533
- ❖ Kaspersky Anti-Virus 7.0.1.321a
- ❖ McAfee VirusScan Plus 2008 12.0.176
- ❖ Microsoft Live OneCare 2.0.2500.22
- ❖ Norman SS Antivirus & Anti-Spyware 7.0
- ❖ Sophos Anti-Virus 7.0.7
- ❖ Symantec Norton Anti-Virus 2008 15.0.0.58
- ❖ TrustPort Antivirus Workstation 2.8.0.1629
- ❖ VBA32<sup>2</sup> Scanner for Windows 3.12.6.0

## 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 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.

---

<sup>1</sup> incl. default "Statik" heuristic

<sup>2</sup> on request of VBA32, "Excessive heuristic" and "Thourough mode" were disabled, as they are "mostly useless, but increase scanning time" (and false alarm rate). If activated, VBA32 would score ~4% higher in this test.

### 3. Test results

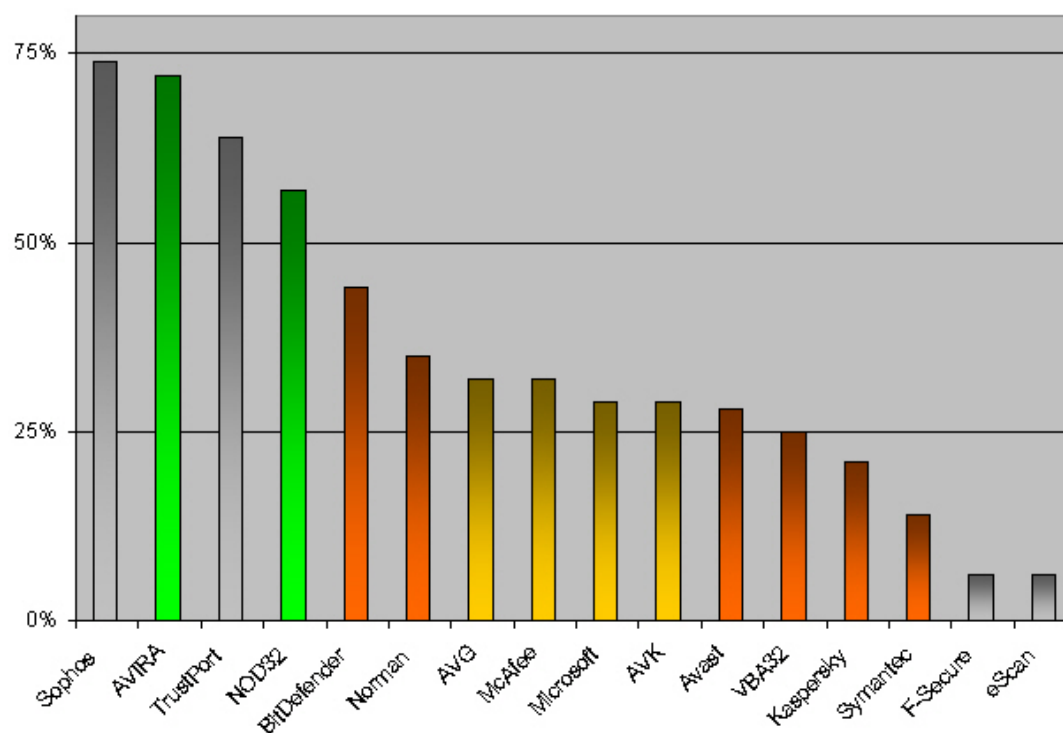
This test differs a bit from previous retrospective tests: the time-frame for samples has been shortened to only about one week. In past some peoples suggested that a short period would reflect better the real world - but this assumption did not consider everything and introduced some bias. Next time we will include a short and a long period, which (due higher amount/variety of samples) will reduce possible bias.

Company	AVIRA		G DATA Security		Alwil Software		AVG Technologies		
Product	AntiVir PE Premium		AntiVirusKit (AVK)		Avast! Professional		AVG Anti-Malware		
Program version	7.06.00.308		18.0.7227.533		4.7.1098		7.5.516		
Engine / signature version	7.06.00.62 / 7.00.02.90		18.2654 / 18.123		080203-0		269.19.19 / 1258		
Number of virus records	1.092.160		unknown		unknown		unknown		
<b>Certification level reached'</b>	<b>ADVANCED+</b>		<b>ADVANCED</b>		<b>STANDARD</b>		<b>ADVANCED</b>		
<b>Number of false positives'</b>	<b>few</b>		<b>few</b>		<b>many</b>		<b>few</b>		
On-demand scanning speed*	<i>fast</i>		<i>slow</i>		<i>average</i>		<i>average</i>		
<b>ProActive detection of "NEW" samples''</b>									
Windows viruses	190	171	90%	151	79%	149	78%	145	76%
Script malware	287	95	33%	17	6%	14	5%	66	23%
Worms	586	418	71%	159	27%	154	26%	241	41%
Backdoors	4.055	3.193	79%	1.702	42%	1.682	41%	1.592	39%
Trojans	6.258	4.340	69%	1.274	20%	1.267	20%	1.618	26%
other malware	133	59	44%	13	10%	13	10%	40	30%
<b>TOTAL</b>	<b>11.509</b>	<b>8.276</b>	<b>72%</b>	<b>3.316</b>	<b>29%</b>	<b>3.279</b>	<b>28%</b>	<b>3.702</b>	<b>32%</b>

Company	BitDefender		MicroWorld		F-Secure		Kaspersky Labs		
Product	BitDefender AV		eScan Anti-Virus		F-Secure Anti-Virus		Kaspersky AV		
Program version	11.0.15		9.0.768.1		8.00.101		7.0.1.321a		
Engine / signature version	7.17325		N/A		7.30.13161		N/A		
Number of virus records	978.896		unknown		unknown		574.209		
<b>Certification level reached'</b>	<b>STANDARD</b>						<b>STANDARD</b>		
<b>Number of false positives'</b>	<b>many</b>		<b>very few</b>		<b>very few</b>		<b>very few</b>		
On-demand scanning speed*	<i>average</i>		<i>slow</i>		<i>slow</i>		<i>slow</i>		
<b>ProActive detection of "NEW" samples''</b>									
Windows viruses	190	166	87%	110	58%	110	58%	144	76%
Script malware	287	33	11%	3	1%	9	3%	5	2%
Worms	586	294	50%	50	9%	54	9%	108	18%
Backdoors	4.055	2.022	50%	165	4%	165	4%	782	19%
Trojans	6.258	2.556	41%	340	5%	340	5%	1.371	22%
other malware	133	41	31%	0	0%	3	2%	3	2%
<b>TOTAL</b>	<b>11.509</b>	<b>5.112</b>	<b>44%</b>	<b>668</b>	<b>6%</b>	<b>681</b>	<b>6%</b>	<b>2.413</b>	<b>21%</b>

Company	McAfee		Microsoft		ESET		Norman ASA		
Product	McAfee VirusScan+		Microsoft OneCare		NOD32 Anti-Virus		Norman ISS AV+AS		
Program version	12.0.176		2.0.2500.22		3.0.621.0		7.0		
Engine / signature version	5200.2160 / 5222		1.3204 / 1.27.6270.0		2847		5.91.10		
Number of virus records	371.817		723.778		unknown		1.310.735		
<b>Certification level reached'</b>	<b>ADVANCED</b>		<b>ADVANCED</b>		<b>ADVANCED+</b>		<b>STANDARD</b>		
<b>Number of false positives'</b>	<b>none</b>		<b>few</b>		<b>few</b>		<b>many</b>		
On-demand scanning speed*	<i>average</i>		<i>average</i>		<i>average</i>		<i>average</i>		
<b>ProActive detection of "NEW" samples''</b>									
Windows viruses	190	148	78%	125	66%	45	24%	135	71%
Script malware	287	23	8%	36	13%	9	3%	15	5%
Worms	586	214	37%	140	24%	425	73%	148	25%
Backdoors	4.055	1.676	41%	1.182	29%	2.713	67%	1.821	45%
Trojans	6.258	1.574	25%	1.818	29%	3.309	53%	1.954	31%
other malware	133	24	18%	41	31%	19	14%	6	5%
<b>TOTAL</b>	<b>11.509</b>	<b>3.659</b>	<b>32%</b>	<b>3.342</b>	<b>29%</b>	<b>6.520</b>	<b>57%</b>	<b>4.079</b>	<b>35%</b>

