

Anti-Virus Comparative
No. 21, February 2009



**On-demand Detection of
Malicious Software**

includes false alarm and on-demand scanning speed test

Language: English

February 2009

Last Revision: 2009-03-21

www.av-comparatives.org

Table of Contents



Tested Products	3
Conditions for participation and test methodology	4
Tested product versions	4
Comments	5
Test results	7
Graph of missed samples	9
Summary results	10
False positive/alarm test	11
Scanning speed test	23
Award levels reached in this test	24
Copyright and Disclaimer	25



Tested Products

- avast! Professional Edition 4.8
- AVG Anti-Virus 8.0
- AVIRA AntiVir Premium 8.2
- BitDefender Anti-Virus 2009
- Command Anti-Malware 5.0.8
- eScan Anti-Virus 10.0
- ESET NOD32 Antivirus 3.0
- F-Secure Anti-Virus 2009
- G DATA AntiVirus 2009
- Kaspersky Anti-Virus 2009
- Kingsoft AntiVirus 2009
- McAfee VirusScan Plus 2009
- Microsoft Live OneCare 2.5
- Norman Antivirus & Anti-Spyware 7.10
- Sophos Anti-Virus 7.6.4
- Symantec Norton Anti-Virus 2009
- Trustport Antivirus 2.8

Conditions for participation and test methodology

The conditions for participation in our tests are listed in the methodology document at <http://www.av-comparatives.org/seiten/ergebnisse/methodology.pdf>. Before proceeding with this report, readers are advised to first read the above-mentioned document.

Products included in our tests constitute already some very good anti-virus software with relatively high on-demand detection rates, as this is one of the requirements needed to be included in our tests. The participation is limited to 16-18 well-known and worldwide used quality anti-virus products with high detection rates, which vendors agreed to get tested and included in this public report.

Only vendors which detected more than 97% of the Test-Set A (April 06 to April 08) have been included in this comparative. New included and qualified participants are Authentium and Kingsoft.

Tested Product Versions

The Malware sets and system Test-beds were frozen at the beginning of February 2009. All products were updated on the 9th February 2009.

The following 17 products were included in this public test:

- avast! Professional Edition 4.8.1335
- AVG Anti-Virus 8.0.234
- AVIRA AntiVir Premium 8.2.0.374
- BitDefender Anti-Virus 12.0.11.4
- Command Anti-Malware 5.0.8
- eScan Anti-Virus 10.0.946.341
- ESET NOD32 Antivirus 3.0.684.0
- F-Secure Anti-Virus 9.00.149
- G DATA AntiVirus 19.1.0.0
- Kaspersky Anti-Virus 8.0.0.506a
- Kingsoft AntiVirus 2008.11.6.63
- McAfee VirusScan Plus 13.3.117
- Microsoft Live OneCare 2.5.2900.20
- Norman Antivirus & Anti-Spyware 7.10.02
- Sophos Anti-Virus 7.6.4
- Symantec Norton Anti-Virus 16.2.0.7
- Trustport Antivirus 2.8.0.3011

Some products may offer additional options/features e.g. to provide additional protection against malware during its execution (if not detected in advance on-access or on-demand).

Please try the products on your own system before making a purchase decision based on these tests. There are also some other program features and important factors (e.g. price, ease of use/management, compatibility, graphical user interface, language, update frequency, HIPS / behaviour blocker functions, etc.) to consider.

Although extremely important, the detection rate of a product is only one aspect of a complete Anti-Virus product. AV-Comparatives will provide this year also a full product (proactive and normal) dynamic test report, as well as other test reports which cover different aspects/features of the products.

Comments

As almost all products run nowadays in real life with highest protection settings by default or switch automatically to highest settings in case of a detected infection, we tested all products with highest settings (except Sophos). Below are some notes about the used settings (scan of all files etc. is always enabled) and some technologies which need to be explained:

- avast:** runs (in case of an infection) by default automatically with highest settings.
- AVG:** runs with highest settings by default.
- AVIRA:** runs with medium heuristic by default and not all extended categories enabled. AVIRA asked already last year to get tested with all extended categories enabled and with heuristic set to high. Due to that, we recommend users to consider also setting the heuristics to high.
- BitDefender:** runs with highest settings by default.
- Command:** runs with high heuristic by default (which is also the recommended highest setting according to Authentium). Command has also maximum heuristic mode, but it is not recommended to enable it (due to too many false alarms).
- eScan:** runs with highest settings by default.
- ESET:** runs with highest settings (webfilter) by default.
- F-Secure:** runs with highest on-demand scan settings by default.
- G DATA:** runs (depending from hardware) with highest settings by default.
- Kaspersky:** runs with low heuristic setting by default. Kaspersky asked already last year to get tested with heuristics set to high. Due to that, we recommend users to consider also setting the heuristics to high.
- Kingsoft:** runs with highest settings by default.
- McAfee:** In McAfee's Consumer product Artemis Technology is called Active Protection and it is enabled by default and only if an Internet connection is available. The Internet is the most prevalent infection vector so the test results with an Internet connection represent the capabilities to detect incoming malware more realistically. Artemis was tested at the same time as other products were updated so it did not have any time advantage over other products. The Artemis Technology sends out short fingerprints of suspicious files without any Personally Identifiable Information. Artemis currently provides almost instantaneous protection in addition to McAfee's DAT updates for the most prevalent malware. McAfee updates how Artemis detects malware via its DAT signatures.

- Microsoft:** runs with highest settings by default.
- Norman:** runs with highest settings by default.
- Sophos:** runs without suspicious detection by default. Sophos (a product for enterprises) asked already months ago to get this year tested and awarded based on its default settings. For informational purposes, we noted also the results with highest settings (suspicious detection enabled etc.).
- Symantec:** runs with automatic heuristic by default. Symantec asked already last year to get tested with heuristic set to advanced, although it made practically no difference. Anyway, we recommend users to consider also setting the heuristic to advanced.
- TrustPort:** asked already last year to get tested with highest settings with two enabled engines (AVG and Norman), like used while scanning in the background (on-access).

Test Results

In this test we were more selective than during previous tests - only vendors which detected more than 97% of the Test-Set A (April 06 to April 08) have been included in this comparative.

Getting high awards is now harder, because now the Awards are based on the detection rates over Set-B only, which contains malware from the last nine months (May 08 to the beginning of February 09). In this case the detection rates (percentages) may look lower than during previous tests, where we counted the overall rating based on both Set A and Set B (where Set A is well covered by almost all vendors). Furthermore, False Alarms starting from this test will lower Award levels. Lower awards do not mean that the products are getting worse – in fact they all improved a lot, here an example: in this test Kingsoft has 85% (based on SET B only). If it were counted as in previous years (SET A + SET B), Kingsoft would have had about 92%.

