Anti-Virus Comparative

On-demand Detection of Malicious Software

includes false alarm and on-demand scanning speed test

Language: English
August 2011
Last Revision: 27th September 2011

www.av-comparatives.org

Table of Contents

Tested Products

- avast! Free Antivirus 6.0
- AVG Anti-Virus Free Edition 10.0
- AVIRA AntiVir Personal 10.2
- BitDefender Antivirus Plus 2012
- eScan Anti-Virus 11.0
- ESET NOD32 Antivirus 5.0
- F-Secure Anti-Virus 2011
- G DATA AntiVirus 2012
- K7 TotalSecurity 11.1
- Kaspersky Anti-Virus 2012
- McAfee AntiVirus Plus 2011
- Microsoft Security Essentials 2.1
- Panda Cloud Antivirus 1.5
- PC Tools Spyware Doctor with AV 8.0
- Qihoo 360 Antivirus 2.0
- Sophos Anti-Virus 9.7
- Symantec Norton Anti-Virus 2012
- Trend Micro Titanium AntiVirus+ 2012
- Trustport Antivirus 2012
- Webroot AntiVirus with Spy Sweeper 7.0

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.

The participation is limited to not more than 20 well-known Anti-Virus products, which vendors agreed to get tested and included in the public test-series of 2011.

Tested Product Versions

The Malware sets have been frozen the 1st August 2011. The system sets and the products were updated and frozen on the 12th August 2011. The following 20 up-to-date products[1] were included in this public test:

- avast! Free Antivirus 6.0.1203
- AVG Anti-Virus Free Edition 10.0.1392
- AVIRA AntiVir Personal 10.2.0.700
- BitDefender Anti-Virus+ 15.0.27.319
- eScan Anti-Virus 11.0.1139.998
- ESET NOD32 Antivirus 5.0.90.0
- F-Secure Anti-Virus 10.51.106
- G DATA AntiVirus 22.0.2.32
- K7 TotalSecurity 11.1.0050
- Kaspersky Anti-Virus 12.0.0.374 (abc)
- McAfee AntiVirus Plus 15.0.291
- Microsoft Security Essentials 2.1.1116.0
- Panda Cloud Antivirus Free 1.5.1
- PC Tools Spyware Doctor with Antivirus 8.0.0.655
- Qihoo 360 Antivirus 2.0.1.1332
- Sophos Anti-Virus 9.7.4
- Symantec Norton Anti-Virus 19.1.0.21
- Trend Micro Titanium AntiVirus Plus 2012
- Trustport Antivirus 10.0.0.4796
- Webroot AntiVirus with Spy Sweeper 7.0.11.25

Please try the products[2] 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, HIPS / behaviour blocker functions, URL filter/reputation services, support, etc.) to consider. Some products may offer additional features e.g. to provide additional protection against malware during its execution (if not detected in advance on-access or on-demand).

Although extremely important, the detection rate of a product is only one aspect of a complete Anti-Virus product. AV-Comparatives provides also a whole product dynamic test, as well as other test reports which cover different aspects/features of the products.

---

[1] Avast, AVG, AVIRA and Panda wanted to participate in the tests with their free product version.

[2] Information about used additional third-party engines/signatures inside the products: **eScan**, **F-Secure** and **Qihoo 360** are based on the Bitdefender engine. **G DATA** is based on the Avast and Bitdefender engines. **PC Tools** is using the signatures of Symantec. **Trustport** is based on the AVG and Bitdefender engines. **Webroot** is based on the Sophos engine.

Comments

Nowadays, almost all products run with the highest protection settings by default (at least during on-demand / scheduled scans), some however may automatically switch to the highest settings once infection detections begin to occur. Due to this, and in order to ensure comparable results, we tested all products with the highest settings unless explicitly advised otherwise by the security vendors. The vendors may do this as they prefer the highest settings not to be used due to high number of False Alarms, or perhaps the highest settings will have a performance impact, or maybe they are planning to change/remove the setting in the near future. Below are some notes about the settings used (scan all files etc is always enabled), e.g.: where the settings are not set to the highest by default:

Avast, AVIRA, Kaspersky, Symantec: asked to get tested with heuristic set to high/advanced. For this reason, we recommend users to consider also setting the heuristics to high/advanced.
F-Secure, Sophos: asked to get tested and awarded based on their default settings (i.e. without using their advanced heuristics / suspicious detections setting).
AVG, AVIRA: asked to do not enable/consider the informational warnings of packers as detections. So, we did not count them as detections (neither on the malware set, nor on the clean set).