Company	Symantec	Sophos	AEC	VirusBlokAda					
Product	<b>Horton Anti-Virus</b>	<b>Sophos Anti-Virus</b>	<b>TrustPort AV WS</b>	<b>VBA32 Anti-Virus</b>					
Program version	15.0.0.58	7.0.7	1.4.2.428	3.12.6.0					
Engine / signature version	100204 / 78215	2.70.1 / 4.26E+132	2.6.0.1237	unknown					
Number of virus records	73.845	345.615	unknown	unknown					
<b>Certification level reached<sup>1</sup></b>	<b>STANDARD</b>			<b>STANDARD</b>					
<b>Number of false positives<sup>2</sup></b>	<b>very few</b>	<b>(very) many</b>	<b>(very) many</b>	<b>many</b>					
On-demand scanning speed <sup>3</sup>	<i>fast</i>	<i>average</i>	<i>slow</i>	<i>slow</i>					
<b>ProActive detection of "NEW" samples<sup>4</sup></b>									
Windows viruses	190	12	6%	164	86%	173	91%	134	71%
Script malware	287	63	22%	59	21%	80	28%	1	0%
Worms	586	141	24%	422	72%	351	60%	93	16%
Backdoors	4.055	938	23%	3.526	87%	2.935	72%	1.221	30%
Trojans	6.258	891	14%	4.323	69%	3.736	60%	1.422	23%
other malware	133	4	3%	44	33%	53	40%	9	7%
<b>TOTAL</b>	<b>11.509</b>	<b>2.049</b>	<b>18%</b>	<b>8.538</b>	<b>74%</b>	<b>7.328</b>	<b>64%</b>	<b>2.880</b>	<b>25%</b>



#### 4. Summary results

The results show the proactive on-demand<sup>3</sup> 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.

Please also have a look on our methodology document for further details (<http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf><sup>4</sup>).

<sup>3</sup> this test is performed on-demand – it is **NOT** an on-execution/behavioral test. Testing in on-demand scan mode does not exercise e.g. McAfee's ScriptScan functionality, which is available at the point of execution.

<sup>4</sup> this document will be updated during next months, as many things contained in it are now outdated

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.	Sophos	76%
2.	AVIRA	73%
3.	TrustPort	64%
4.	NOD32	58%
5.	BitDefender	44%
6.	Norman	36%
7.	McAfee, AVG	31%
8.	Microsoft, AVK	29%
9.	Avast	28%
10.	VBA32	25%
11.	Kaspersky	21%
12.	Symantec	18%
13.	F-Secure, eScan	5%

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

1.	AVIRA	64%
2.	Sophos	61%
3.	TrustPort	57%
4.	BitDefender	46%
5.	NOD32	45%
6.	AVG	43%
7.	McAfee	36%
8.	AVK	31%
9.	Avast	30%
10.	Microsoft, Norman	28%
11.	Kaspersky	24%
12.	VBA32	21%
13.	Symantec	20%
14.	F-Secure, eScan	15%

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

1.	Sophos	74%
2.	AVIRA	72%
3.	TrustPort	64%
4.	NOD32	57%
5.	BitDefender	44%
6.	Norman	35%
7.	AVG, McAfee	32%
8.	Microsoft, AVK	29%
9.	Avast	28%
10.	VBA32	25%
11.	Kaspersky <sup>5</sup>	21%
12.	Symantec <sup>6</sup>	14%
13.	F-Secure, eScan	6%

*Note: Due the shortened time-frame of only 1-week, the variety of the sample population is limited and e.g. targeted well-known products may score considerably lower than expected against the malware in this specific period. Next time we will use both an 1-week AND e.g. a 1-month samples collecting window, in order that the variety and amount of the samples compensates e.g. such kind of influences and results are more meaningful. This time the results may not be generally applicable.*

<sup>5</sup> KIS v8 would score ~42% - separate report available at: <http://www.av-comparatives.org/seiten/ergebnisse/KIS8.pdf>

<sup>6</sup> a preview of Symantec's improved technology (not yet publicly available) scored ~41%

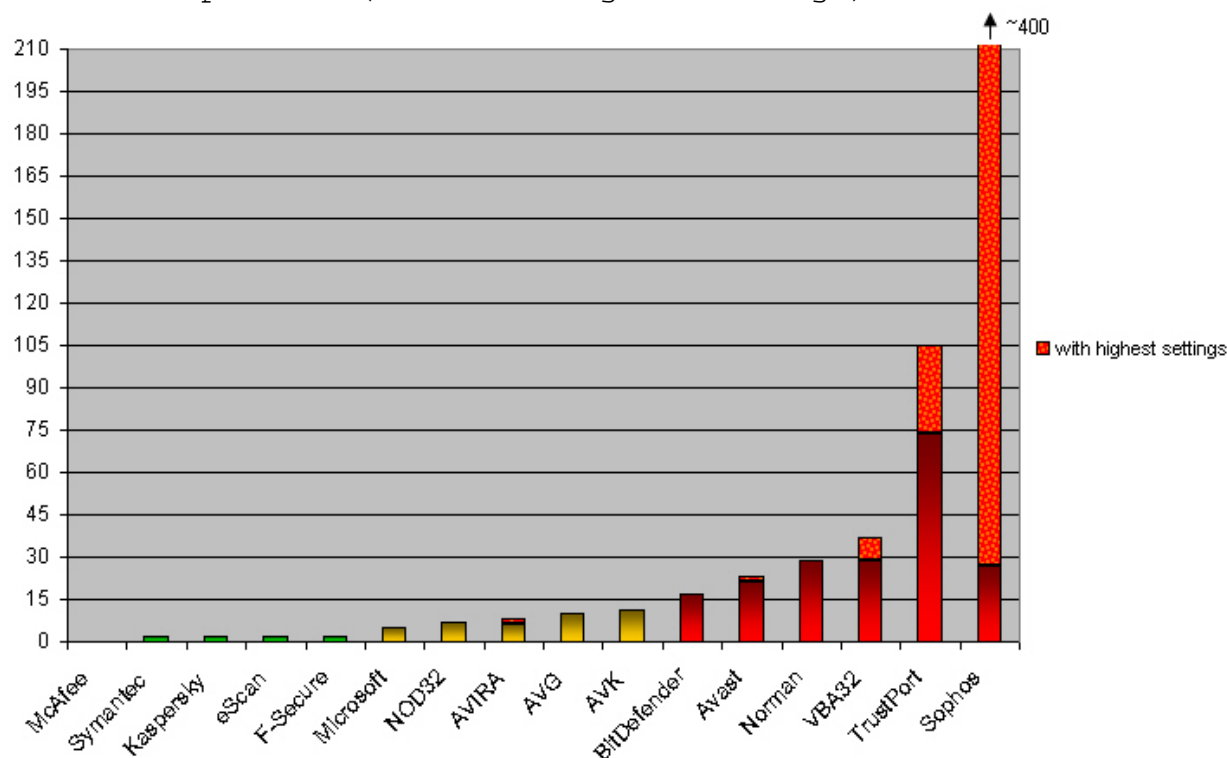
## 5. False positive/alarm test

We provide in our retrospective test reports also a false alarm test, in order to better evaluate the quality of the 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. Please consider the false alarm rate also when looking at the test results of February, as a product which is prone to cause false alarms achieves easier higher scores. In future the false alarm test will be included in the test report of February and August instead of May and November.

Number of false alarms found in our clean set (lower is better):

1. McAfee	0	none or
2. Symantec, Kaspersky, eScan, F-Secure	2	very few FP's
3. Microsoft	5	
4. NOD32	7	
5. AVIRA	8	few FP's
6. AVG	10	
7. AVK	11	
8. BitDefender	17	
9. Avast	23	
10. Norman	29	many FP's
11. VBA32	37	
12. TrustPort	105	
13. Sophos	~400	very many FP's

The graph below shows the number of false alarms by the various Anti-Virus products (default<sup>7</sup> + highest settings):



In future we will include the false alarm test already in the reports of February and August.

<sup>7</sup> default detection settings and scan of all files and archives activated

### **5.1 Details about the discovered false alarms**

All listed false alarms were reported and sent 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. Also the false alarm test is done with highest detection settings. You can anyway see how many of the listed false alarms would occur also with default settings.

The false alarm test indicates that in general the false alarm rate increased compared to previous test results and that most false alarms would occur also already with default settings. Could be that since most vendors start blacklisting packers/cryptors and use more generic detection methods to increase detection rates this raises more false alarms than in past. Most products with a low proactive detection rate in the retrospective test had this time also a low false alarm rate.

Another reason could be that some few vendors simple add detection for files that are detected by some other vendors, incl. false alarms. Mistakes can happen and the products included in our tests usually do this within reasonable ranges, while some other products (usually not-well known anti-virus products) do it systematically.

