Anti-Virus Comparative

File Detection Test of Malicious Software

including false alarm test

Language: English
March 2016

Last Revision: 14th April 2016

www.av-comparatives.org

Table of Contents

Tested Products

- Avast Free Antivirus 11.1
- AVG Internet Security 2016
- AVIRA Antivirus Pro 15.0
- Bitdefender Internet Security 20.0
- BullGuard Internet Security 16.0
- Emsisoft Anti-Malware 11.0
- eScan Internet Security 14.0
- ESET Smart Security 9.0
- F-Secure Safe 14.150
- Fortinet FortiClient 5.2
- Kaspersky Internet Security 16.0
- Lavasoft Ad-Aware Pro Security 11.10
- McAfee Internet Security 18.0
- Microsoft Windows Defender 4.9
- Quick Heal Total Security 16.0
- Sophos Endpoint Security and Control 10.3
- Tencent PC Manager 11.2
- ThreatTrack VIPRE Internet Security Pro 9.3
- Trend Micro Internet Security 10.0

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 24th February 2016 and consisted of 163763 malware samples. The products had Internet/cloud-access during the test, were last updated on the 3th of March 2016 and tested under Microsoft Windows 10 64-Bit. The following up-to-date products were included in this public test (most current versions available at the time of testing):

- Avast Free Antivirus 11.1.2245
- AVG Internet Security 2016.0.7442
- AVIRA Antivirus Pro 15.0.16.282
- Bitdefender Internet Security 20.0.25.1377
- BullGuard Internet Security 16.0.315.1
- Emsisoft Anti-Malware 11.0.0.6191
- eScan Internet Security 14.0.1400.1831
- ESET Smart Security 9.0.349
- F-Secure Safe 14.150.101
- Fortinet FortiClient 5.2.5.0658
- Kaspersky Internet Security 16.0.1.445 (a)
- Lavasoft Ad-Aware Pro Security 11.10.767.8917
- McAfee Internet Security 18.0.5011
- Microsoft Windows Defender 4.9.10586.0
- Quick Heal Total Security 16.00.9.0.24.4
- Sophos Endpoint Security and Control 10.3.15.69
- Tencent PC Manager 11.2.26147.901
- ThreatTrack VIPRE Internet Security Pro 9.3.2.17
- Trend Micro Internet Security 10.0.1186

Please try the products[1] 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.

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.

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

Notes: ***Tencent*** participates with their official English language Tencent PC Manager (http://www.pcmgr-global.com), which is based on the Bitdefender engine and their in-house engine. ***Quick Heal*** participates 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. AMTSO[2] 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. Furthermore, the distribution of families in the test-set has been weighted based on family-prevalence and was build based on Microsoft's global telemetry data. This means that as more prevalent a malware family is, as more samples from that family are included in the test-set.