AV-Comparatives prefers to test with default settings. As most products run with highest settings by default (or switch to highest automatically when malware is found, making it impossible to test against various malware with "default" settings), in order to get comparable results we set also the few remaining products to highest settings (or leave them to lower settings) in accordance with the respective vendors. We kindly ask vendors to provide stronger settings by default, i.e. set their default settings to highest levels of detection, esp. for scheduled scans or scans initiated by the user this would make more sense. We also kindly ask vendors to remove paranoid settings inside the user interface which are too high to be ever of any benefit for normal users. As some vendors decided to take part in our tests using the stronger settings, it appears that the better option would be to go for the stronger settings by default and that is why we recommend users to consider to use those settings too.

Several products make use of cloud technologies, which require an active internet connection. Our test is performed using an active internet connection. Although we do not longer show the baseline detection rates without cloud and show instead only the results with active cloud, users should be aware that detection rates may in some few cases be lower if the scan is performed while offline (or when the cloud is unreachable without their knowledge). The cloud should be considered as an additional benefit/feature to increase detection rates (as well as response times and false alarm suppression) and not as a full replacement for local offline detections. Vendors should make sure that users are warned in case that the connectivity to the cloud gets lost e.g. during a scan, which may affect considerably the provided protection and make e.g. the initiated scan useless. We have seen that products which rely much on the cloud may perform better in detecting PE malware, while scoring lower in detecting malware in non-PE format, like present in the "other malware/viruses" category.

Telemetry data has been consulted to include prevalent malware samples which are/were hitting users in the last six months. Due the focus on prevalent/widespread and recent samples (majority is from last three months), the size of the test-set is much smaller than in previous years.

Test Results

Below are the test results tables containing the detection rate details of the various products over the used test-set.

During the test Sophos and Webroot (who also use Sophos technology) scored lower detection rates due to issues with their cloud technology. The results shown include estimated cloud detections (but are listed out of competition).

Company *Product* *Program version*		Qihoo **360 Antivirus** 2.0.1.1332		AVIRA **AntiVir Personal** 10.2.0.700		Avast Software **avast! Free Antivirus** 6.0.1203		AVG Technologies **AVG Free Anti-Virus** 10.0.1392	
Award reached in this test		ADVANCED		ADVANCED+		ADVANCED+		ADVANCED	
Number of false positives On-demand scanning speed		many slow		few fast		few fast		many average	
Worms	9.707	9.674	99,7%	9.680	99,7%	9.464	97,5%	9.143	94,2%
Backdoors/Bots	20.502	20.458	99,8%	20.469	99,8%	19.846	96,8%	19.924	97,2%
Trojans	170.352	169.811	99,7%	169.767	99,7%	166.083	97,5%	163.595	96,0%
other malware/viruses	5.482	4.983	90,9%	5.091	92,9%	4.981	90,9%	4.589	83,7%
TOTAL	**206.043**	204.926	**99,5%**	205.007	**99,5%**	200.374	**97,2%**	197.251	**95,7%**

Company *Product* *Program version*		BitDefender **BitDefender AV Plus** 15.0.27.319		MicroWorld **eScan Anti-Virus** 11.0.1139.998		F-Secure **F-Secure Anti-Virus** 10.51.106		G DATA Security **G DATA AntiVirus** 22.0.2.32	
Award reached in this test		ADVANCED+		ADVANCED		ADVANCED+		ADVANCED+	
Number of false positives On-demand scanning speed		few average		many average		few average		few average	
Worms	9.707	9.534	98,2%	9.534	98,2%	9.536	98,2%	9.689	99,8%
Backdoors/Bots	20.502	20.193	98,5%	20.213	98,6%	20.223	98,6%	20.454	99,8%
Trojans	170.352	168.150	98,7%	168.228	98,8%	168.302	98,8%	169.932	99,8%
other malware/viruses	5.482	4.955	90,4%	4.971	90,7%	4.970	90,7%	5.372	98,0%
TOTAL	**206.043**	202.832	**98,4%**	202.946	**98,5%**	203.031	**98,5%**	205.447	**99,7%**