## **Avast**

<b>False alarm found in some part(s) of</b>	<b>Detected as</b>	<b>Settings</b>
Adobe Premiere package	Win32:JunkPoly [Cryp]	default
Advanced IM Password Recovery package	Win32:Trojan-gen {Other}	default
Batch2ExeConverter package	Win32:Shutdown-D [Trj]	default
BWMeter package	Win32:Trojan-gen {Other}	default
Datei CommanderLE package	Win32:Trojan-gen {Other}	default
diHTPC package	Win32:Agent-NJP [Trj]	default
Image Optimizer package	Win32:Nimosw-F [Trj]	default
KidKey package	Win32:Trojan-gen {VB}	default
LANNetScan package	Win32:Trojan-gen {Delphi}	default
MalwareBouncer package	Win32:Trojan-gen {Other}	default
MultipleChoice QuizMaker package	VBS:Malware-gen	default
NetControl package	Win32:Agent-NXF [Trj]	default
NOD32 AV package	Win32:Trojan-gen {Other}	default
Parallaxis iAlbum package	Win32:Downloader-LL [Trj]	default
Pioneer Driver package	Win32:Nimosw-B [Trj]	thorough scan
PowerQuiz package	Win32:Delf-CKU [Trj]	thorough scan
TaskManager package	Win32:Trojan-gen {Other}	default
TaskSwitchXP package	Win32:Wopla-AI [Trj]	default
TDSL SupportCenter package	Win32:Adware-gen [Adw]	default
Wetterspiegel package	Win32:Small-CAI [Trj]	default
WimUtil package	Win32:Agent-RNO [Trj]	default
WinPLOSSION package	Win32:Trojan-gen {Other}	default
WormRadar package	Win32:Doomjuice [Wrm]	default

Avast had in total 23 false alarms, 21 with default settings.

## McAfee

McAfee was this time the only product with no false alarms in our set of clean files.

## AVG

False alarm found in some part(s) of	Detected as	Settings
Ares package	IRC/BackDoor.SdBot3.QNN	default
Fezee package	Generic9.VRS	default
Hide In Picture package	Downloader.Generic6.XZK	default
HoverWheel package	SHeur.ABKE	default
McAfee Firewall package	Worm.Bobic.cx	default
McAfee PatchScanner package	Generic4.IVW	default
NVidia Driver package	Downloader.Swizzor	default
PHP-Nuke package	Hijacker.Iframe.1	default
System Safety Monitor package	Delf.BIJ	default
TDSL SpeedManager package	Generic9.SHV	default

AVG Anti-Malware had 10 false alarms, all with default settings.

## AVIRA (AntiVir)

False alarm found in some part(s) of	Detected as	Settings
CacheBoost package	TR/Agent.920268	default
Creative Driver package	TR/ReadReg	default
MaulwurfsMover package	PCK/FSG	extended (packer)
McAfee PatchScanner package	TR/Agent.516096.A	default
MS Base Cryptographic Provider package	TR/Packed.2465	default
PersonalTranslator package	TR/Crypt.CFI.Gen	default
SystemSafetyMonitor package	HEUR/Malware	high heuristic
TCPfilter package	TR/Spy.Agent.NEZ.4	default

AVIRA had in total 8 false alarms, 6 with default settings.

## Norman

False alarm found in some part(s) of	Detected as	Settings
AirSnare package	W32/SDBot.BFRK	default
Aptajm package	Adclicker.BMF	default
Artweaver package	Adclicker.BMC	default
AudioVideo2Exe package	W32/Suspicious_U.gen	default
C-Media Driver package	W32/Malware.BFQC	default
ClamWin package	Adclicker.BMF	default
Creative Driver package	W32/Malware.BHIF	default
DiskChart package	Adclicker.BMF	default
FrameFun package	Adclicker.BMC	default
Gem package	Adclicker.BMF	default
HotCPU package	Adclicker.BMC	default
Kaspersky AV package	W32/Malware	default
KillTask package	W32/Malware	default
Lysoft package	W32/Malware	default
MaulwurfsMover package	Suspicious_F.gen	default



McAfee PatchScanner package	W32/Malware.XVQ	default
Omnipage package	W32/Malware	default
Orb package	Adclicker.BMC	default
PC Accelerator package	W32/Smalltroj.CQJX	default
QuickStart package	Adclicker.BMF	default
RaBiT package	W32/Malware	default
RunWithParameters package	W32/Suspicious_U.gen	default
TDSLTest package	W32/Malware	default
TunePoint package	W32/Smalltroj.CQJX	default
TVgenial package	W32/Delf.AXFD	default
TwonkyW package	W32/Malware	default
USB-Access package	Adclicker.BMF	default
Vispa package	W32/Suspicious_U.gen	default
VitoSketchArtist package	W32/DLoader.CQU	default

Norman had 29 false alarms, all with default settings.

### Kaspersky

False alarm found in some parts of	Detected as	Settings
Mandrake package	Trojan-Dropper.MSWord.1Table.es	default
TrafficMonitor package	Backdoor.Win32.FTP.Matiteman	default

Kaspersky had 2 false alarms, both with default settings.

### F-Secure

False alarm found in some parts of	Detected as	Settings
Mandrake package	Trojan-Dropper.MSWord.1Table.es	default
TrafficMonitor package	Backdoor.Win32.FTP.Matiteman	default

F-Secure had 2 false alarms, both with default settings.

### eScan

False alarm found in some parts of	Detected as	Settings
Mandrake package	Trojan-Dropper.MSWord.1Table.es	default
TrafficMonitor package	Backdoor.Win32.FTP.Matiteman	default

eScan had 2 false alarms, both with default settings.

### Microsoft

False alarm found in some part(s) of	Detected as	Settings
AnimDesk package	Trojan:Win32/Killav.gen!A	default
Aranea package	Dialer:Win32/EGroupInstantAccess.A	default
BitDefender AV package	Trojan:Win32/VNCKill.A	default
Miranda package	VirTool:Win32/Obfuscator.C	default
SparkleXP package	Trojan:Win32/VNCKill.A	default

Microsoft OneCare had 5 false alarms, all with default settings.

**NOD32 (ESET)**

False alarm found in some part(s) of	Detected as	Settings
ABBYY FineReader package	Win32/Statik application	default
DeltaForce LandWarrior package	Win32/Statik application	default
dotWidget package	Win32/Statik application	default
McAfee PatchScanner package	NewHeur_PE virus	default
Raiload Pioneer package	Win32/Statik application	default
Secret Wars package	Win32/Statik application	default
The Punic Wars package	Win32/Statik application	default

ESET NOD32 had 7 false alarms, all with default settings.

**Symantec (NAV)**

False alarm found in some part(s) of	Detected as	Settings
Batch2Exe Converter package	Backdoor.Bifrose	default
MyPhotoBook package	Backdoor.Trojan	default

Symantec Norton Anti-Virus had 2 false alarms, both with default settings.

**BitDefender**

False alarm found in some part(s) of	Detected as	Settings
AlleMakros package	Macro.VBA	default
Advanced PDF Password Recovery package	Trojan.Generic.75317	default
BWMeter package	Trojan.Generic.77993	default
CacheBoost package	Trojan.Generic.78438	default
Desktop Notes package	DeepScan:Generic.Malware.M!H@mm.62540566	default
Kaspersky AV package	Trojan.Horse.Symbos.Drever.B	default
MailPerfect package	DeepScan:Generic.Malware.P!Pk.095E49D1	default
MemoryCleaner package	Trojan.Generic.78764	default
MS Base Cryptographic Provider package	Trojan.Packed.2465	default
Net Control package	Generic.Malware.SL!g.EAEAF616	default
Notepad++ package	Trojan.Generic.75502	default
PictureAceLite package	Trojan.Generic.75019	default
RegRun package	Trojan.Generic.59792	default
TCPfilter package	Trojan.Spy.Agent.NEZ	default
TrafMeter package	Worm.Padobot.C	default
WinPlosion package	Dropped:Trojan.Generic.52226	default
WormRadar package	Generic.XPL.IIS.2A9587B7	default

Bitdefender had 17 false alarms, all with default settings.

