Anti-Virus Comparative



File Detection Test of Malicious Software

including false alarm test

Language: English

March 2015

Last Revision: 30th April 2015

www.av-comparatives.org

Table of Contents



Tested Products	3
Introduction	4
Graph of missed samples	6
Results	7
False positive (false alarm) test	8
Award levels reached in this test	9
Convright and Disclaimer	10



Tested Products

- Avast Free Antivirus 2015
- AVG Internet Security 2015
- AVIRA Antivirus Pro 15.0
- Baidu Antivirus 5.0
- Bitdefender Internet Security 2015
- BullGuard Internet Security 15.0
- Emsisoft Anti-Malware 9.0
- eScan Internet Security 14.0
- ESET Smart Security 8.0
- F-Secure Internet Security 2015
- Fortinet FortiClient 5.2

- Kaspersky Internet Security 2015
- Lavasoft Ad-Aware Free Antivirus+ 11.5
- McAfee Internet Security 2015
- Microsoft Security Essentials 4.7
- Panda Free Antivirus 15.1
- Quick Heal Total Security 16.0
- Sophos Endpoint Security and Control 10.3
- Tencent PC Manager 10.4
- ThreatTrack Vipre Internet Security 8.0
- Trend Micro Internet Security 8.0

Introduction

Before proceeding with this report, readers are advised to first read the methodology documents as well as the information provided on our website. The malware sets were frozen on the 17th February 2015 and consisted of 131189 malware samples. The products had Internet/cloud-access during the test, were last updated on the 3rd of March 2015 and tested under Microsoft¹ Windows 7 SP1 64-Bit. The following up-to-date products² were included in this public test (most current versions available at the time of testing):

- Avast Free Antivirus 2015.10.2.2214
- AVG Internet Security 2015.0.5751
- AVIRA Antivirus Pro 15.0.8.644
- Baidu Antivirus 5.0.9.104946
- Bitdefender Internet Security 18.21.0.1497
- BullGuard Internet Security 15.0.295.1
- Emsisoft Anti-Malware 9.0.0.4985
- eScan Internet Security 14.0.1400.1700
- ESET Smart Security 8.0.304.0
- F-Secure Internet Security 2015
- Fortinet FortiClient 5.2.3.0633

- Kaspersky Internet Security 15.0.2.361
- Lavasoft Ad-Aware Free Antivirus+ 11.5.202.7299
- McAfee Internet Security 18.0.177
- Microsoft Security Essentials 4.7.205.0
- Panda Free Antivirus 15.1.0
- Quick Heal Total Security 16.00.9.0.0.16
- Sophos Endpoint Security and Control 10.3.12.89
- Tencent PC Manager 10.4.25461.501
- ThreatTrack Vipre Internet Security 8.0.5.3
- Trend Micro Internet Security 8.0.1133

Please try the products³ 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, compatibility, graphical user interface, support, etc.) to consider. Although very important, the file detection rate of a product is only one aspect of a complete anti-virus product. AV-Comparatives also provides a whole-product dynamic "real-world" protection test, as well as other test reports that cover different aspects/features of the products. We invite users to look at our other tests and not only at this type of test. A good file detection rate is still one of the most important, deterministic and reliable basic features of an anti-virus product. Additionally, most products provide at least some kind of functionality to block (or 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 has failed (these protection features are evaluated in other types of tests that we provide on our website).

All products were tested using default settings. Although the test-set contains only executable (PE) files, we enabled scan of all files, scan of archives and scan for PUA in all products.

³ Information about additional third-party engines/signatures used inside the products: **BullGuard**, **Emsisoft**, **eScan**, **F-Secure**, **Lavasoft** and **Quick Heal** (Total Security) use the Bitdefender engine. **Baidu** (English version) and **Tencent** use the Avira engine.



- 4 -

¹ We additionally tested the Windows Defender included in Windows 8 (we observed the same results as achieved by Security Essentials under Windows 7).

² Qihoo 360 has been suspended from the 2015 public main-test series – its results have been removed.

In principle, we used Internet security suites for this test. However, some vendors asked us to test their (free) antivirus program instead, which we did.

Notes: Baidu decided to participate with their English language Baidu Antivirus (Enhanced Version) (http://sadu.baidu.com/en/) which is based on the Avira engine instead of the Kaspersky engine. Quick Heal participated with their Total Security product version which is based on the Bitdefender engine and their in-house engine, while their other products are based only on their in-house engine. Therefore, the results of this test apply only to the tested products and not to any other products on any official website of these vendors.