Company *Product* *Program version*		K7 Computing **K7 TotalSecurity** 11.1.0050		Kaspersky Labs **Kaspersky AV** 12.0.0.374 (abc)		McAfee **McAfee AntiVirus +** 15.0.291		ESET **NOD32 Antivirus** 5.0.90.0	
Award reached in this test		TESTED		ADVANCED+		ADVANCED+		ADVANCED+	
Number of false positives On-demand scanning speed		many fast		very few average		none fast		very few average	
Worms	9.707	8.128	83,7%	9.546	98,3%	9.102	93,8%	9.461	97,5%
Backdoors/Bots	20.502	18.331	89,4%	20.313	99,1%	20.133	98,2%	19.979	97,4%
Trojans	170.352	145.650	85,5%	167.341	98,2%	165.785	97,3%	166.301	97,6%
other malware/viruses	5.482	4.323	78,9%	5.321	97,1%	4.480	81,7%	4.807	87,7%
TOTAL	**206.043**	176.432	**85,6%**	202.521	**98,3%**	199.500	**96,8%**	200.548	**97,3%**

Company *Product* *Program version*		Symantec **Norton Anti-Virus** 19.1.0.21		Panda Security **Panda Cloud AV** 1.5.1		Microsoft **Security Essentials** 2.1.1116.0		Sophos **Sophos Anti-Virus** 9.7.4	
Award reached in this test		ADVANCED		ADVANCED+		ADVANCED		N/A	
Number of false positives On-demand scanning speed		many average		very few average		very few slow		many average	
Worms	9.707	9.311	95,9%	9.675	99,7%	9.318	96,0%	8.841	91,1%
Backdoors/Bots	20.502	20.031	97,7%	20.490	99,9%	18.319	89,4%	18.953	92,4%
Trojans	170.352	162.771	95,5%	169.917	99,7%	157.361	92,4%	161.601	94,9%
other malware/viruses	5.482	3.737	68,2%	4.418	80,6%	4.668	85,2%	4.788	87,3%
TOTAL	**206.043**	195.850	**95,1%**	204.500	**99,3%**	189.666	**92,1%**	194.183	**94,2%**

Company *Product* *Program version*		PC Tools **SpywareDoctor+AV** 8.0.0.655		Trend Micro **Trend Micro TiAV+** 2012		Trustport **Trustport Antivirus** 10.0.0.4796		Webroot **Webroot AV+SS** 7.0.11.25	
Award reached in this test		TESTED		ADVANCED+		ADVANCED		N/A	
Number of false positives On-demand scanning speed		**many** slow		**few** fast		**many** slow		**many** average	
Worms	9.707	8.379	86,3%	9.386	96,7%	9.683	99,8%	8.825	90,9%
Backdoors/Bots	20.502	18.548	90,5%	19.819	96,7%	20.467	99,8%	18.928	92,3%
Trojans	170.352	152.836	89,7%	165.244	97,0%	169.961	99,8%	161.499	94,8%
other malware/viruses	5.482	2.331	42,5%	4.579	83,5%	5.102	93,1%	4.787	87,3%
TOTAL	**206.043**	182.094	**88,4%**	199.028	**96,6%**	205.213	**99,6%**	194.039	**94,2%**

The total detection rates are grouped by the testers after looking at the clusters build with the hierarchal clustering method. The false alarms are taken into account as usual, but we are evaluating to change the FP test and rating in future.

By using clusters, there are no longer fixed thresholds to reach, as the thresholds change based on the various results. The testers may group the clusters rationally and not rely solely on the clusters, to avoid that if e.g. all products would in future score badly, they do not get high rankings anyway. We are evaluating to apply next year additional rules to avoid that too many vendors appear in the first cluster just due the presence of outsiders occupying lower clusters. Users which prefer the old award system can apply themselves a rating system based on fixed percentages.