Tables of Results

Company	AVIRA	Alwil Software	AVG Technologies	BitDefender
Product	AntiVir Premium	avast! Professional	AVG Anti-Virus	BitDefender AV
Program version	8.2.0.374	4.8.1335	8.0.234	12.0.11.4
Engine / signature version	8.02.00.76/7.01.01.248	090209-0	270.10.19/1941	N/A
Award reached in this test	ADVANCED	ADVANCED	STANDARD	ADVANCED
Number of false positives*	many	many	many	many
On-demand scanning speed*	average	fast	slow	slow
DETECTION RATES:				
SET A (Apr06 - Apr08)	1.820.238	PASSED	PASSED	PASSED
SET B (May08-Jan09):				
Windows viruses	24.476	24.459 99,9%	24.346 99,5%	23.831 97,4%
Macro viruses	2.492	2.480 99,5%	2.478 99,4%	2.278 91,4%
Script malware	8.811	8.717 98,9%	8.495 96,4%	3.740 42,4%
Worms	53.326	53.202 99,8%	52.655 98,7%	50.962 95,6%
Backdoors/Bots	253.892	253.232 99,7%	249.199 98,2%	244.363 96,2%
Trojans	912.104	908.950 99,7%	896.338 98,3%	845.088 92,7%
other malware	19.827	19.645 99,1%	18.599 93,8%	15.838 79,9%
TOTAL	1.274.928	1.270.685 99,7%	1.252.110 98,2%	1.186.100 93,0%

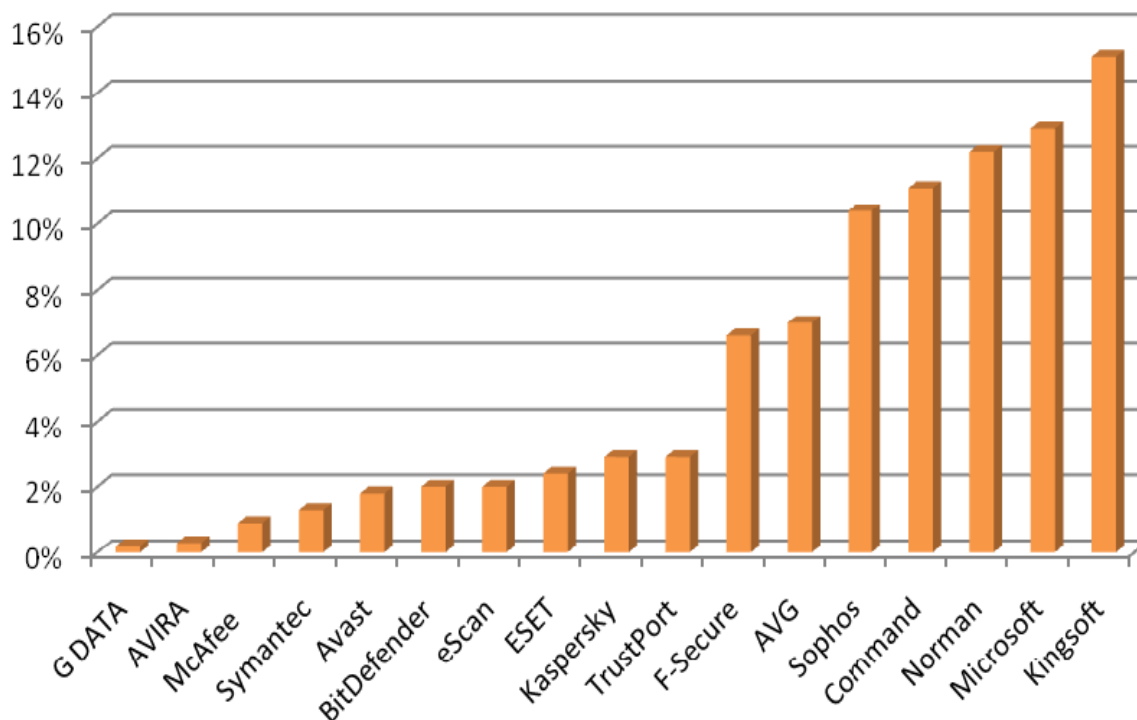
Company	Authentium	MicroWorld	F-Secure	G DATA Security
Product	Command AM	eScan ISS	F-Secure Anti-Virus	G DATA AntiVirus
Program version	5.0.8	10.0.946.341	9.00.149	19.1.0.0
Engine / signature version	20090209	N/A	8.10.14240	19.3715 / 19.219
Award reached in this test	TESTED	ADVANCED	ADVANCED	ADVANCED
Number of false positives*	many	many	few	many
On-demand scanning speed*	average	slow	slow	average
DETECTION RATES:				
SET A (Apr06 - Apr08)	1.820.238	PASSED	PASSED	PASSED
SET B (May08-Jan09):				
Windows viruses	24.476	21.309 87,1%	24.365 99,5%	23.906 97,7%
Macro viruses	2.492	2.485 99,7%	2.438 97,8%	2.470 99,1%
Script malware	8.811	6.248 70,9%	7.444 84,5%	8.293 94,1%
Worms	53.326	42.380 79,5%	52.458 98,4%	50.560 94,8%
Backdoors/Bots	253.892	231.252 91,1%	250.125 98,5%	239.171 94,2%
Trojans	912.104	816.239 89,5%	893.927 98,0%	847.458 92,9%
other malware	19.827	13.118 66,2%	18.770 94,7%	18.922 95,4%
TOTAL	1.274.928	1.133.031 88,9%	1.249.527 98,0%	1.190.780 93,4%

<i>Company</i>	Kaspersky Labs		Kingsoft		McAfee		Microsoft		
<i>Product</i>	Kaspersky AV		Kingsoft AntiVirus		McAfee VirusScan+		Microsoft OneCare		
<i>Program version</i>	8.0.0.506a		2008.11.6.63		13.3.117		2.5.2900.20		
<i>Engine / signature version</i>	N/A		2009.2.8.1		5300.2777 / 5521		1.51.391.0		
Award reached in this test	ADVANCED+		TESTED		ADVANCED+		STANDARD		
Number of false positives*	few		many		few		very few		
On-demand scanning speed*	average		fast		average		average		
DETECTION RATES:									
SET A (Apr06 - Apr08)	1.820.238	PASSED		PASSED		PASSED		PASSED	
SET B (May08-Jan09):									
Windows viruses	24.476	24.297	99,3%	22.096	90,3%	24.425	99,8%	23.400	95,6%
Macro viruses	2.492	2.470	99,1%	1.204	48,3%	2.492	100%	2.190	87,9%
Script malware	8.811	8.362	94,9%	4.010	45,5%	6.673	75,7%	6.312	71,6%
Worms	53.326	52.295	98,1%	45.867	86,0%	52.909	99,2%	46.529	87,3%
Backdoors/Bots	253.892	247.054	97,3%	223.022	87,8%	252.692	99,5%	213.611	84,1%
Trojans	912.104	884.422	97,0%	774.888	85,0%	906.128	99,3%	803.069	88,0%
other malware	19.827	19.160	96,6%	11.569	58,3%	17.889	90,2%	15.385	77,6%
TOTAL	1.274.928	1.238.060	97,1%	1.082.656	84,9%	1.263.208	99,1%	1.110.496	87,1%