Although no samples were executed during this test, we considered cases where malware would be recognized on-access, but not on-demand. The test is thus called File Detection Test (as opposed to the earlier On-Demand Tests), as on-access scanning is taken into consideration.

Several products make use of cloud technologies, which require an active Internet connection. Our tests are performed using an active Internet connection. Users should be aware that detection rates may in some cases be drastically lower if the scan is performed while offline (or when the cloud service is unreachable for various reasons). 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 appropriately warned in the event that the connectivity to the cloud is lost, which may considerably affect the protection provided, and e.g. make an initiated scan useless. While in our test we check whether the cloud services of the respective security vendors are reachable, users should be aware that being online does not necessarily mean that the cloud service of the products they use is reachable/working properly. In fact, sometimes products with cloud functionality have various network issues due to which no cloud security is provided, but the user is not warned. AMTSO⁴ has a rudimentary test to verify the proper functionality of cloud-supported products.

The test-set used has been built consulting telemetry data with the aim of including prevalent samples from the last weeks/months prior to the test date which are/were endangering users in the field.

Even if we deliver various tests and show different aspects of anti-virus software, users are advised to evaluate the software by themselves and form their own opinions about them. Test data or reviews just provide guidance on some aspects that users cannot evaluate by themselves. We encourage readers to additionally consult 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. A list of various reputable testing labs can be found on our website.

The overall standard of detection in this test is very high. This is partly due to the focus on prevalent malware samples, and partly due to the time required to find out what is prevalent and for sample verification. The results may indirectly show which products have a lower time-to-detect rate, i.e. are faster in detecting/reacting to new malware. Furthermore, several products in the test make use of third-party engines (see footnote on page 4), due to which they all score similarly highly.

_

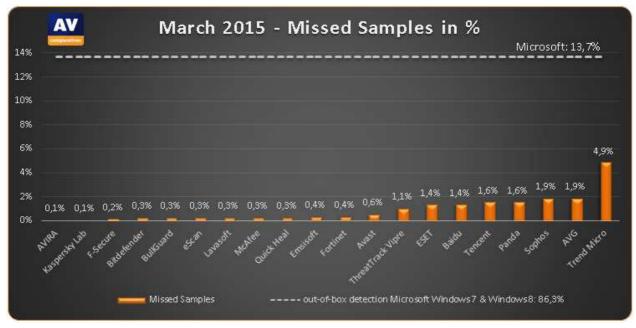


^{4 &}lt;a href="http://www.amtso.org/check-desktop">http://www.amtso.org/check-desktop

The malware detection rates are grouped by the testers after looking at the clusters built with the hierarchal clustering method. However, the testers do not stick rigidly to this in cases where it would not make sense. For example, in a scenario where all products achieve low detection rates, the highest-scoring ones will not necessarily receive the highest possible award.

	Detection Rate Clusters/Groups (given by the testers after consulting statistical methods)			
	4	3	2	1
Very few (0-1 FP's) Few (2-10 FP's)	TESTED	STANDARD	ADVANCED	ADVANCED+
Many (11-50 FP's)	TESTED	TESTED	STANDARD	ADVANCED
Very many (51-100 FP's)	TESTED	TESTED	TESTED	STANDARD
Crazy many (over 100 FP's)	TESTED	TESTED	TESTED	TESTED

Graph of missed samples (lower is better)



The graph above shows the test results against "out-of-box" malware detection provided by Microsoft Windows. In Windows 8, this is provided by Windows Defender, which is pre-installed by default with the operating system. The equivalent in Windows 7 is Microsoft Security Essentials, which is not pre-installed, but can easily be added for free as an option via the Windows Update service. We use this to compare the value of this feature – i.e. static malware detection - provided to users of third-party Anti-Virus solutions.



Results

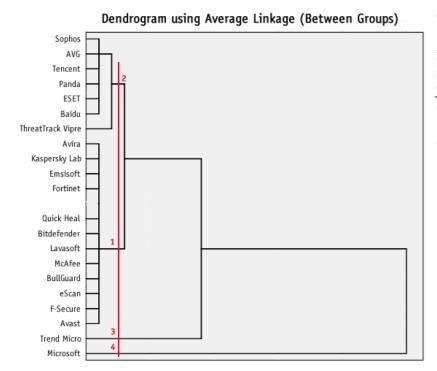
Total detection rates (clustered in groups):

Please consider also the false alarm rates when looking at the file detection rates below.