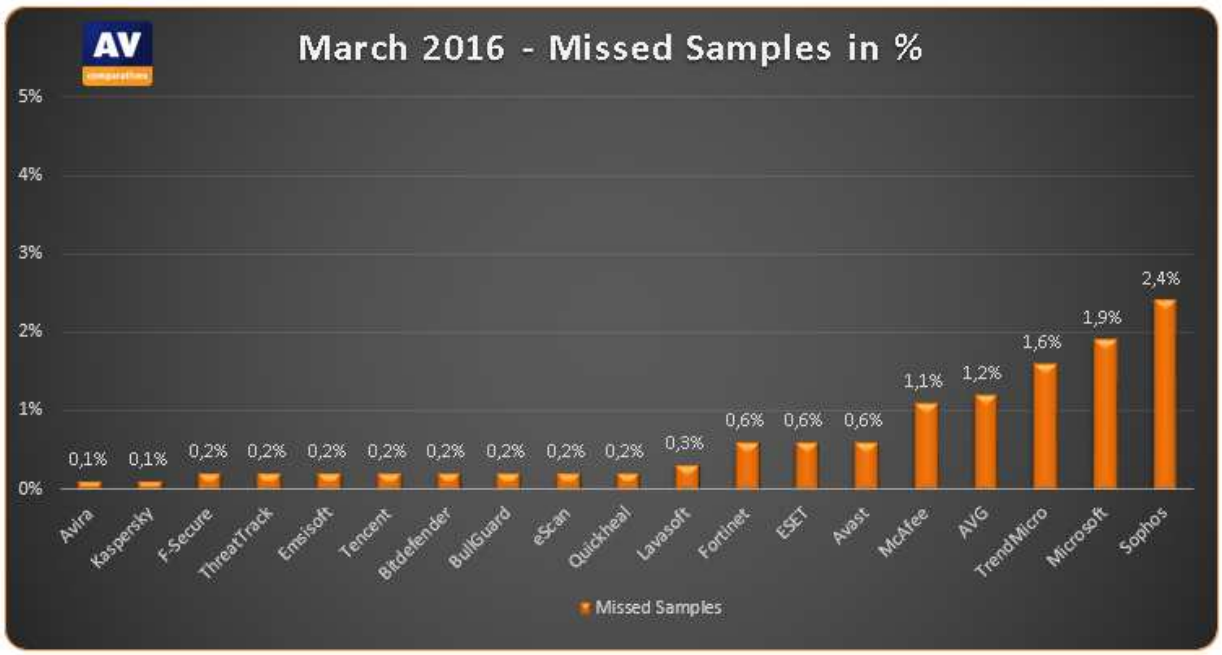
Even if we deliver various tests and show different aspects of anti-virus software, users are advised to evaluate the software by themselves and form their own opinions about them. Test data or reviews just provide guidance on some aspects that users cannot evaluate by themselves. We encourage readers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

[2] http://www.amtso.org/feature-settings-check-for-desktop-solutions/

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)



Results

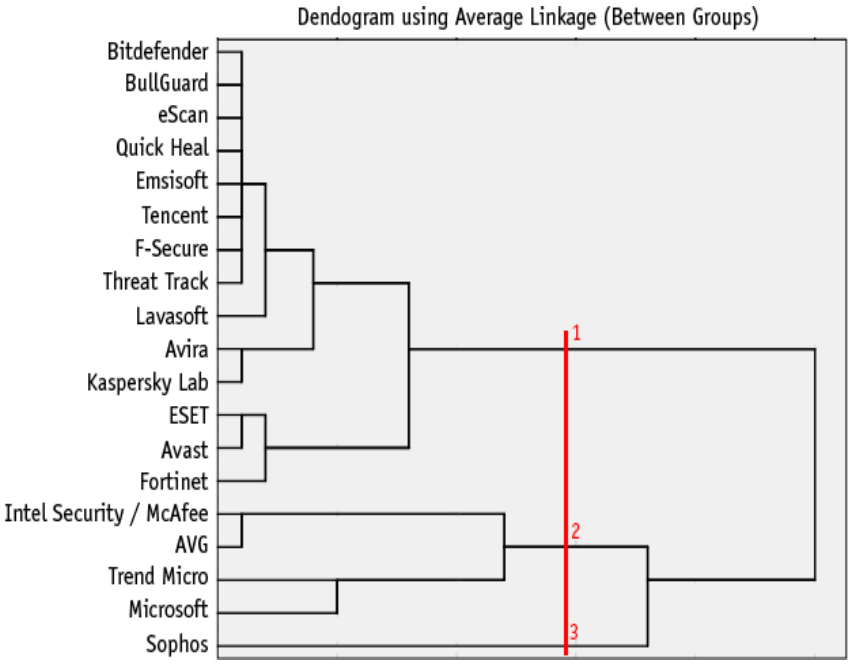
Total detection rates (clustered in groups):

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

1.	AVIRA, Kaspersky Lab	99.9%
2.	F-Secure, ThreatTrack, Emsisoft, Tencent, Bitdefender, BullGuard, eScan, Quick Heal	99.8%
3.	Lavasoft	99.7%
4.	Fortinet, ESET, Avast	99.4%
5.	McAfee	98.9%
6.	AVG	98.8%
7.	Trend Micro	98.4%
8.	Microsoft	98.1%
9.	Sophos	97.6%

The test-set used contained 163763 recent/prevalent samples[3] from last few weeks/months.