<i>Company</i>	ESET		Norman ASA		Symantec		Sophos		
<i>Product</i>	NOD32 Antivirus		Norman AV+AS		Norton Anti-Virus		Sophos Anti-Virus		
<i>Program version</i>	3.0.684.0		7.10.02		16.2.0.7		7.6.4		
<i>Engine / signature version</i>	3839.1180		6.00.06		110208v / 91468		2.83.3 / 4.38E+180		
Award reached in this test	ADVANCED+		TESTED		ADVANCED+		STANDARD		
Number of false positives*	few		many		few		few		
On-demand scanning speed*	average		slow		fast		average		
DETECTION RATES:									
SET A (Apr06 - Apr08)	1.820.238	PASSED		PASSED		PASSED		PASSED	
SET B (May08-Jan09):									
Windows viruses	24.476	24.039	98,2%	22052	90,1%	24.427	99,8%	24.465	~100%
Macro viruses	2.492	2.492	100%	2434	97,7%	2.492	100%	2.308	92,6%
Script malware	8.811	8.505	96,5%	3962	45,0%	7.549	85,7%	8.517	96,7%
Worms	53.326	51.794	97,1%	46861	87,9%	52.699	98,8%	46.757	87,7%
Backdoors/Bots	253.892	249.399	98,2%	224683	88,5%	251.575	99,1%	226.595	89,2%
Trojans	912.104	890.002	97,6%	806290	88,4%	900.425	98,7%	819.102	89,8%
other malware	19.827	18.523	93,4%	13187	66,5%	19.282	97,3%	14.963	75,5%
TOTAL	1.274.928	1.244.754	97,6%	1.119.469	87,8%	1.258.449	98,7%	1.142.707	89,6%

<i>Company</i>	Trustport		
<i>Product</i>	TrustPort AV		
<i>Program version</i>	2.8.0.3011		
<i>Engine / signature version</i>	N/A		
Award reached in this test	ADVANCED		
Number of false positives*	many		
On-demand scanning speed*	slow		
DETECTION RATES:			
SET A (Apr06 - Apr08)	1.820.238	PASSED	
SET B (May08-Jan09):			
Windows viruses	24.476	24.305	99,3%
Macro viruses	2.492	2.461	98,8%
Script malware	8.811	5.319	60,4%
Worms	53.326	52.467	98,4%
Backdoors/Bots	253.892	251.163	98,9%
Trojans	912.104	884.630	97,0%
other malware	19.827	17.359	87,6%
TOTAL	1.274.928	1.237.704	97,1%

Graph of missed samples (lower is better)



Please do not miss the second part of the report (it will be published in a few months) containing the retrospective test, which evaluates how well products are at detecting new/unknown malware. Further test reports covering other aspects of the various products will be released from time to time during the year on our website.

The results of our on-demand tests are usually applicable also for the on-access scanner (if configured the same way), but not for on-execution protection technologies (like HIPS, behaviour blockers, etc.).

A good detection rate is still one of the most important, deterministic and reliable features of an antivirus product. Additionally, most products provide at least some kind of HIPS, behaviour-based or other functionalities to block (or at least warn about the possibility of) malicious actions e.g. during the execution of malware, when all other on-access and on-demand detection/protection mechanism failed. Those special protection features will be evaluated by us later this year.

Even if we deliver various tests and show different aspects of anti-virus software, users are advised to evaluate the software by themselves and build their own opinion about them. Test data or reviews just provide guidance to some aspects that users cannot evaluate by themselves.

We suggest and encourage readers to research also other independent test results provided by various independent testing organizations, in order to get a better overview about the detection and protection capabilities of the various products over different test scenarios and various test-sets.

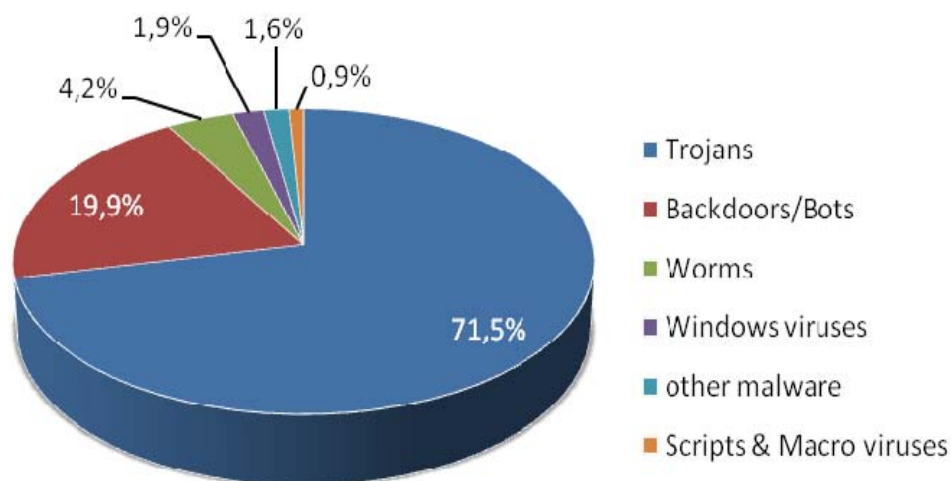
Summary results

The test-set has been split in two parts. The percentages below refer to SET B, which contains only malware from the last 9 months. As a result, percentages may look lower than in previous tests. SET A is covered very well (>97%) by all the tested products and contains malware from April 2006 to April 2008. Please consider also the false alarm rates (listed on next page) when looking at the below detection rates!