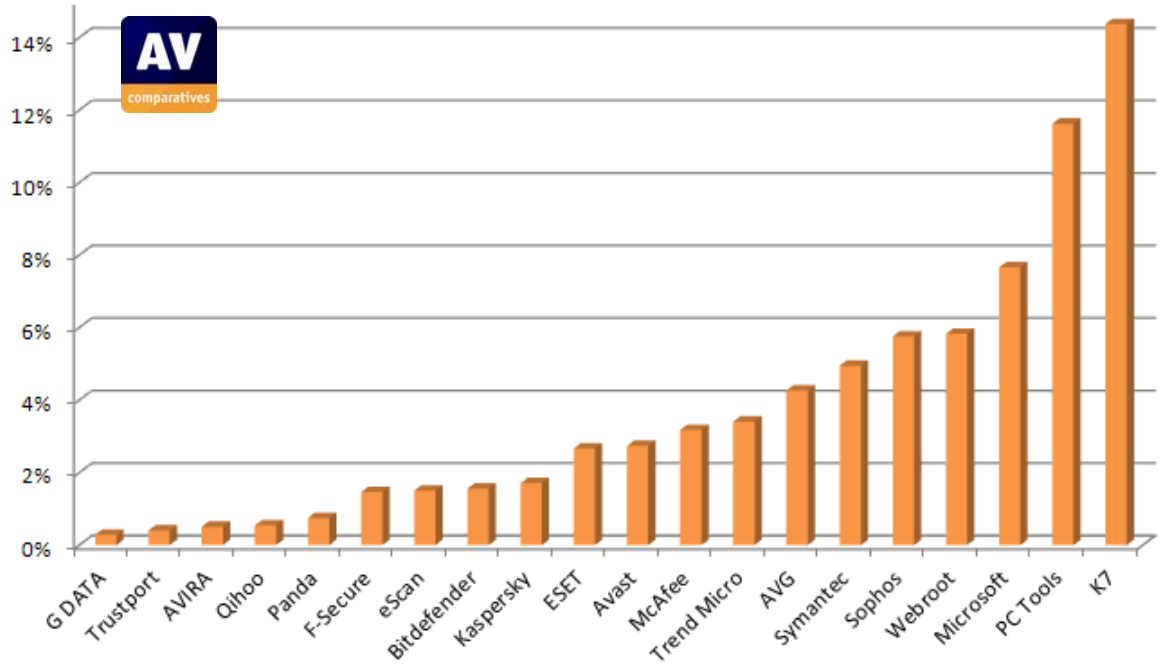
	Detection Rate Clusters/Groups (given by the testers after consulting statistical methods)			
	4	**3**	**2**	**1**
Few (0-15 FP's)	**TESTED**	**STANDARD**	**ADVANCED**	**ADVANCED+**
Many (16-100 FP's)	**TESTED**	**TESTED**	**STANDARD**	**ADVANCED**
Very many (101-500 FP's)	**TESTED**	**TESTED**	**STANDARD**	**STANDARD**
Crazy many (over 500 FP's)	**TESTED**	**TESTED**	**TESTED**	**TESTED**

We observed some few vendors potentially are trying to game the tests to get higher scores. Such practices include e.g. strongly disputing malicious files as "clean" or "potentially wanted software" etc. Some try disputing every malicious files which are not detected by the own product as "unimportant/non-prevalent", even if other telemetry data shows otherwise. Sometimes some vendors also claim that their cloud should have been detecting all the samples that according to us where not detected. Often we could prove that even with an actual cloud/product they are not detected or could not have been detected back then. In our opinion, vendors which rely on the cloud should make sure that their products are always able to send/get cloud data and warn the user if their cloud is offline/unreachable. If a vendors cloud is down or unreachable at time of testing, it is the fault of the product/vendor and not of the user or test as long as it is done with enabled Internet connection.

The results reflect the detection rate provided at that time. If certain clouds require a perfectly stable and ultra-fast internet connection, this should be made clear in the system requirements. Otherwise vendors should provide local clouds to home users like some are already doing for corporates with strict privacy policies.