**TrustPort**

False alarm found in some part(s) of	Detected as	Settings
0190 Warner package	Trojan.Rootkit.origin	default
AceFTP package	Trojan.PWS.Bancos.307	default
Ad-Aware SE package	Downloader.Zlob.8	highest
ADVgrid package	Win32.Swaduk.6891	default
AirSnare package	W32/SDBot.BFRK	default
AktienProfi package	BackDoor.Danton.46	default

AmokPlayList package	Backdoor.XiaoBird.3	highest
Anvil Studio package	BAT.Mtr.1429	default
AOL Browser package	Trojan.StartPage.41	highest
AOL ConnFix package	Trojan.PWS.Gamania	default
AOL IM package	Trojan.StartPage.41	highest
Apache package	BAT.Julia.1000	default
aReaker package	P2P-Worm.Win32.Franvir	default
Ares package	IRC/BackDoor.SdBot3.QNN	default
Artweaver package	Adclicker.BMC	default
Auctamer package	Trojan.WinSpy.origin	default
AudioVideo2Exe package	W32/Suspicious_U.gen	default
Bagder Finance package	Backdoor.Agent.78	highest
Batch2ExeConverter package	OScope.Dialer.GMHA	default
BitComet package	Downloader.Zlob.8	highest
CatsCrad package	Trojan.Click.origin	default
ClamWin package	Adclicker.BMF	default
C-Media Driver package	W32/Malware.BFQC	default
Corel package	Exploit.Signature	default
CrazyVideos package	Flooder.VB.1	highest
Creative Driver package	W32/Malware.BHIF	default
Diashow package	Trojan.KeyLogger.origin	default
DigiFoto package	Backdoor.XiaoBird.43	highest
Dimanage package	DLOADER.Trojan	default
DiskChart package	Adclicker.BMF	default
Duden package	Backdoor.XiaoBird.23	highest
Ebay-Rechner package	BackDoor.BOrifice.112	default
eDVarDo package	BackDoor.BOrifice.112	default
EMIS package	TR.Spy.Banco.FR.2.C	default
Erunt package	Trojan.PWS.Banker.3682	default
F-Secure AV package	DLOADER.Trojan	default
Fezee package	Generic9.VRS	default
FlexInfo package	BACKDOOR.Trojan	default
FolderPatrol package	BackDoor.BOrifice.112	default
FrameFun package	Adclicker.BMC	default
FritzBox package	Trojan.Click.2798	default
G3D package	Downloader.Small.133	highest
GeForceTweakUtility package	Unknown.Win32Virus	default
Gem package	Adclicker.BMF	default
Gothic2 package	Trojan-PSW.Win32.Nilage.aer	default
HDDVDJump package	Win32.HLLW.Dbot	default
Hide In Picture package	Downloader.Generic6.XZK	default
HotCPU package	Adclicker.BMC	default
HoverWheel package	SHeur.ABKE	default
Imdb2Movid package	Trojan.Packed.194	default
InkScape package	Downloader.Zlob.10	highest
IPCop package	Downloader.Swizzor	default
Kaspersky AV package	Backdoor.Win32.Agent.aro	default
LANTool package	Trojan.DownLoader.10130	default
Lysoft package	W32/Malware	default
Matroska package	Embedded.Trojan.Hanspy	default
MaulwurfsMover package	Suspicious_F.gen	default
McAfee Firewall package	Worm.Bobic.cx	default
McAfee PatchScanner package	W32/Malware.XVQ	default

MoViC package	BackDoor.Danton.46	default
MovieClone package	BackDoor.Generic.1208	default
MS InternetExplorer package	BackDoor.Danton.46	default
MS Office 2007 package	Downloader.Zlob.7	highest
MyZippa package	Malware.Delf.128	highest
NaturPur package	Trojan.KillFiles.11340	default
Nmap package	Trojan-PSW.Game.30	highest
NZBPlayer package	Backdoor.XiaoBird.33	highest
OfficerBlue package	Trojan.Touch.origin	default
OfficeVorlagen package	Unknown.MacroVirus	highest
PC Grundlagen package	BackDoor.BOrifice.112	default
PDFExperte package	Trojan.MulDrop	default
PerfectMenu package	Trojan.DownLoader.origin	default
PestBlock package	Backdoor.XiaoBird.22	highest
PhotoRescue package	Downloader.Zlob.10	highest
PictureNaut package	Downloader.Zlob.10	highest
QuickStart package	Adclicker.BMF	default
QuickSurfer package	Trojan-PSW.Game.42	highest
RaBiT package	W32/Malware	default
RunWithParameters package	W32/Suspicious_U.gen	default
Scout EasyScan package	BackDoor.Danton.46	default
ShortCut package	BackDoor.NetBus.31	default
Streaming Encoder package	Trojan-Spy.xBank.6	highest
StudioLine package	Downloader.Zlob.7	highest
Symantec AV package	Downloader.Zlob.7	highest
System Safety Monitor package	Delf.BIJ	default
TDSL SpeedManager package	Generic9.SHV	default
TDSLTest package	W32/Malware	default
Termine package	VBS.Phereal	default
TrendMicro AV package	Email-Worm.Win32.LovGate.ck	default
TunePoint package	W32/Smalltroj.CQJX	default
TVgenial package	W32/Delf.AXFD	default
Typo3 package	Backdoor.Agent.78	highest
UndeletePlus package	Trojan-Spy.Banker.58	highest
USB-Access package	Adclicker.BMF	default
VideoCapture package	Backdoor.XiaoBird.32	highest
Vispa package	W32/Suspicious_U.gen	default
VitoSketchArtist package	W32/DLoader.CQU	default
VorlagenExplorer package	Trojan-Downloader.Agent.55	highest
WinBuilder package	Backdoor.Delf.180	highest
Windows Forensic Toolchest package	Embedded.Flooder.Win32.UDP.c	default
WinRAR package	Worm.Viking.5	highest
Xmpeg package	BackDoor.Danton.46	default
XPUManager package	Trojan.DownLoader.origin	default
XPupdater package	Backdoor.XiaoBird.27	highest
ZenoReader package	Backdoor.XiaoBird.57	highest

TrustPort had 105 false alarms, 74 with default (detection) settings.

**G DATA AVK**

False alarm found in some part(s) of	Detected as	Settings
Adobe Premiere package	Win32:JunkPoly	default
Batch2ExeConverter package	Win32:Shutdown-D	default
BWMeter package	Win32:Trojan-gen	default
Image Optimizer package	Win32:Nimosw-F	default
Mandrake package	Trojan-Dropper.MSWord.1Table.es	default
NOD32 AV package	Win32:Trojan-gen	default
Pioneer Driver package	Win32:Nimosw-B	default
PowerQuiz package	Win32:Delf-CKU	default
TaskManager package	Win32:Trojan-gen	default
TrafficMonitor package	Backdoor.Win32.FTP.Matiteman	default
WimUtil package	Win32:Agent-RNO	default

GDATA AVK had 11 false alarms, all with default settings.

**VBA32**

False alarm found in some part(s) of	Detected as	Settings
AktienProfi package	BackDoor.Danton.46	default
AmokPlayList package	Backdoor.XiaoBird.3	maximum
AOL ConnFix package	Trojan.PWS.Gamania	default
aReaker package	P2P-Worm.Win32.Franvir	default
Batch2ExeConverter package	OScope.Dialer.GMHA	default
BitComet package	Downloader.Zlob.8	maximum
ClamWin package	Trojan-Downloader.Win32.QQHelper.gt	default
Corel package	Exploit.Signature	default
Ebay-Rechner package	BackDoor.BOrifice.112	default
eDVarDo package	BackDoor.BOrifice.112	default
EMIS package	TR.Spy.Banco.FR.2.C	default
Erunt package	Trojan.PWS.Banker.3682	default
FritzBox package	Trojan.Click.2798	default
GeForceTweakUtility package	Unknown.Win32Virus	default
Gothic2 package	Trojan-PSW.Win32.Nilage.aer	default
HDDVDJump package	Win32.HLLW.Dbot	default
ImageEnhance package	Backdoor.XiaoBird.32	default
Imdb2Movid package	Trojan.Packed.194	default
JkDefrag package	Trojan-Downloader.Win32.AutoIt.cs	default
Kaspersky AV package	Backdoor.Win32.Agent.aro	default
LANTool package	Trojan.DownLoader.10130	default
Matroska package	Embedded.Trojan.Hanspy	default
MoViC package	BackDoor.Danton.46	default
MS InternetExplorer package	BackDoor.Danton.46	default
NZBPlayer package	Backdoor.XiaoBird.33	maximum
OfficeVorlagen package	Unknown.MacroVirus	maximum
PC Grundlagen package	BackDoor.BOrifice.112	default
PDFExperte package	Trojan.MulDrop	default
Personal Backup package	Trojan-Spy.xBank.1	maximum
Scout EasyScan package	BackDoor.Danton.46	default
StudioLine package	Downloader.Zlob.7	maximum
System Safety Monitor package	Trojan.SpamBot	default
TrendMicro AV package	Email-Worm.Win32.LovGate.ck	default
VideoCapture package	Backdoor.XiaoBird.32	maximum

Windows Forensic Toolchest package	Embedded.Flooder.Win32.UDP.c	default
Xmpeg package	BackDoor.Danton.46	default
ZenoReader package	Backdoor.XiaoBird.57	maximum

VBA32 had 37 false alarms, 29 with default settings.