Total detection rates¹:

1.	G DATA	99.8%
2.	AVIRA	99.7%
3.	McAfee ²	99.1%
4.	Symantec	98.7%
5.	Avast	98.2%
6.	BitDefender, eScan	98.0%
7.	ESET	97.6%
8.	Kaspersky, TrustPort	97.1%
9.	F-Secure	93.4%
10.	AVG	93.0%
11.	Sophos	89.6%
12.	Command	88.9%
13.	Norman	87.8%
14.	Microsoft	87.1%
15.	Kingsoft	84.9%

SET B contains nearly 1.3 million malware samples. The used malware test-set consists of:



¹ We estimate the remaining error margin for those detection rates to be around 0.4%

² McAfee VirusScan Plus 13.3 comes with the "in-the-cloud" Artemis technology turned on by default. For some users it may be important to know what the baseline minimum detection rate of McAfee would be, should the Internet connection be not available. So we measured also the detection rate of McAfee with no Internet connection. **The McAfee detection rate without Internet connection was 95.2%.**

False positive/alarm test

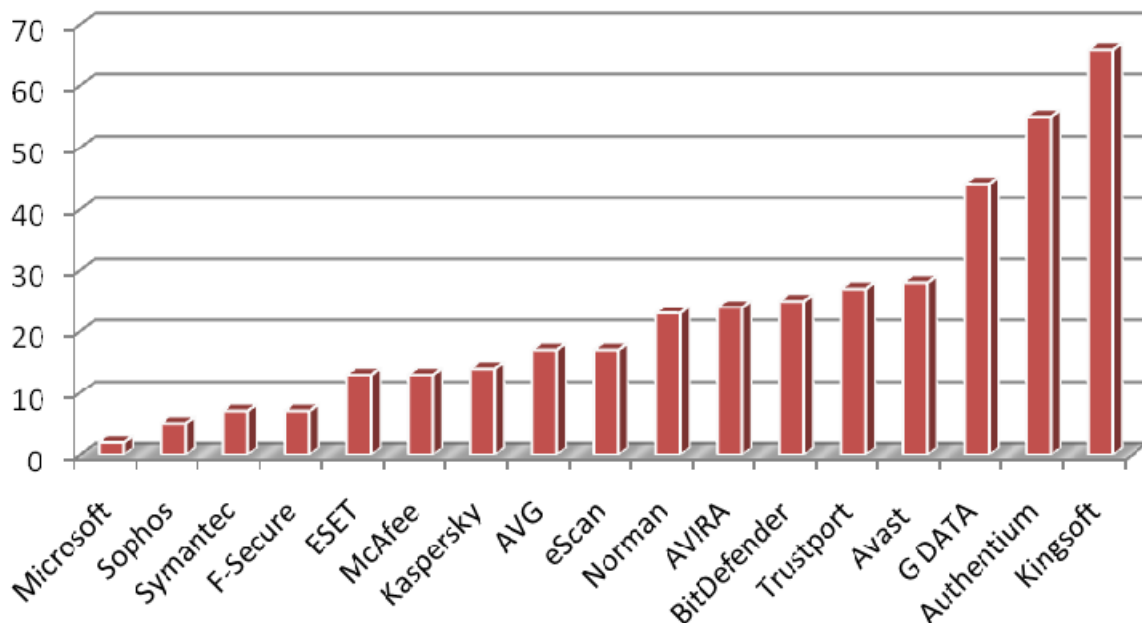
In order to better evaluate the quality of the detection capabilities of anti-virus products, we provide also a false alarm test. False alarms can sometimes cause as much troubles as a real infection. Please consider the false alarm rate when looking at the detection rates, as a product which is prone to cause false alarms achieves higher scores easier.

False Positive Results

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

1.	Microsoft	2	very few FP's
2.	Sophos	5	
3.	Symantec, F-Secure	7	few FP's
4.	ESET, McAfee	13	
5.	Kaspersky	14	
6.	AVG, eScan	17	
7.	Norman	23	
8.	AVIRA	24	
9.	BitDefender	25	
10.	Trustport	27	many FP's
11.	Avast	28	
12.	G DATA	44	
13.	Authentium	55	
14.	Kingsoft	66	

The graph below shows the number of false alarms found in our set of clean files by the tested Anti-Virus products.



Details about the discovered false alarms

With AV testing it is important to measure not only detection capabilities but also reliability - one of reliability aspects is certainly product's tendency to flag clean files as infected. No product is immune from false positives (FP's) but there are differences among them and the goal is to measure them. Nobody has all legitimate files that exist and so no "ultimate" test of FP's can be done. What can be done and is reasonable, is to create and use a set of clean files which is independent. If on such set one product has e.g. 100 FP's and another only 50, it is likely that the first product is more prone to FP's than the other. It doesn't mean the product with 50 FP's doesn't have more than 50 FP's globally, but important is the relative number.

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 were not counted. If a product had several false alarms belonging to the same software, it is counted here as only one false alarm (that's why we label all software in general as "package"). Cracks, keygens, etc. or other questionable applications and tools, as well as FP's distributed by vendors or other non independent sources are not counted here as False Positives.

Below you will find the false alarms we observed in our independent set of clean files. In future we may provide this list as a separate document and not include it in the test report.

Microsoft

False alarm found in some parts of

BackProtection package
InkScapePortable package

Detected as

Trojan:Win32/Vhorse.EY
VirTool:Win32/Obfuscator.C

Microsoft OneCare had 2 false alarms.

Sophos

False alarm found in some parts of

eScan package
PhotoMatix package
RegistryHealer package
SpyCop package
TorChat package

Detected as

Istbar
Mal/Generic-A
Mal/HckPk-A
Mal/VB-A
Mal/HckPk-E

Sophos had 5 false alarms with default settings. With enabled suspicious detection there were about 68 FP's; around 20000 additional malware samples would be detected with enabled "Suspicious" detections. As Sophos is a product for corporate users, which computers are managed by an administrator, the discovered FP's are not a big issue. These files are technically FP's, but the administrators most likely would like to know about the presence of those applications.

Symantec

False alarm found in some parts of

0190warner package
 Burn4Free package
 CL08 package
 CSFireMonitor package
 NirCmd package
 OpenOffice package
 RegCool package

Detected as

Suspicious.MH690
 SecurityRisk.NavHelper
 Trojan Horse
 Downloader
 Backdoor.Trojan
 Suspicious.MH690
 Backdoor.Bifrose

Symantec Norton Anti-Virus had 7 false alarms.

F-Secure

False alarm found in some parts of

CSFireMonitor package
 eScan package
 GoogleTool package
 Lektora package
 NetMeter package
 Photomatix package
 SweetDream package

Detected as

Trojan-Downloader.Win32.Small.afxn
 Trojan.Win32.Genome.erg
 SMS-Flooder.Win32.Delf.l
 Email-Worm.Win32.Skybag.c
 Backdoor.Win32.Delf.kxp
 Net-Worm.Win32.Kolabc.dtf
 Trojan.Win32.Agent.bkjm

F-Secure had 7 false alarms.