Furthermore, some vendors which see themselves scoring low in a test often aim to get their results removed from a test for marketing reasons. But we do not allow to withdraw from tests as we want to provide results to our readers. We might think in future about ways to solve this problems, too.

Graph of missed samples (lower is better)



During the test Sophos and Webroot (who also use Sophos technology) scored lower detection rates due to issues with their cloud technology. The results shown include estimated cloud detections (but are listed out of competition).

Percentages refer to the used test-set only. Even if it is just a subset of malware, it is important to look at the number of missed malware.

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 Anti-Virus product. Additionally, most products provide at least some kind of HIPS, behaviour-based, reputation-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.

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 completely new/unknown malware (by on-demand/on-access scanner with local heuristic and generic signatures without cloud).

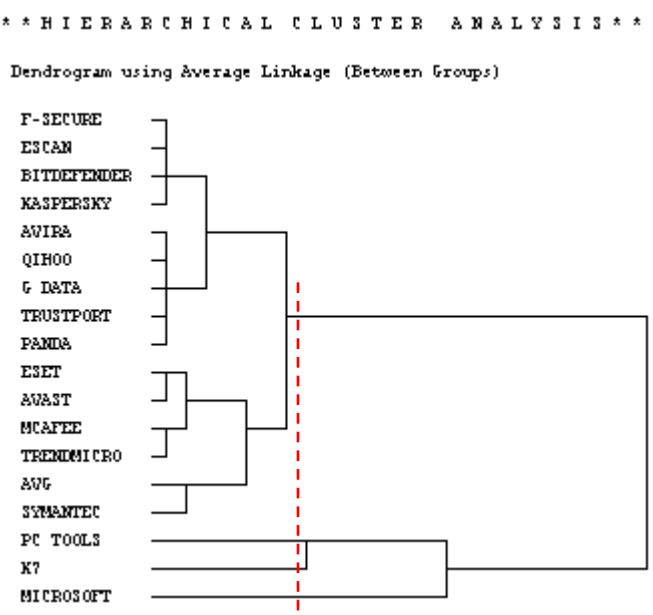
Even if we deliver various tests and show different aspects of Anti-Virus software, users are advised to evaluate the software by themselves and build their own opinion about them. Test data or reviews just provide guidance to some aspects that users cannot evaluate by themselves. We suggest and encourage readers to research also other independent test results provided by various well-known and established 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

Please consider also the false alarm rates when looking at the below detection rates[3].

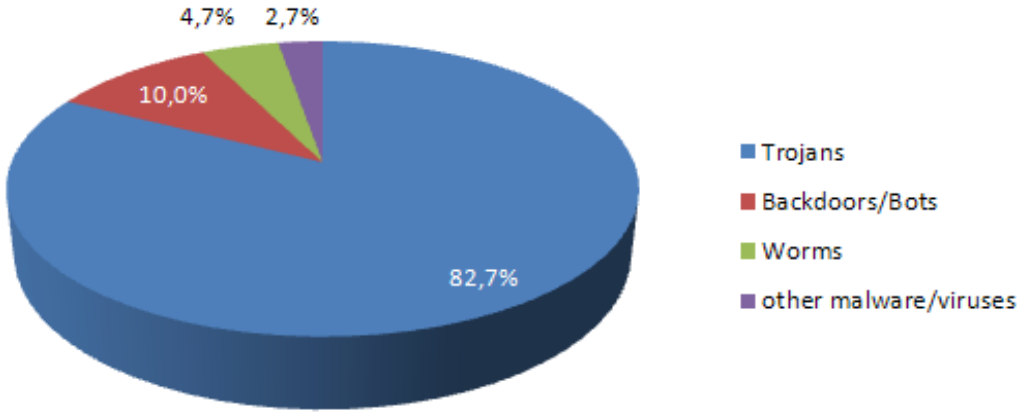
Total detection rates (clustered into four groups):