## Sophos

False alarm found in some parts of	Detected as	Settings
0190Warner package	Sus/Madcode-A	suspicious
21 Solitaire package	Sus/ComPack-C	suspicious
3D UltraPong package	Sus/UnkPacker	extensive + suspicious
3D-Analyze package	Sus/Malware-B	extensive + suspicious
a2 HijackFree package	Sus/Malware-B	extensive + suspicious
ABBYY FineReader package	Sus/UnkPacker	extensive + suspicious
Acronis TrueImage package	Sus/Malware-A	extensive + suspicious
Adobe Photoshop Elements package	Sus/Parasit-A	extensive + suspicious
Advanced Encryption package	Sus/UnkPacker	extensive + suspicious
Advanced Launcher package	Sus/ComPack-C	suspicious
Advanced Process Termination package	Sus/Malware-C	suspicious
AIDA package	Sus/Malware-A	extensive + suspicious
AirSnare package	Sus/Malware-A	extensive + suspicious
AlbumToGoDesktop package	Mal/Heuri-E	extensive
AlcoholVirtualDVD package	Sus/ComPack-C	suspicious
AlienShooter package	Sus/ComPack-C	suspicious
AlleMeinePasswörter package	Mal/Packer	default
AlphaPlayer package	Sus/Dropper-A	suspicious
Altavista package	Sus/ComPack-C	suspicious
AM-Deadlink package	Sus/Malware-A	extensive + suspicious
AmoK DVDShrinker package	Mal/Packer	default
Anno 1701 package	Sus/Malware-B	extensive + suspicious
Anonymizer package	Mal/Behav-053	default
Anti-Spy package	Sus/ComPack-C	suspicious
AnyPassword package	Sus/ComPack-C	suspicious
Anytime package	Sus/ComPack-C	suspicious
AOL Optimized DialIn package	Sus/Behav-1015	extensive + suspicious
AOL2POP3 package	Sus/Malware-B	extensive + suspicious
ApplicationAccessServer package	Mal/Heuri-D	default
ArchiCryptX package	Sus/ComPack-C	suspicious
AsteriskPasswordRecovery package	Sus/ComPack-E	suspicious
Aston package	Sus/ComPack-C	suspicious
ASUS Digital VCR package	Sus/Malware-B	extensive + suspicious
AttachmentSecurity package	Sus/UnkPacker	extensive + suspicious
Auctionaut package	Sus/Malware-B	extensive + suspicious
AuctionTamer package	Sus/Malware-B	extensive + suspicious
AudioCD Ripper package	Sus/ComPack-C	suspicious
AudioConverter package	Sus/ComPack-C	suspicious
AudioTags package	Sus/ComPack-C	suspicious
Auktionsverwalter package	Sus/Malware-B	extensive + suspicious
Auralog package	Sus/Behav-1021	suspicious
AutoDialUp package	Sus/Malware-B	extensive + suspicious
AutoFeedback package	Sus/Malware-B	extensive + suspicious
AuWatch package	Sus/Malware-B	extensive + suspicious

AVG AV package	Sus/Malware-C	extensive + suspicious
AVI Joiner package	Sus/ComPack-C	suspicious
AVIedit package	Sus/ComPack-C	suspicious
Backup package	Sus/Malware-B	extensive + suspicious
BandwidthController package	Sus/ComPack-C	suspicious
Batch2Exe Converter package	Sus/Dropper-A	suspicious
BatMon package	Sus/Malware-A	extensive + suspicious
BattlestarGalactica package	Sus/Malware-B	extensive + suspicious
BC package	Sus/Malware-B	extensive + suspicious
Bertelsmann Lexikon package	Sus/Behav-1018	suspicious
Bewerbungsmaster package	Mal/Behav-109	extensive
Bikerace package	Sus/ComPack-D	extensive + suspicious
BIOSAgent package	Sus/ComPack-C	suspicious
BitComet package	Sus/UnkPacker	extensive + suspicious
Blaze MediaConvert package	Sus/Malware-A	suspicious
BlueFritz Driver package	Sus/Behav-1013	extensive + suspicious
BOClean package	Sus/Malware-A	extensive + suspicious
BootStrapper package	Sus/Malware-B	extensive + suspicious
Borland Debugger package	Sus/Malware-B	extensive + suspicious
Brother Driver package	Sus/Behav-1014	extensive + suspicious
Bukster package	Sus/Malware-A	extensive + suspicious
Burn4Free package	Sus/UnkPacker	extensive + suspicious
ByteMobile package	Sus/Malware-B	extensive + suspicious
Canon Driver package	Sus/Behav-1013	extensive + suspicious
CCleaner package	Sus/Behav-1001	suspicious
CD ImageConverter package	Sus/ComPack-D	extensive + suspicious
CE Zebra package	Sus/Malware-A	extensive + suspicious
CFMinibar package	Mal/Reload-A	default
ChipInfo package	Sus/Dropper-A	suspicious
ClamWin package	Sus/Behav-1021	suspicious
CleanRAM package	Sus/ComPack	suspicious
ClipboardRecorder package	Sus/Behav-1011	extensive + suspicious
ClipInc3 package	Sus/Malware-B	extensive + suspicious
CodeStuff package	Sus/Malware-A	suspicious
Colin McRae Rally package	Sus/UnkPacker	extensive + suspicious
CommanderWin package	Sus/ComPack-D	extensive + suspicious
CompuServe package	Sus/UnkPacker	suspicious
ConnectionWatch package	Sus/ComPack-E	suspicious
CopyHandler package	Sus/UnkPacker	extensive + suspicious
Creative Driver package	Sus/Malware-A	extensive + suspicious
CryptoCrat package	Sus/UnkPacker	extensive + suspicious
Cubase VST32 package	Sus/ComPack-C	suspicious
CyberCorder package	Sus/Malware-A	suspicious
Daemon package	Sus/Behav-1005	suspicious
DAXChart package	Mal/Heuri-E	extensive
Decoder package	Sus/Behav-1018	suspicious
DeepBurner package	Sus/Malware-A	suspicious
DefendGate package	Sus/Malware-B	extensive + suspicious
Defrag package	Sus/ComPack-C	suspicious
DeltaForce LandWarrior package	Sus/ComPack-C	suspicious
DeskKit package	Sus/Malware-B	extensive + suspicious
DesktopIconManager package	Sus/Malware-B	extensive + suspicious
DigiBook package	Sus/Behav-1015	extensive + suspicious

DiManage package	Sus/Malware-B	extensive + suspicious
DivX package	Mal/HckPk-D	default
dotWidget package	Sus/MzEntry-A	extensive + suspicious
Dr.Hardware package	Sus/MzEntry-A	extensive + suspicious
Dr.Hobby package	Sus/MzEntry-A	extensive + suspicious
DriveCrypt package	Sus/ComPack-C	suspicious
DrWeb AV package	Sus/Malware-A	extensive + suspicious
Duden Korrektor package	Sus/UnkPacker	extensive + suspicious
DUN package	Sus/DelpDldr-A	suspicious
DVD Identifier package	Sus/ComPack-B	extensive + suspicious
DVDRegionFree package	Sus/ComPack-C	suspicious
DVDRipper package	Sus/ComPack-C	suspicious
DyCE IM package	Sus/ComPack-C	suspicious
Easy MP3Mover package	Sus/ComPack-C	suspicious
EasyCDExtractor package	Sus/UnkPacker	extensive + suspicious
EasyScreenRecorder package	Sus/Behav-113	suspicious
Ebaycheck package	Sus/Malware-B	extensive + suspicious
EF Commander package	Sus/ComPack-C	suspicious
eJay package	Sus/UnkPacker	extensive + suspicious
El Matador package	Sus/UnkPacker	extensive + suspicious
ElsterFormular package	Sus/ComPack-C	suspicious
Email Address Validator package	Sus/ComPack-C	suspicious
EMIS package	Mal/Emogen-B	extensive
Enfish Find package	Sus/Malware-B	extensive + suspicious
EP ProcessManager package	Sus/ComPack-C	suspicious
Epson Driver package	Sus/Behav-1014	extensive + suspicious
eSan Audio package	Sus/Malware-B	suspicious
etopeLister package	Sus/Malware-B	extensive + suspicious
eTrust AV package	Sus/Malware-B	extensive + suspicious
Everest package	Sus/Malware-B	extensive + suspicious
EvilPlayer package	Sus/Malware-B	extensive + suspicious
Explorer2000 package	Sus/ComPack-C	suspicious
ExtractOnlinezeit package	Sus/DelpDldr-A	extensive + suspicious
FavMan package	Sus/Malware-B	extensive + suspicious
FeedReader package	Sus/Malware-A	extensive + suspicious
FileSharing Sentinel package	Mal/Emogen-M	default
FileShredder package	Sus/Malware-B	suspicious
FileZilla package	Sus/Behav-1021	suspicious
FinePrint package	Sus/Malware-B	extensive + suspicious
FireTune package	Sus/ComPack-C	suspicious
FlashSaver package	Sus/Malware-B	extensive + suspicious
Flying Picture package	Sus/ComPack-C	suspicious
FotoColor package	Sus/Malware-B	extensive + suspicious
FreshDiagnose package	Sus/Malware-A	extensive + suspicious
FreshDownload package	Sus/Malware-A	extensive + suspicious
F-Secure AV package	Sus/Malware-C	extensive + suspicious
FSM package	Sus/Malware-A	extensive + suspicious
GeMail package	Sus/Malware-B	extensive + suspicious
GenoPro package	Sus/Behav-1014	extensive + suspicious
Gentleman package	Sus/ComPack-C	suspicious
GenTrain package	Sus/Malware-B	extensive + suspicious
GeoShell package	Sus/Behav-1014	extensive + suspicious
GetThePictures package	Sus/Malware-B	extensive + suspicious