ESET

False alarm found in some parts of

6-Zip package
 BattlestationsMidway package
 dotWidget package
 F1Challenge package
 FineReaderPro package
 InkScapePortable package
 IZArc package
 JkDefrag package
 KnightsOfHonor package
 Musketeers package
 PunicWar package
 T-Online package
 WinDVD package

Detected as

Win32/Agent
 Win32/Statik
 Win32/Statik
 Win32/Genetik
 Win32/Statik
 Win32/Spy.Agent
 Win32/Statik
 Win32/Packed.Autoit.Gen
 Win32/Statik
 Win32/Statik
 Win32/Statik
 Win32/Statik
 NewHeur_PE
 Win32/Genetik

ESET NOD32 had 13 false alarms.

McAfee

False alarm found in some parts of

6-Zip package
 AutoStartAdmin package

Detected as

Generic.dx
 Generic!Artemis

CDDVDBurner package	Generic.dx
FileFolderUnlocker package	Generic!Artemis
GoogleDesktop package	Generic.dx
GoogleTool package	Generic Flooder
MultiInstall package	Generic!Artemis
Noctramic package	Generic!Artemis
RegRun package	Generic!Artemis
RootkitUnhooker package	Generic.dx
Soldner package	Generic!Artemis
TaskManager package	PWS-LDPinch
XPTweaker package	Generic!Artemis

McAfee with Artemis had 13 false alarms.

Kaspersky

False alarm found in some parts of

CleanCenter package
 CSFireMonitor package
 Downutube package
 DVDIdentifier package
 eScan package
 GoogleTool package
 Lektora package
 NetMeter package
 PAR package
 Photomatix package
 PicSize package
 SweetDream package
 WinMerge package
 WinPlosion package

Detected as

Backdoor.Win32.SdBot.itt
 Trojan-Downloader.Win32.Small.afxn
 Trojan-Downloader.Win32.Generic
 Trojan.Win32.Generic
 Trojan.Win32.Genome.erg
 SMS-Flooder.Win32.Delf.l
 Email-Worm.Win32.Skybag.c
 Backdoor.Win32.Delf.kxp
 Trojan-Dropper.Script.Generic
 Net-Worm.Win32.Kolabc.dtf
 Trojan-Dropper.Script.Generic
 Trojan.Win32.Agent.bkjm
 Email-Worm.Script.Generic
 Trojan.Win32.Hooker.t

Kaspersky had 14 false alarms.

AVG

False alarm found in some parts of

AVIRA package
 BattleMaps package
 BlackMirror package
 BlazeMediapro package
 CDDVDBurner package
 CreateMovie package
 Cubes package
 FreeMSNWinks package
 HotLaunch package
 InkScapePortable package
 Linkman package
 PCDoorGuard package
 SmartMorph package
 Soldner package

Detected as

Generic11.BJHA
 Win32/Heur
 Downloader.Swizzor
 Generic12.BLDZ
 Generic10.VAH
 BackDoor.Hupigon4.AEWM
 Win32/Heur
 Generic6.IYW
 Generic12.BLDZ
 Obfustat.NPF
 SHeur.ERY
 BackDoor.Generic10.LFG
 Generic12.BLDZ
 PSW.Generic6.FR

Sophos package
 StartKiller package
 SummerBound package

Agent.AOUE
 Generic12.BLDZ
 Generic12.BLDZ

AVG had 17 false alarms.

eScan

False alarm found in some parts of

ApplicationAccessServer package
 BitTorrent package
 CDDVDBurner package
 CFOS package
 CityGuide package
 CL08 package
 GoogleTool package
 HPRestore package
 InkScapePortable package
 LogMeIn package
 MediaConverter package
 PCSecurityTest package
 PowerTools package
 Putty package
 SmartNIC package
 Word2Web package
 Zattoo package

Detected as

Trojan.Spy.Sigatar.5041.B
 Trojan.Generic.376185
 Trojan.Generic.97211
 Trojan.Heur.GM.0440616120
 Trojan.AgentMB.Delf.HZGAB0939497
 Trojan.Generic.430620
 Trojan.Generic.1267563
 BAT.KillAV.Gen
 Trojan.Generic.103962
 Virtool.903
 Backdoor.Generic.148978
 Trojan.Generic.1397003
 Macro.VBA
 Worm.Generic.15375
 Trojan.Downloader.JLPP
 Macro.VBA
 Trojan.Generic.1372495

eScan had 17 false alarms.

Norman

False alarm found in some parts of

AudioVideo2Exe package
 Azureus package
 BookmarkBuddy package
 dBPower package
 Firefox package
 GPSphoto package
 IconHider package
 Insaniquarium package
 JSplit package
 Kazaa package
 MaulwurfsMover package
 Nero package
 NirCmd package
 PocketChess package
 RadLight package
 PDPSoftware package
 RivaTuner package
 StreamRipper package
 TaskManager package

Detected as

W32/Packed_Upack.A
 DLoader.LOXQ
 Ircbot.YJP
 W32/Malware.ERCK
 HTML/Iframe.gen.A
 W32/Joiner.BRV.dropper
 W32/Webmoner.ABJ
 W32/Smalltroj.IBLY
 W32/Crypto
 W32/Packed_PeX.B
 Suspicious_F.gen
 W32/OnLineGames.HUPN
 Smalldoor.CGNH
 W32/Agent.GZWS.dropper
 Malware.DNHL
 Malware.FNSF
 W32/Agent.IQHH
 NetworkWorm.EMS
 W32/LdPinch.SFX

TyperShark package	W32/Smalltroj.IBLY
Vitascene package	W32/EMailWorm.BES
XP-AS package	Antivirus2008.PU
Zuma package	W32/Smalltroj.IBLU

Norman had 23 false alarms.

AVIRA

False alarm found in some parts of

3DScreensaver package
6-Zip package
AdKiller package
BOM package
CDSearch package
ClipboardRecorder package
CSFireMonitor package
DashBoard package
DrWeb package
Edimax driver package
EKalkulator package
EUPrice package
GoogleTool package
HP scanner package
InternetDownloadManager package
iRejectTrash package
LaunchExpress package
MSI WLAN package
NeighborsFromHell package
Paraworld package
PCDoorGuard package
SmartProtector package
StickSecurity package
TrendMicro package

Detected as

TR/Spy.8369026.A
TR/Agent.239371.A
HEUR/Malware
HEUR/HTML.Malware
HEUR/HTML.Malware
HEUR/Malware
DR/Dldr.Small.afxn
HEUR/Malware
TR/QQShou.E0.1
SPR/Hacktool.57344
TR/Crypt.ULPM.Gen
HEUR/Macro.Word95
DR/Flood.Delf.L
HEUR/Malware
TR/Crypt.XPACK.Gen
HEUR/Malware
HEUR/Malware
ADSPY/Agent.emg
TR/Dropper.Gen
TR/Downloader.Gen
BDS/Beasty.A
TR/Agent.593920.A
HEUR/Malware
TR/Hijacker.Gen

AVIRA had 24 false alarms.