1.	G DATA	99.7%
2.	Trustport	99.6%
3.	AVIRA, Qihoo	99.5%
4.	Panda	99.3%
5.	F-Secure, eScan	98.5%
6.	Bitdefender	98.4%
7.	Kaspersky	98.3%
8.	ESET, Avast	97.3%
9.	McAfee	96.8%
10.	Trend Micro	96.6%
11.	AVG	95.7%
12.	Symantec	95.1%
13.	Microsoft	92.3%
14.	PC Tools	88.4%
15.	K7	85.6%



During the test Sophos and Webroot (who also use Sophos technology) scored lower detection rates due to issues with their cloud technology. Further investigations working with the vendor could not determine the root cause of the issue and the results shown include cloud detections. As we are unable to fully verify them independently (as the cloud can not be reverted back), the results of Webroot and Sophos are shown "out of competition". The results of Sophos and Webroot are only a rough estimate. Sophos and Webroot had a detection rate of ~94.2%[4].

The used test-set contains about 200-thousands recent/prevalent malware samples from last months and consists of:



[3] We estimate the remaining error margin to be under 0.2%

[4] Although the affected vendors are in good-standing, we have to handle their cloud-issue this way to avoid potential misuse / gaming of other future vendors in future tests.

False positive/alarm test

In order to better evaluate the quality of the detection capabilities (distinguish good files from malicious files) of anti-virus products, we provide 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. All discovered false alarms were reported/sent to the respective Anti-Virus vendors and have been fixed.

False Positive Results

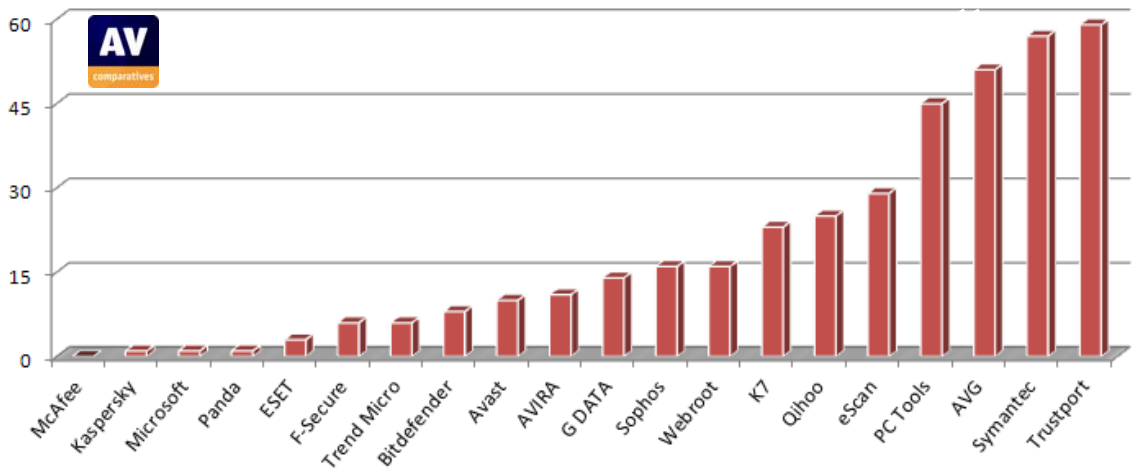
Number of false alarms found in our set of clean files (lower is better):

1.	McAfee	0	
2.	Kaspersky, Microsoft, Panda	1	very few FPs
3.	ESET	3	
4.	F-Secure, Trend Micro	6	
5.	Bitdefender	8	
6.	Avast	10	few FP's
7.	AVIRA	11	
8.	G DATA	14	
9.	Sophos, Webroot	16*	
10.	K7	23	
11.	Qihoo	25	
12.	eScan	29	
13.	PC Tools	45	many FP's
14.	AVG	51	
15.	Symantec	57	
16.	TrustPort	59	

* Due to issues with the cloud technology of Sophos/Webroot, we can not know if there would have been more FPs if the cloud connection would have been worked properly. Their results are listed out of competition.