Hierarchical Cluster Analysis



This dendrogram shows the results of the cluster analysis[4]. 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.

[3] We estimate the remaining error margin on the final percentages to be below 0.2%
[4] For more information about cluster analysis, see e.g. this easy to understand tutorial: http://strata.uga.edu/software/pdf/clusterTutorial.pdf

False positive (false alarm) test

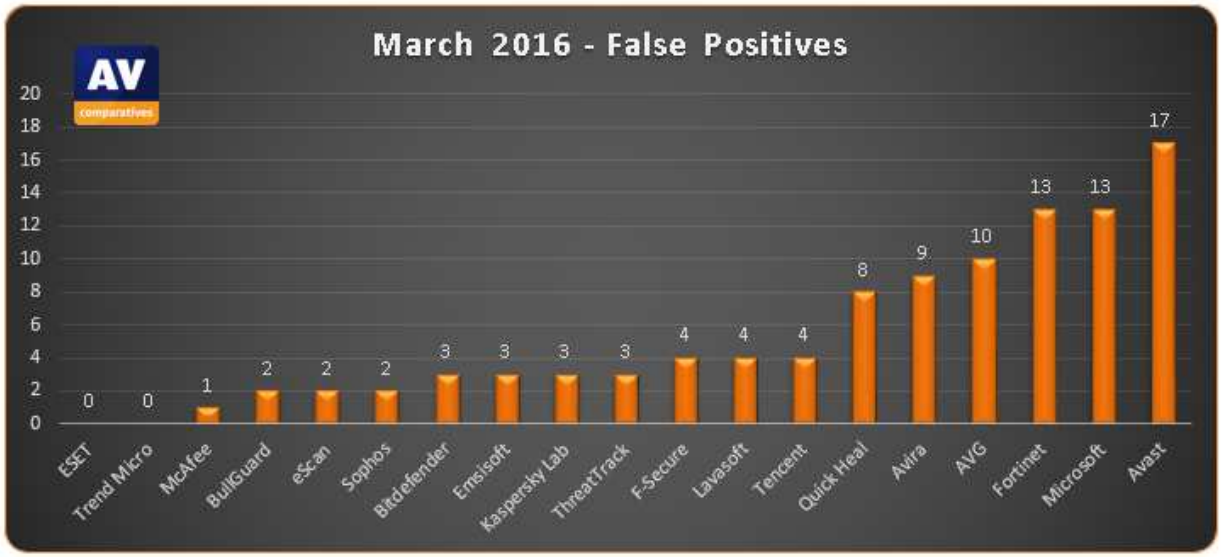
In order to better evaluate the quality of the file detection capabilities (distinguish good files from malicious files) of anti-virus products, we provide a false alarm test. False alarms can sometimes cause as much trouble as a real infection. Please consider the false alarm rate when looking at the 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.	ESET, Trend Micro	0	none/very few FPs
2.	McAfee	1	
3.	BullGuard, eScan, Sophos	2	
4.	Bitdefender, Emsisoft, Kaspersky Lab, ThreatTrack	3	
5.	F-Secure, Lavasoft, Tencent	4	few FP's
6.	Quick Heal	8	
7.	AVIRA	9	
8.	AVG	10	
9.	Fortinet, Microsoft	13	many FP's
10.	Avast	17	

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/2016/04/avc_fps_201603_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
	✓ AVIRA ✓ Kaspersky Lab ✓ F-Secure ✓ ThreatTrack ✓ Emsisoft ✓ Tencent ✓ Bitdefender ✓ BullGuard ✓ eScan ✓ Quick Heal ✓ Lavasoft ✓ ESET
	✓ Fortinet* ✓ Avast* ✓ McAfee ✓ AVG ✓ Trend Micro
	✓ Microsoft* ✓ Sophos
	✓ -

*: 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.

Copyright and Disclaimer

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

AV-Comparatives (April 2016)