BitDefender

False alarm found in some parts of

ApplicationAccessServer package
BitTorrent package
Browster package
CDDVDBurner package
CFOS package
CityGuide package
CL08 package
DiaShowPro package
FotoWorks package
GoogleTool package
Haushaltsbuch package

Detected as

Trojan.Spy.Sigatar.5041.B
Trojan.Generic.376185
Win32.ExplorerHijack
Trojan.Generic.97211
Trojan.Heur.GM.0440616120
Trojan.AgentMB.Delf.HZGAB0939497
Trojan.Generic.430620
Packer.Morphine
Packer.Morphine
Trojan.Generic.1267563
Generic.PWS.Games.4.4E81B454

HPRestore package	BAT.KillAV.Gen
InkScapePortable package	Trojan.Generic.103962
LogMeIn package	Virtool.903
MediaConverter package	Backdoor.Generic.148978
PCSecurityTest package	Trojan.Generic.1397003
PowerTools package	Macro.VBA
Putty package	Worm.Generic.15375
ShopToDate package	Trojan.Generic.1287015
SKS_CD package	Trojan.Generic.1055076
SmartNIC package	Trojan.Downloader.JLPF
TeamSpeak package	Trojan.Pws.Hooker.TR
Word2Web package	Macro.VBA
Zattoo package	Trojan.Generic.1372495

Bitdefender had 25 false alarms.

TrustPort

False alarm found in some parts of

AudioVideo2Exe package
 AVIRA package
 Azureus package
 BookmarkBuddy package
 CDDVDBurner package
 CreateMovie package
 dBPower package
 Firefox package
 GPSphoto package
 IconHider package
 Insaniquarium package
 JSplit package
 Kazaa package
 MaulwurfsMover package
 NirCmd package
 PCDoorGuard package
 PocketChess package
 RadLight package
 RivaTuner package
 Soldner package
 Sophos package
 StreamRipper package
 TaskManager package
 TyperShark package
 Vitascene package
 XP-AS package
 Zuma package

Detected as

W32/Packed_Upack.A
 Generic11.BJHA
 DLoader.LOXQ
 Ircbot.YJP
 Generic10.VAH
 BackDoor.Hupigon4.AEWM
 W32/Malware.ERCK
 HTML/Iframe.gen.A
 W32/Joiner.BRV.dropper
 W32/Webmoner.ABJ
 W32/Smalltroj.IBLY
 W32/Crypto
 W32/Packed_PeX.B
 Suspicious_F.gen
 Smalldoor.CGNH
 BackDoor.Generic10.LFG
 W32/Agent.GZWS.dropper
 Malware.DNHL
 W32/Agent.IQHH
 PSW.Generic6.FR
 Agent.AOUE
 NetworkWorm.EMS
 W32/LdPinch.SFX
 W32/Smalltroj.IBLY
 W32/EMailWorm.BES
 Antivirus2008.PU
 W32/Smalltroj.IBLU

TrustPort had 27 false alarms.

Avast

False alarm found in some parts of

3DScreensaver package
 0190warner package
 Burn4Free package
 CDDVDBurner package
 CheckMail package
 CL08 package
 CreateMovie package
 CSFireMonitor package
 CTManager package
 Dirwat package
 edVARdo package
 ExelockExpress package
 FolderPatrol package
 FTP4Pro package
 GoogleTool package
 iNetQuery package
 iPodAccess package
 LockFolderXP package
 MDAdressbuch package
 NetMeter package
 Noctramic package
 PDFExplorer package
 PhotoMatix package
 SharpEye package
 SKS package
 StartpageSave package
 Suse package
 Winter package

Detected as

Win32:Trojan-gen {Other}
 Win32:Rootkit-gen [Rtk]
 Win32:Navexcel-H [Trj]
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Delf-GJF [Trj]
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:Delf-GJF [Trj]
 Win32:Trojan-gen {Other}
 Win32:Hgweb-B [Trj]
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 Win32:SkiMorph [Cryp]
 Win32:Trojan-gen {Other}
 Win32:Trojan-gen {Other}
 ELF:Race-D [Expl]
 Win32:Trojan-gen {Other}

Avast had 28 false alarms.

G DATA

False alarm found in some parts of

0190warner package
 3DScreensaver package
 ApplicationAccessServer package
 BitTorrent package
 Burn4Free package
 CDDVDBurner package
 CFOS package
 CheckMail package
 CityGuide package
 CL08 package
 CreateMovie package
 CSFireMonitor package
 CTManager package
 Dirwat package

Detected as

Win32:Badya
 Win32:Badya
 Trojan.Spy.Sigatar.5041.B
 Trojan.Generic.376185
 Win32:Badya
 Win32:Badya
 Trojan.Heur.GM.0440616120
 Win32:Badya
 Trojan.AgentMB.Delf.HZGAB0939497
 Trojan.Generic.430620
 Win32:Badya
 Win32:Badya
 Win32:Badya
 Win32:Daum.A

edVARdo package	Win32:Badya
ExelockExpress package	Win32:Badya
FolderPatrol package	Win32:Badya
FTP4Pro package	Win32:Badya
GoogleTool package	Win32:Badya
HPRestore package	BAT.KillAV.Gen
iNetQuery package	Win32:Badya
InkScapePortable package	Trojan.Generic.103962
iPodAccess package	Win32:Trojan-gen {Other}
LockFolderXP package	Win32:Badya
LogMeIn package	Virtool.903
MAddressbuch package	Win32:Badya
MediaConverter package	Backdoor.Generic.148978
NetMeter package	Win32:Trojan-gen {Other}
Noctramic package	Win32:Badya
PCSecurityTest package	Trojan.Generic.1397003
PDFExplorer package	Win32:Trojan-gen {Other}
PhotoMatix package	Win32:Trojan-gen {Other}
PowerTools package	Macro.VBA
Putty package	Worm.Generic.15375
SharpEye package	Win32:SkiMorph [Cryp]
SKS package	Win32:Trojan-gen {Other}
SmartNIC package	Trojan.Downloader.JLPF
StartpageSave package	Win32:Trojan-gen {Other}
Suse package	ELF:Race-D [Exp]
Winter package	Win32:Trojan-gen {Other}
Word2Web package	Macro.VBA
Zattoo package	Trojan.Generic.1372495

G DATA had 44 false alarms.