GFA package	Sus/Malware-B	extensive + suspicious
GIF Animator package	Sus/ComPack-E	suspicious
GoogleDesktopSearch package	Sus/Malware-B	extensive + suspicious
GoogleMonitor package	Sus/ComPack-C	suspicious
GoOnline package	Sus/ComPack-C	suspicious
Gothic2 package	Sus/Malware-C	extensive + suspicious
gPhotoShow package	Sus/UnkPacker	extensive + suspicious
HardwareTuning Spezialist package	Sus/ComPack-C	suspicious
Hauppauge Driver package	Sus/ComPack-C	suspicious
HD Speed package	Sus/UnkPacker	extensive + suspicious
HDDTemperature package	Sus/ComPack-C	suspicious
Hmonitor package	Sus/ComPack-B	extensive + suspicious
Home-Box package	Sus/UnkPacker	extensive + suspicious
HookExplorer package	Sus/Malware-B	extensive + suspicious
HotChime package	Sus/UnkPacker	suspicious
HP Driver package	Sus/UnkPacker	extensive + suspicious
HP ScanManager package	Sus/Malware-C	extensive + suspicious
HyperCam package	Sus/Malware-A	suspicious
HyperMaker package	Sus/ComPack-D	extensive + suspicious
HyperSnap package	Sus/Malware-A	suspicious
iAudio package	Sus/ComPack-C	suspicious
IB Manager package	Sus/ComPack-C	suspicious
IDA package	Sus/Malware-A	extensive + suspicious
ImageRecovery package	Sus/ComPack-C	suspicious
ImageTrace package	Sus/Malware-A	extensive + suspicious
Impulsiv package	Sus/UnkPacker	extensive + suspicious
InstantSearch package	Sus/ComPack-C	suspicious
InternetSammmler package	Sus/Behav-1014	extensive + suspicious
InternetTV package	Sus/ComPack-D	extensive + suspicious
iPing package	Sus/UnkPacker	extensive + suspicious
IPMonitor package	Sus/Malware-B	extensive + suspicious
iPod2PC package	Sus/Malware-B	extensive + suspicious
ipX package	Sus/Malware-B	extensive + suspicious
IrfanView package	Sus/Malware-A	extensive + suspicious
Jamt package	Sus/Malware-B	extensive + suspicious
Joshuas-PreShell package	Sus/Malware-A	suspicious
JovaKonto package	Sus/UnkPacker	suspicious
JPEG Imager package	Sus/ComPack	suspicious
Jugglor package	Sus/Malware-B	suspicious
Junkanoo package	Sus/Malware-B	extensive + suspicious
Jyve package	Sus/Malware-A	extensive + suspicious
Kalah package	Sus/UnkPacker	extensive + suspicious
KillBox package	Sus/Malware-B	suspicious
KlipFolio package	Sus/Malware-C	extensive + suspicious
KomaMail package	Sus/Malware-B	extensive + suspicious
Konvertor package	Sus/ComPack-C	suspicious
LANTool package	Sus/Malware-B	extensive + suspicious
Lauge package	Sus/Malware-B	extensive + suspicious
Lazyputs package	Sus/UnkPacker	extensive + suspicious
LEGO Star Wars package	Sus/UnkPacker	extensive + suspicious
Leserbefragung package	Sus/Parasit-A	suspicious
Lexmark Driver package	Sus/Behav-1014	extensive + suspicious
LimeWire package	Sus/ComPack-C	suspicious

LinkGenerator package	Sus/ComPack-D	extensive + suspicious
ListLeaf package	Sus/Malware-B	extensive + suspicious
LittleBigBar package	Sus/DelpDldr-A	extensive + suspicious
LockMyPC package	Sus/ComPack-C	suspicious
LogiTech Driver package	Sus/Behav-1018	suspicious
LottoFee package	Sus/Malware-B	extensive + suspicious
Macromedia Flash package	Sus/Behav-1011	extensive + suspicious
MailBell package	Sus/Malware-B	extensive + suspicious
Mandrake package	Sus/DOSCom-A	extensive + suspicious
Marcellinos Restaurant package	Sus/ComPack-D	extensive + suspicious
Matrox Driver package	Sus/Dropper-A	extensive + suspicious
MaulwurfsMover package	Mal/Packer	default
McAfee AV package	Sus/DelpDldr-A	extensive + suspicious
McAfee PatchScanner package	Sus/Malware-A	extensive + suspicious
Media Wizard package	Sus/Malware-A	suspicious
Medion Driver package	Sus/UnkPacker	suspicious
Messenger Lite package	Sus/Malware-B	extensive + suspicious
Miranda package	Mal/EncPk-BW	default
Morse Pilot package	Sus/UnkPacker	suspicious
MountImagePro package	Sus/Malware-A	suspicious
MP3 Rightname package	Sus/Dropper-A	suspicious
MP3Juke package	Sus/ComPack-C	suspicious
MP3Man package	Sus/DelpDldr-A	suspicious
MP3Tag package	Sus/Malware-B	extensive + suspicious
MP3vergleich package	Sus/ComPack-D	extensive + suspicious
MS Base Cryptographic Provider package	Mal/Packer	default
MS CodeDownload package	Sus/Malware-B	extensive + suspicious
MS Forefront package	Sus/Behav-1014	extensive + suspicious
MS Identity Integration Server package	Sus/GamerPSW-A	extensive + suspicious
MS Messenger package	Sus/Parasit-A	extensive + suspicious
MS OfficeProfessional2001 package	Sus/Behav-1014	extensive + suspicious
MS OneCare package	Sus/Malware-B	extensive + suspicious
MS OutlookExpress package	Sus/Behav-1014	extensive + suspicious
MS TV Viewer package	Sus/Behav-1014	extensive + suspicious
MS Windows NT4 SP3 package	Sus/Malware-B	extensive + suspicious
MS Windows NT4 SP5 package	Sus/Malware-B	extensive + suspicious
MS Windows2000 Q285156 update package	Sus/UnkPacker	extensive + suspicious
MS Windows2000 Q285851 update package	Sus/UnkPacker	extensive + suspicious
MS Windows2000 Q296185 update package	Sus/UnkPacker	extensive + suspicious
MS WindowsXP Hotfix Q307969 package	Sus/UnkPacker	extensive + suspicious
MusicBase package	Sus/ComPack-C	suspicious
MusicMatch package	Sus/Behav-1014	extensive + suspicious
myHTPC package	Sus/Malware-B	extensive + suspicious
MyIE package	Mal/Emogen-P	extensive
NeoBookPlayer package	Sus/Malware-A	extensive + suspicious
Nero package	Sus/ComPack-C	suspicious
NetNak package	Sus/ComPack-C	suspicious
NetStat package	Sus/Madcode-A	suspicious
NetTransport package	Sus/UnkPacker	suspicious
Ngrep package	Sus/UnkPacker	suspicious
NoRightClick package	Sus/ComPack-C	suspicious
Norton AV package	Sus/Malware-B	extensive + suspicious
NSIS package	Sus/Dropper-A	extensive + suspicious