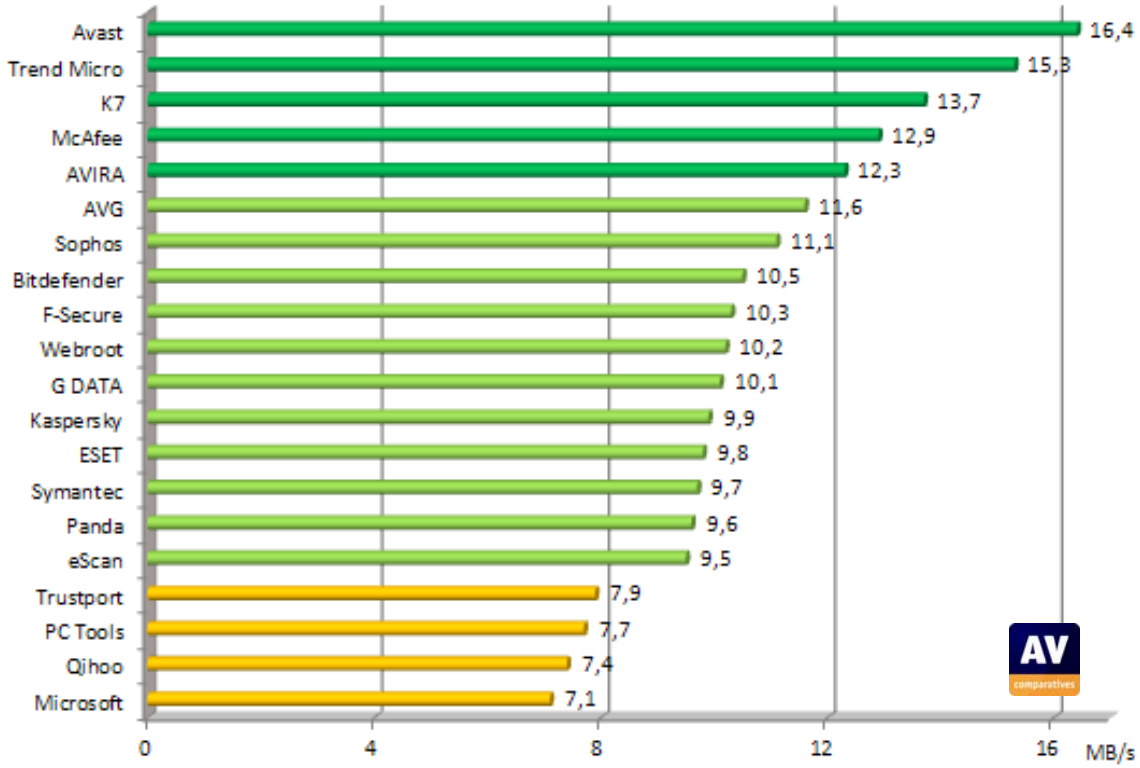
Comments and details about the discovered false alarms (including their assumed prevalence) can be seen in a separate report available at:
http://www.av-comparatives.org/images/stories/test/fp/avc_fp_aug2011.pdf

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



On-Demand 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 querying cloud data, 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, if it really scans all file types (or uses e.g. white lists in the cloud), etc. Most 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 fingerprinting technologies are disabled and 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 the 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 files[5], 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.
In 2012 we will no longer provide the on-demand scanning speed test[6].

[5] to know how fast various products would be on *your* PC at scanning *your* files, we advise you to try the products yourself
[6] Various performance tests can be found at: http://www.av-comparatives.org/comparativesreviews/performance-tests

Award levels reached in this test

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

AWARDS (based on detection rates and false alarms)	PRODUCTS
	✓ G DATA ✓ AVIRA ✓ Panda ✓ F-Secure ✓ Bitdefender ✓ Kaspersky ✓ ESET ✓ Avast ✓ McAfee ✓ Trend Micro
	✓ Trustport* ✓ Qihoo* ✓ eScan* ✓ AVG* ✓ Symantec* ✓ Microsoft
	-
	✓ PC Tools* ✓ K7

*: those products got lower awards due false alarms

Sophos and Webroot were tested out of competition (see comments on page 9), due to issues with their cloud technology during the testing period.

The Awards are not only based on detection rates - also False Positives found in our set of clean files are considered. On page 7 of this report you can see how awards are being given.

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.

Copyright and Disclaimer

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

AV-Comparatives e.V. (September 2011)