Command

False alarm found in some parts of

3DScreensaver package
 320mph package
 Air2Mp3 package
 AnimateDesktop package
 AVIRA package
 Blitzkrieg package
 Budgeter package
 Burn4Free package
 CDDVDBurning package
 ClonyXXL package
 CookieCooker package
 CPUZ package
 DM package
 DriveImage package
 DriveIndexTool package
 DrWeb package
 Enfish package

Detected as

W32/Malware!1b74
 W32/Backdoor2.YMQ
 W32/Banload.E.gen!Eldorado
 W32/Heuristic-187!Eldorado
 W32/Agent.K.gen!Eldorado
 W32/IRCBot-based!Maximus
 W32/Backdoor2.RWA
 W32/Malware!e664
 W32/Heuristic-210!Eldorado
 W32/Heuristic-210!Eldorado
 Security_Risk
 W32/Downldr2.DYOA
 W32/OnlineGames.F.gen!Eldorado
 W32/D_Downloader!GSA
 W32/Autoit.B
 W32/Downloader.N.gen!Eldorado
 W32/Threat-SysAdderSml!Eldorado

ePaper package	SWF/Downloader.D!Camelot
EzDesk package	Security_Risk
FileAnalyser package	W32/Backdoor.AJKH
FlashGet package	W32/Malware!0e45
Generals package	W32/IRCBot-based!Maximus
GIMP package	W32/Onlinegames.gen
Gothic package	W32/Trojan.BHOT
iNetControl package	W32/NewMalware-Rootkit-I-based!Maximus
JAlbum package	SWF/Downloader.D!Camelot
Kasperky package	W32/Heuristic-KPP!Eldorado
KCFM package	W32/BankerP.FJ
McAfee package	W32/Blocker-based!Maximus
Memtest package	Heuristic-90
Myth package	W32/IRCBot-based!Maximus
NGame package	W32/AV2008.E
OutlookTuner package	W32/Heuristic-C02!Eldorado
PCWizard package	W32/Heuristic-USU!Eldorado
Pidgin package	W32/Onlinegames.gen
Powerstrip package	W32/Heuristic-210!Eldorado
RadioRipper package	W32/Trojan3.CC
RegCool package	W32/Backdoor.AJKH
RootkitUnhooker package	W32/Heuristic-210!Eldorado
Sims package	W32/Hijack.A.gen!Eldorado
Stammbaum package	W32/Downloader.B.gen!Eldorado
TaskManager package	W32/Heuristic-210!Eldorado
TCPfilter package	W32/Backdoor2.DARJ
ThirdReich package	W32/IRCBot-based!Maximus
TrendMicro package	W32/Downldr2.FCFK
TweakPower package	W32/Backdoor.AJKH
UltraStar package	W32/Zlob.R.gen!Eldorado
Unreal package	W32/Heuristic-119!Eldorado
UPACK compression tool package	W32/Virut.AI!Generic
USBtray package	W32/Banload.C.gen!Eldorado
WebZip package	W32/Downloader.L.gen!Eldorado
WinMHT package	W32/Downloader.L.gen!Eldorado
WinSplit package	W32/AV2008.C
Worms3D package	W32/IRCBot-based!Maximus
XPTweaker package	W32/Heuristic-210!Eldorado

Command had 55 false alarms. Please note that Command is a new entry in our tests. We expect that in the next test the number of false alarms will be much lower.

Kingsoft

False alarm found in some parts of

ACER driver package
 AlbumCoverArt package
 Animation package
 Astra package
 Autoruns package
 BaldursGate package

Detected as

Win32.Troj.Monder.475648
 Win32.Troj.StartPage.a.1585049
 Win32.Hack.ThinPackerT.a.378833
 Win32.Hack.HacDef.1245184
 Win32.Troj.Chuzy.352256
 Win32.Hack.Kelebek.1120149

CCleaner package	Win32.Troj.Selfish.1497584
ClonyXXL package	Worm.Roron.136332
ColoringBook package	Win32.Troj.Unknown.az.186112
CounterStrike package	Worm.Roron.136332
CPUZ package	Win32.TrojDownloader.Small.624231
Creative driver package	Win32.Troj.Obfuscated.40960
DarkHorizons package	Win32.Troj.Unknown.az.186112
eMule package	Win32.Troj.Agent.3534076
FAR package	Win32.Troj.Taris.1418369
Fifa package	Win32.Hack.Beastdoor.1154875
Folder2ISO package	Win32.TrojDownloader.Delf.us.3174400
F-Secure package	Win32.Hack.ThinLPackerT.a.378833
Gothic2 package	Win32.PSWTroj.Nilage.42496
Grep package	Win32.Troj.VB.96768
HotSpotShield package	Win32.Troj.Agent.oe.1035231
HoverWheel package	Win32.Hack.IRCBot.1444845
IceAge2 package	Win32.Hack.ThinLPackerT.a.378833
Intel driver package	Win32.Hack.ThinLPackerT.a.378833
Less package	Win32.Troj.Agent.15872
LoginControl package	Win32.VirInstaller.Agent.508937
MagischesAuge package	Win32.Hack.ThinLPackerT.a.378833
MapInfo package	Win32.Troj.Varvar.292864
MapleXP package	Win32.VirInstaller.Agent.842830
Medion driver package	Win32.Troj.Hidrag.110592
MIRC package	Win32.Troj.Plutor.1007616
MS Links package	Win32.Troj.SysJunkT.hh
MS Office97 package	Win32.Troj.Undersor__5B.318976
MS Windows95 package	Worm.Ganda__3E514.70199
MS Windows95 SP1 package	Win32.Troj.Pres__130B9A.66672
MS Windows98 package	Worm.Ganda__6A7DE.70199
MS Windows2000 package	Worm.Ridnu.4880
MS WindowsXP package	Win32.Troj.Patched.14336
MS WindowsXP SP1 package	Worm.Polip.274432
MS WindowsXP SP2 package	Worm.Polip.388608
MS WindowsXP SP3 package	Worm.Wast__66F897.156550
MS WindowsME package	Win32.Troj.Pres__CCA2FB.81920
MS Works package	Win32.Hack.ThinLPackerT.a.378833
NortonSystemWorks package	Worm.Brontok.176911
PCW package	JS.Agent.dg.4982
PEiD package	Win32.Troj.Sality.158720
Perl package	VBS.DNAOrder.aa.35780
PowerStrip package	Win32.Hack.Huigezi.1012719
ProcessExplorer package	Win32.Troj.Stagol.192512
RegistryMonitor package	Win32.Troj.Taris.98304
RegistryOptimizer package	Worm.Beagle.102400
Resistance package	Win32.Troj.JunkDLL.ao.147559
SataRaid package	Win32.Troj.Virut.905216
Scanner package	Win32.Troj.Sality.160256
ShellOut package	Win32.Joke.MovingMouse.k.20480
SIW package	Win32.Troj.Tvido.1598976
SpaceShooter package	Win32.Hack.Kelebek.1120149
SQL package	Win32.Troj.Selfish.90166

TCPview package	Win32.PSWTroj.LdPinch.94208
T-Online package	Win32.Hack.ThinLPackerT.a.378833
Unreal package	Win32.Hack.Shark.429069
Video2Brain package	Win32.Hack.ThinLPackerT.a.378833
WinRAR package	Win32.Troj.Selfish.1004712
WinRoll package	Win32.Troj.OnLineGames.of.15360
WISO package	Win32.Hack.ThinLPackerT.a.378833
Zzzap package	Win32.IRC.Flood.n.2103523

Kingsoft had 66 false alarms, and some of them were on operating system files. Please note that Kingsoft is a new entry in our tests. We expect that in the next test the number of false alarms will be much lower.