NTI CD Maker package	Sus/Behav-1014	extensive + suspicious
NVidia Driver package	Sus/Behav-1014	extensive + suspicious
OnlineCounter package	Sus/Behav-1014	extensive + suspicious
OnlineOptimizer package	Sus/ComPack-D	extensive + suspicious
OperationCenter package	Sus/ComPack-D	extensive + suspicious
Outpost Pro package	Sus/ComPack-C	suspicious
Panda Anti-Rootkit package	Sus/Malware-B	extensive + suspicious
Panda AV package	Sus/Malware-B	extensive + suspicious
Panda TruPrevent package	Sus/Madcode-A	suspicious
PC SecurityTest package	Mal/Behav-053	default
PC Telephone package	Sus/ComPack-D	extensive + suspicious
PC Wizard package	Sus/Behav-1021	suspicious
PC-Lock package	Sus/Malware-C	extensive + suspicious
PCRecall package	Sus/ComPack-C	suspicious
PD Protector package	Sus/Malware-A	extensive + suspicious
PDA Benchmark package	Sus/Malware-A	extensive + suspicious
PDF2Word package	Sus/Malware-A	extensive + suspicious
PEiD package	Sus/Malware-A	extensive + suspicious
PerfectMenu package	Sus/ComPack-C	suspicious
PersonalBackup package	Sus/Malware-B	extensive + suspicious
Photo Wizard package	Sus/UnkPacker	extensive + suspicious
PhotoResizer package	Sus/ComPack-C	suspicious
PhotoWatermark package	Sus/ComPack-B	extensive + suspicious
PictureBase package	Sus/ComPack-C	suspicious
PlacemarkManager package	Mal/Behav-010	default
Pluz package	Sus/UnkPacker	extensive + suspicious
PodPlayer package	Sus/ComPack-B	extensive + suspicious
PodTools package	Mal/Packer	default
PopURL package	Mal/Heuri-D	default
PowerClick package	Sus/Malware-A	extensive + suspicious
PowerShrink package	Sus/Malware-A	suspicious
PowerVR RegistryUtility package	Sus/Behav-1014	extensive + suspicious
PrimoPDF package	Sus/UnkPacker	extensive + suspicious
PrivacyInspector package	Sus/Malware-B	suspicious
ProactiveSecurityAuditor package	Sus/ComPack-C	suspicious
ProcessGuard package	Sus/Malware-B	extensive + suspicious
Profan package	Sus/DOSCom-A	extensive + suspicious
PSM Firewall package	Sus/Madcode-A	suspicious
QuickTime package	Sus/Parasit-A	extensive + suspicious
Radar WebsiteMonitor package	Sus/Malware-B	extensive + suspicious
RAIDE package	Sus/ComPack-C	suspicious
RainMeter package	Mal/Heuri-E	extensive
RAM Idle package	Sus/Behav-1014	extensive + suspicious
RauchRechner package	Sus/Malware-A	extensive + suspicious
Reach-a-Mail package	Sus/Malware-B	extensive + suspicious
ReGet package	Sus/ComPack-C	suspicious
RegistryClean package	Sus/ComPack-C	suspicious
RegSeeker package	Sus/Malware-A	extensive + suspicious
Remind package	Sus/ComPack-C	suspicious
RFactor package	Sus/Behav-1018	suspicious
RootkitUnhooker package	Mal/EncPk-C	default
Rose PEHead package	Mal/Packer	default
Rose Utilities package	Sus/Malware-C	extensive + suspicious

Router Syslog package	Mal/Packer	default
RouterControl package	Sus/Malware-A	extensive + suspicious
RunWithParameters package	Mal/Packer	default
Sandboxie package	Sus/Malware-B	extensive + suspicious
SanDisk Driver package	Sus/Behav-1014	extensive + suspicious
Sateira package	Sus/ComPack-C	suspicious
Save2FTP package	Sus/Malware-B	extensive + suspicious
ScreenshotCaptor package	Sus/ComPack-B	extensive + suspicious
SearchMyDisks package	Sus/ComPack-C	suspicious
Security Taskmanager package	Sus/Malware-A	extensive + suspicious
SeriousSam package	Sus/UnkPacker	extensive + suspicious
Settler package	Mal/Packer	default
SFS package	Sus/ComPack-B	extensive + suspicious
Shareholder package	Sus/Malware-A	extensive + suspicious
Simple FileShredder package	Sus/Malware-A	extensive + suspicious
Sis Driver package	Sus/Behav-1014	extensive + suspicious
Sizer package	Sus/Malware-A	extensive + suspicious
SlimXP package	Sus/UnkPacker	extensive + suspicious
SmartStore package	Sus/UnkPacker	extensive + suspicious
SoundControl package	Sus/UnkPacker	extensive + suspicious
SpeedCommander package	Sus/ComPack-C	suspicious
SpeeDefrag package	Mal/Emogen-M	default
Spellforce package	Sus/Malware-B	extensive + suspicious
Spirex package	Sus/UnkPacker	extensive + suspicious
Splitting package	Sus/ComPack-B	extensive + suspicious
Spybot FileLocator package	Sus/Malware-B	extensive + suspicious
SpyBotSD package	Sus/Malware-B	extensive + suspicious
StartPatrol package	Sus/ComPack-C	suspicious
StrokeIt package	Sus/Malware-B	extensive + suspicious
SuperCopier package	Sus/Madcode-A	suspicious
SuperMailer package	Sus/Malware-B	extensive + suspicious
SuperSpamKillerPro package	Sus/Malware-B	extensive + suspicious
SyncBack package	Sus/Malware-B	extensive + suspicious
SyncExpert package	Sus/ComPack-B	extensive + suspicious
SystemInformationViewer package	Sus/Malware-B	extensive + suspicious
TagScanner package	Sus/Malware-B	extensive + suspicious
TaskTracker package	Sus/Malware-B	extensive + suspicious
Tauscan package	Sus/ComPack-C	suspicious
Telefonbuch package	Sus/ComPack-C	suspicious
Texefex package	Sus/ComPack-C	suspicious
ThaiTrainer package	Sus/Malware-B	suspicious
The Punic Wars package	Sus/UnkPacker	extensive + suspicious
TheWitcher package	Sus/Malware-B	extensive + suspicious
ThumbView package	Sus/ComPack-C	suspicious
TinyHexer package	Sus/Malware-B	extensive + suspicious
TippGenerator package	Mal/Heuri-E	extensive
T-Online package	Sus/Malware-A	extensive + suspicious
ToolWorks package	Sus/Malware-A	suspicious
Tor package	Sus/Malware-B	extensive + suspicious
TorrentSpy package	Sus/Malware-A	extensive + suspicious
Total Text Container package	Sus/Behav-1021	suspicious
TotalCommander package	Sus/MzEntry-A	extensive + suspicious
TransXP package	Sus/Behav-1021	suspicious

TraxTime package	Sus/Malware-A	suspicious
TrendMicro AV package	Sus/Dropper-A	extensive + suspicious
Trust Driver package	Sus/Behav-1014	extensive + suspicious
TuneUp Utilities package	Sus/Madcode-A	suspicious
TV Plugin package	Mal/Heuri-D	default
TVGenial package	Sus/Malware-A	extensive + suspicious
TweakVista package	Sus/UnkPacker	extensive + suspicious
Uli Driver package	Sus/Behav-1014	extensive + suspicious
UltimateSudoku package	Sus/Malware-A	suspicious
Undisker package	Sus/ComPack-C	suspicious
UnHackMe package	Sus/ComPack-C	suspicious
Universal Mobile Messenger package	Sus/Malware-A	extensive + suspicious
UPACK compression tool package	Mal/EncPk-BW	default
USB Access package	Sus/Behav-166	suspicious
USBDM package	Sus/Malware-B	extensive + suspicious
USBTray package	Sus/Malware-B	extensive + suspicious
Useful File Utilities package	Sus/ComPack-C	suspicious
User Notice Creator package	Mal/Emogen-M	default
Vallen POP3-Checker package	Sus/Malware-B	extensive + suspicious
Vanderlee package	Sus/ComPack-D	extensive + suspicious
Via Driver package	Sus/Behav-1014	extensive + suspicious
Video2Brain package	Sus/Parasit-A	suspicious
Vinyl Driver package	Sus/Behav-1014	extensive + suspicious
VirtualForensicComputing package	Sus/Malware-A	suspicious
VisionGS package	Sus/ComPack-C	suspicious
Vispa package	Mal/EncPk-C	default
VistaDemo package	Sus/Malware-B	suspicious
VMwareACE package	Sus/UnkPacker	extensive + suspicious
VobDec package	Sus/UnkPacker	suspicious
VS2000GUI package	Sus/DelpDldr-A	suspicious
WasherPro package	Sus/ComPack-C	suspicious
WebEffects package	Sus/ComPack-D	extensive + suspicious
WebsiteArchive package	Sus/Malware-A	extensive + suspicious
WebSpamBlocker package	Sus/Malware-B	extensive + suspicious
WengoPhone package	Sus/Behav-1011	extensive + suspicious
Wido package	Sus/Malware-B	extensive + suspicious
Windows XP Optimizer package	Sus/Behav-1014	extensive + suspicious
WinForensic Toolchest package	Sus/Malware-B	extensive + suspicious
WinLock package	Sus/ComPack-C	suspicious
WinMailBackup package	Sus/Malware-B	extensive + suspicious
WinMHT package	Sus/Malware-A	extensive + suspicious
WinPlosion package	Sus/ComPack-C	suspicious
WiseRegistryCleaner package	Sus/Malware-B	extensive + suspicious
WISOMeinGeld package	Sus/Malware-B	extensive + suspicious
WissenLexikon package	Mal/Behav-109	extensive
World of Warcraft package	Sus/GamerPSW-A	extensive + suspicious
WormRadar package	W32/Deadhat-A	default
WTRate package	Sus/ComPack-C	suspicious
Xmailer package	Sus/Malware-B	extensive + suspicious
XMPlay package	Sus/ComPack-D	extensive + suspicious
XP Konfig package	Sus/Malware-B	suspicious
Xpage package	Sus/ComPack-C	suspicious
XPclean package	Sus/Malware-B	extensive + suspicious