1.	AVIRA, Kaspersky Lab	99.9%
2.	F-Secure	99.8%
3.	Bitdefender, BullGuard, eScan,	99.7%
	Lavasoft, McAfee, Quick Heal	
4.	Emsisoft, Fortinet	99.6%
5.	Avast	99.4%
6.	ThreatTrack Vipre	98.9%
7.	ESET, Baidu	98.6%
8.	Tencent, Panda	98.4%
9.	Sophos, AVG	98.1%
10.	Trend Micro	95.1%
11.	Microsoft	86.3%

The test-set used contained 131189 recent/prevalent samples⁵ from last few weeks/months.

Hierarchical Cluster Analysis



This dendrogram shows the results of the cluster analysis⁶. It indicates at what level of similarity the clusters are joined. The red drafted line defines the level of similarity. Each intersection indicates a group.



⁵ We estimate the remaining error margin on the final percentages to be below 0.2%

⁶ For more information about cluster analysis, see e.g. this easy to understand tutorial: http://strata.uqa.edu/software/pdf/clusterTutorial.pdf

False positive (false alarm) test

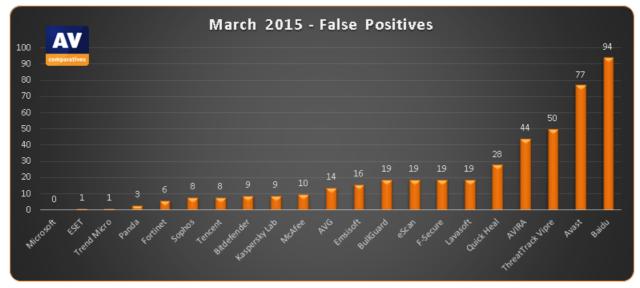
In order to better evaluate the quality of the file detection capabilities (distinguish good files from malicious files) of anti-virus products, we provide a false alarm test. False alarms can sometimes cause as much trouble as a real infection. Please consider the false alarm rate when looking at the detection rates, as a product which is prone to false alarms achieves higher detection rates more easily.

False Positive Results

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

1.	Microsoft	0	
2.	ESET, Trend Micro	1	very few FPs
3.	Panda	3	
4.	Fortinet	6	
5.	Sophos, Tencent	8	few FP's
6.	Bitdefender, Kaspersky Lab	9	
7.	McAfee	10	
8.	AVG	14	
9.	Emsisoft	16	
10.	BullGuard, eScan,	19	
	F-Secure, Lavasoft		many FP's
11.	Quick Heal	28	
12.	AVIRA	44	
13.	ThreatTrack Vipre	50	
14.	Avast	77	very many FP's
15.	Baidu	94	

Details about the discovered false alarms (including their assumed prevalence) can be seen in a separate report available at: http://www.av-comparatives.org/wp-content/uploads/2015/04/avc-fps-201503-en.pdf



A product that is successful at detecting a high percentage of malicious files but suffers from false alarms may not be necessarily better than a product which detects less malicious files but which generates fewer false alarms.



Award levels reached in this test

AV-Comparatives provides ranking awards. As this report also contains 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 ⁷
ADVANCED+ ADVANCED+ FILE DETECTION TEST Comparatives MAR 2015	✓ Kaspersky Lab ✓ Bitdefender ✓ McAfee ✓ Fortinet
ADVANCED ADVANCED FILE DETECTION TEST Comparatives MAR 2015	✓ AVIRA* ✓ F-Secure* ✓ eScan* ✓ BullGuard* ✓ Lavasoft* ✓ Quick Heal* ✓ Emsisoft* ✓ ESET ✓ Tencent ✓ Panda ✓ Sophos
STANDARD FILE DETECTION TEST Comparatives MAR 2015	✓ ThreatTrack Vipre* ✓ AVG* ✓ Avast* ✓ Trend Micro
TESTED FILE DETECTION TEST Comparatives MAR 2015	✓ Baidu*

^{*:} these products got lower awards due to false alarms

The awards are not only based on detection rates - also false positives found in our set of clean files are considered. On page 6 of this report you can see how the awards are given.

⁷ Microsoft security products are not included in the awards page, as their out-of-box detection is included in the operating system and therefore out-of-competition.



- 9 -

Copyright and Disclaimer

This publication is Copyright © 2015 by AV-Comparatives ®. 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, 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.

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

AV-Comparatives (April 2015)