Kingsoft is the first vendor from China, which is brave enough to face the challenge of our international test. Before a product can take part in our public main tests, it first has to pass our minimum requirements. Not many Chinese vendors are eligible to participate in our international tests.

Influence of false alarms on the awards

Please note that - as we announced already last year - false alarms lead now to lower Awards in our test. The labels for false alarms found in our set of clean files are unchanged, as well as the detection rate ranges. The awards are given according to the table below:

		Detection Rates			
		<87%	87 - 93%	93 - 97%	97 - 100%
Few (0-15 FP's)	tested	STANDARD	ADVANCED	ADVANCED+	
Many (16-100 FP's)	tested	tested	STANDARD	ADVANCED	

By having fixed ranges (esp. for FP's) it may be sometimes a bit hard for vendors to accept that they fall down to the next award due to only a few more FP's in our set of clean files. But in our opinion the ranges are already quite generous (esp. considering that all vendors always get the false alarm samples after the test and can fix them, while our clean set does not grow that much over time).

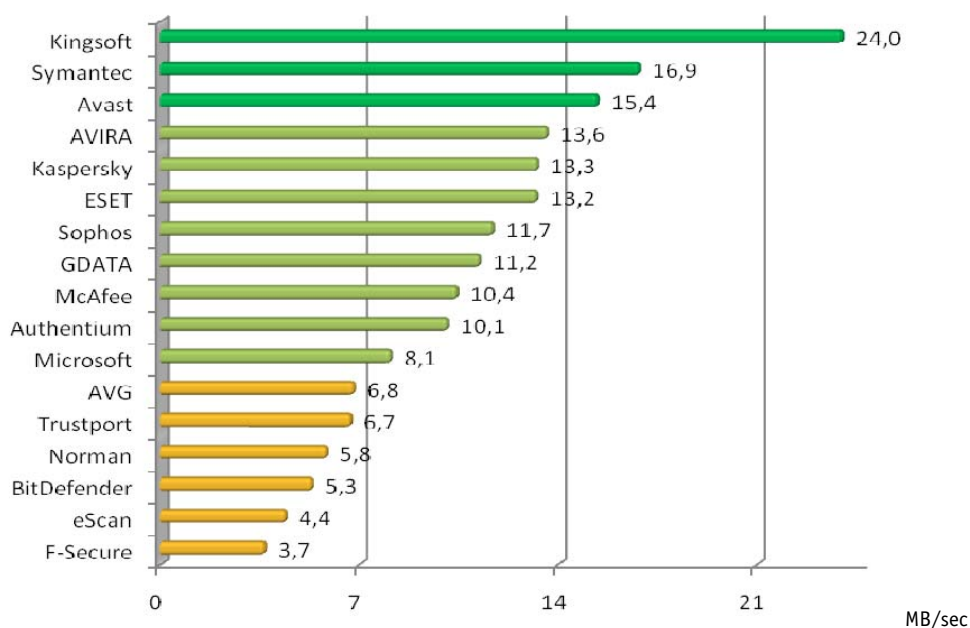
We will not change ranges just to make some vendors happy. We suggest vendors to continue improving their products and they will then get higher Awards when according to our test results they deserve it. Those new rules were announced already last year. Some vendors which would reach higher awards by looking at detection rates only, may be a bit unhappy that those higher requirements for the awards have now been implemented.

Scanning Speed Test

Anti-Virus products have different scanning speeds due to 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 and active rootkit scan, how deep and thorough the unpacking and unarchiving support is, additional security scans, etc.

Some products have technologies to decrease scan times on subsequent scans by skipping previously scanned files. As we want to know the scan speed (when files are really scanned for malware) and not the skipping files speed, those technologies are not taken into account here. In our opinion some products should inform the users more clearly about the performance-optimized scans and then let the users decide if they prefer a short performance-optimized scan (which does not re-check all files, with potential risk of overlooking infected files) or a full-security scan.

The following graph shows the throughput rate in MB/sec (higher is faster) of the various Anti-Virus products when scanning (on-demand) with highest settings our whole set of clean files (used for the false alarm testing). The scanning throughput rate will vary based on the set of clean files³, the settings and the hardware used.



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





The scanning speed tests were done under Windows XP SP3, on identical Intel Core 2 Duo E8300/2.83GHz, 2GB RAM and SATA II disks.

³ to know how fast various products would be on *your* PC at scanning *your* files, we advise you to try the products yourself

Award levels reached in this test

AV-Comparatives provides a 3-level-ranking-system (STANDARD, ADVANCED and ADVANCED+). As this report contains also the raw detection rates (see page 10) and not only the awards, users that do not care about false alarms can rely on that score alone if they want to.

Getting high awards is now harder, because now the Awards are based on detection rates over Set B, which contains malware from the last nine months (May 08 to the beginning of February 09). In this case the detection rates (percentages) are lower than at the last tests, were we counted the overall rating based on Set A and Set B (where Set A is well covered by almost all vendors). Furthermore, False Alarms now reduce the Awards level.

AWARDS (based on detection rates and false alarms)	PRODUCTS (in no specific order) ⁴
	<ul style="list-style-type: none"> ✓ Symantec ✓ ESET ✓ Kaspersky ✓ McAfee⁵
	<ul style="list-style-type: none"> ✓ G DATA* ✓ AVIRA* ✓ Avast* ✓ BitDefender* ✓ eScan* ✓ TrustPort* ✓ F-Secure
	<ul style="list-style-type: none"> ✓ AVG* ✓ Sophos ✓ Microsoft
	<ul style="list-style-type: none"> ✓ Authentium* ✓ Norman* ✓ Kingsoft

*: those products got lower awards due false alarms

The Awards are not only based on detection rates - also False Positives found in our set of clean files are considered. A product that is successful at detecting a high percentage of malware but suffers from false alarms may not be necessarily better than a product which detects less malware but which generates less FP's.

⁴ We suggest to consider products with same the award to be as good as the other products with same award.

⁵ McAfee without Artemis would have earned ADVANCED, please see comments on pages 5 and 10.

Copyright and Disclaimer

This publication is Copyright © 2009 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. AV-Comparatives e.V. 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 e.V. 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. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (March 2009)