XPE package	Mal/Emogen-Y	default
XPlite package	Sus/Malware-B	suspicious
XPTweaker package	Mal/Packer	default
ZoneAlarm package	Sus/Malware-B	extensive + suspicious
ZVolumne package	Sus/UnkPacker	extensive + suspicious
Zwrang package	Sus/ComPack-C	suspicious

Sophos had in total about 400 false alarms, but "only" 27 with default settings. Nearly all false alarms were "Sus" detections, usually on files packed by unusual packers. Please read the blog post<sup>8</sup> of Sophos which explains their "Sus/" detections. Note:

- a) this is the first time that Sophos participates in our false alarm test and therefore it may show more false alarms than other products (because after each false alarm test the vendors get the files which caused the false alarm) and
- b) Sophos products are mainly for corporates/enterprises, which systems are managed by Administrators (which should know the difference between a false alarm and a real threat) and where rarely new software gets installed - when a suspicious application is found, Sophos issues an alert and the user/administrator decides what to do with it.

Activating the Sophos "suspicious file" detection (or HIPS<sup>9</sup>) will increase the malware detection rates (as can be seen in this report), but will also cause false alarms. Home users (which usually can not distinct a false alarm from real malware) which use Sophos Anti-Virus should keep this in mind and in unsure cases contact Sophos and submit the suspicious file (false alarms should be submitted to any vendor of the product used by the user, in order that it can be fixed as soon as possible by the Anti-Virus vendors). With default settings (without extensive and suspicious detections), Sophos would score ~39% and get a 'STANDARD' rating.

**Where to submit possible false alarms** (in those cases, add e.g. "False alarm" in the subject and give to the vendors as many details as possible, like signature version, URL to original file, etc.):

avast!	virus@avast.com
AVG	virus@grisoft.cz
AVIRA	http://analysis.avira.com
BitDefender	virus_submission@bitdefender.com
ESET NOD32	samples@eset.com
F-Secure	samples@f-secure.com
Kaspersky	newvirus@kaspersky.com
McAfee	vsample@avertlabs.com
Microsoft	avsubmit@submit.microsoft.com
Norman	analysis@norman.no
Sophos	samples@sophos.com
Symantec	avsubmit@symantec.com
VBA32	newvirus@anti-virus.by

eScan uses the Kaspersky engine, GDATA AVK uses the avast! and Kaspersky engine and Trustport uses the Norman, Dr.Web, VBA32 and AVG engines. Try to find out which engine caused the false alarm and send the file directly to the respective vendors.

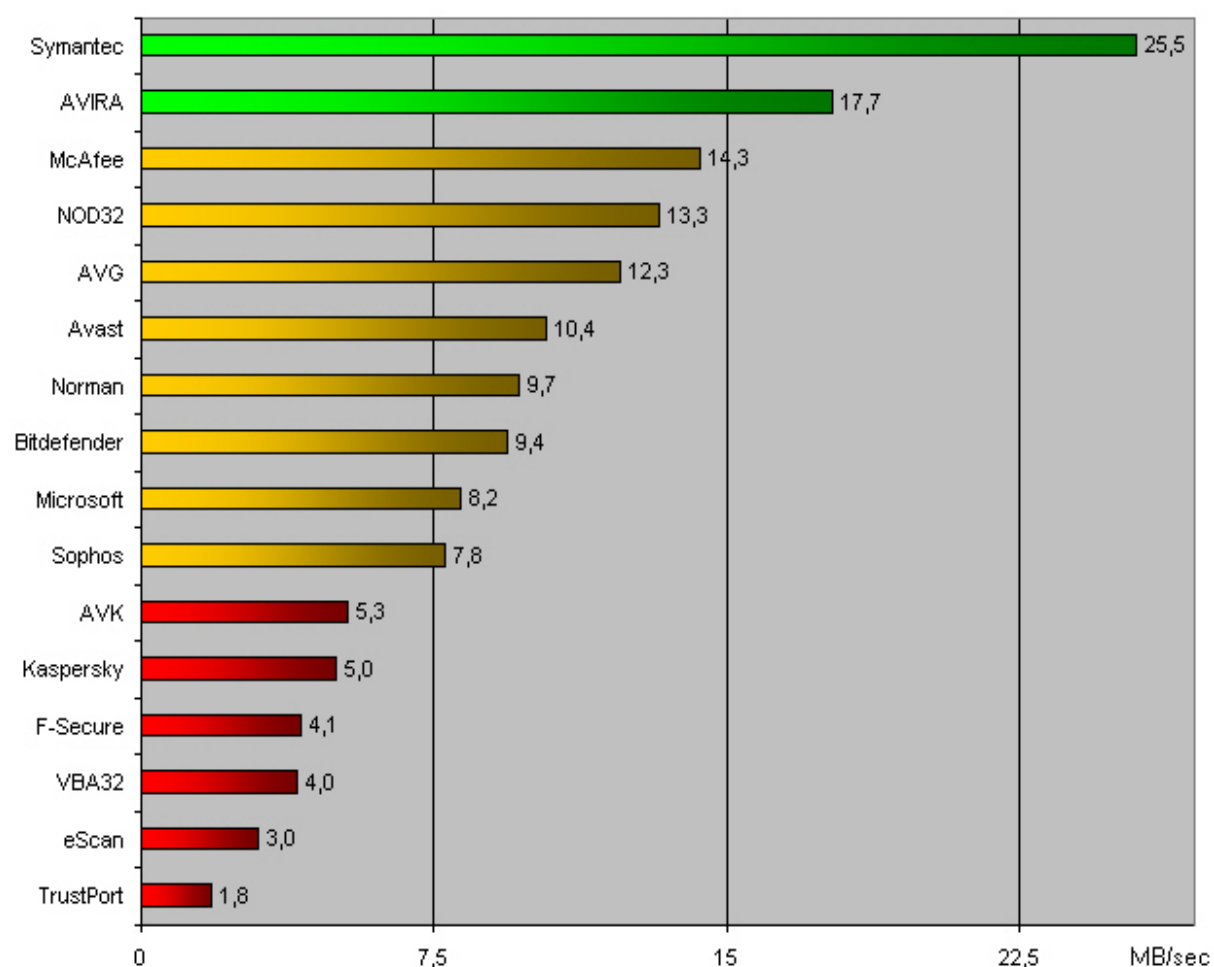
<sup>8</sup> <http://www.sophos.com/security/blog/2008/05/1324.html>

<sup>9</sup> this rule applies to most products with similar technologies

## 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) with best settings. The scanning throughput rate will vary based on the set of clean files<sup>10</sup>, the settings 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 and hardware used etc.




The scanning speed tests were done under Windows XP SP2, on a Intel Core 2 Extreme QX6800EE 2,66 GHz PC, ASUS P5W WS Pro, 4096 MB DDR2-1150 RAM, SATA II disks and without network connection.

All tested products were able to scan the whole set of clean files without problems.

<sup>10</sup> to know how fast the various products would be on *your* PC at scanning *your* files, try yourself the products

## 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>
	AVIRA NOD32
	AVG McAfee Microsoft AVK
	BitDefender* Norman* Avast* Kaspersky VBA32* Symantec
no certification	Sophos* TrustPort* F-Secure eScan

*\*: Products with "many" false alarms do not deserve the proactive detection level they would fall in. Avast, BitDefender, Norman, Sophos, Trustport and VBA32 got penalized according to the new award system below:*

	0-10%	10-25%	25-50%	50-100%
none - few	NO AWARD	STANDARD	ADVANCED	ADVANCED+
many	NO AWARD	NO AWARD	STANDARD	ADVANCED
very many	NO AWARD	NO AWARD	NO AWARD	NO AWARD

Normal 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 product which is more prone to false alarms than other products.

*Note: Many vendors (like e.g. Bitdefender, F-Secure, Kaspersky, McAfee, Microsoft, Sophos, Symantec, etc.) include in their products behavior-based/HIPS-like solutions which work when malware is executed. Such kind of proactive protection features will be included in our evaluations of 2009.*



**8. Copyright and Disclaimer**

This publication is Copyright (c) 2008 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of Andreas Clementi, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

Andreas Clementi, AV-Comparatives (May 2008)