Anti-Virus Comparative

File Detection Test of Malicious Software

including false alarm test

Language: English
March 2014

Last Revision: 22nd April 2014

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
Copyright and Disclaimer	10

Tested Products

- AhnLab V3 Internet Security 8.0
- avast! Free Antivirus 2014
- AVG Internet Security 2014
- AVIRA Internet Security 14.0
- Baidu Antivirus 2014 (English)
- Bitdefender Internet Security 2014
- BullGuard Internet Security 14.0
- Emsisoft Anti-Malware 8.1
- eScan Internet Security 14.0
- ESET Smart Security 7.0
- F-Secure Internet Security 2014
- Fortinet FortiClient 5.0
- Kaspersky Internet Security 2014
- Kingsoft Internet Security 2013.SP6
- Lavasoft Ad-Aware Free Antivirus+ 11.1
- McAfee Internet Security 2014
- Microsoft Security Essentials 4.4
- Panda Cloud Free Antivirus 2.3
- Qihoo 360 Internet Security 4.9 (English)
- Sophos Endpoint Security and Control 10.3
- Tencent QQ PC Manager 8.9
- ThreatTrack Vipre Internet Security 7.0
- Trend Micro Titanium Internet Security 2014

Introduction

Before proceeding with this report, readers are advised to first read the methodology documents as well as the information provided on our website. Malware was collected up to the 21st February 2014 and consisted of 125977 malware samples. The products had Internet/cloud-access during the test, were last updated on the 7th of March 2014 and tested under Microsoft[1] Windows 7 SP1 64-Bit. The following up-to-date products were included in this public test (most current versions available at the time of testing):

- AhnLab V3 Internet Security 8.0.8.2
- avast! Free Antivirus 2014.9.0.2013
- AVG Internet Security 2014.0.4335
- AVIRA Internet Security 14.0.3.350
- Baidu Antivirus 4.0.9.57999 (EN)
- Bitdefender Internet Security 17.26.0.1106
- BullGuard Internet Security 14.0.278.3
- eScan Internet Security 14.0.1400.1572
- Emsisoft Anti-Malware 8.1.0.40
- ESET Smart Security 7.0.302.26
- F-Secure Internet Security 14.99.103
- Fortinet FortiClient 5.0.8.344
- Kaspersky Internet Security 14.0.0.4651 (e)
- Kingsoft Internet Security 2013.SP6.0.030511
- Lavasoft Ad-Aware Free Antivirus+ 11.1.5354.0
- McAfee Internet Security 16.8.708
- Microsoft Security Essentials 4.4.304.0
- Panda Cloud Free Antivirus 2.3.0
- Qihoo 360 Internet Security 4.9.0.4109 (EN)
- Sophos Endpoint Security and Control 10.3.1
- Tencent QQ PC Manager 8.9.25000.501
- ThreatTrack Vipre Internet Security 7.0.6.2
- Trend Micro Titanium Internet Security 7.0.1206

Please note that Baidu and Qihoo wanted to have their official international/English product versions included in this test, which we did. However, we must point out that the English product versions from these vendors are completely different products (different engines, different default settings, etc.) compared to their Chinese versions. Therefore, the results are not applicable for the Chinese product versions.

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, 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).

---

[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] Information about additional third-party engines/signatures used inside the products: **BullGuard**, **Emsisoft**, **eScan**, **F-Secure, Kingsoft**, **Lavasoft** and **Qihoo** use the Bitdefender engine. **Baidu** and **Tencent** use the Avira engine.

All products were tested using default settings. Although the test-set contains only executable (PE) malicious 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. In this test, we would not expect to see any difference between an antivirus program and an Internet security suite.

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 Test), as on-access scanning is taken into consideration. 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.

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[3] 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.

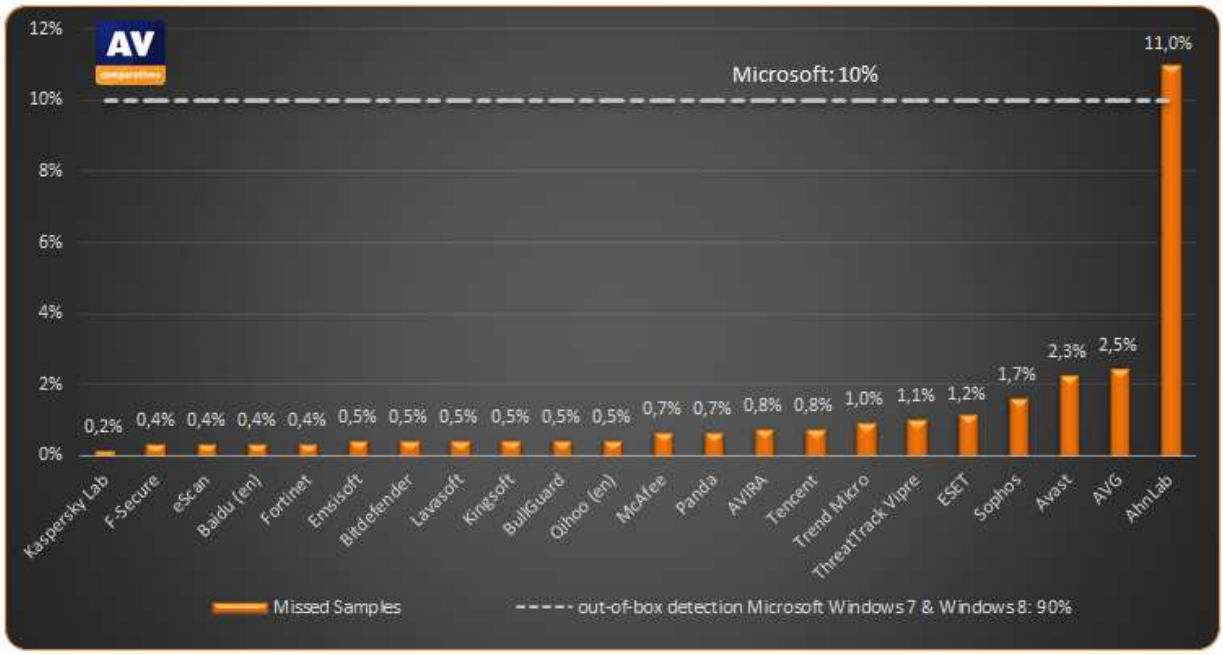
The overall standard of detection in this test is very high. This is partly due to the focus on prevalent malware samples, and partly due to the time required to find out what is prevalent and for sample verification. The results may indirectly show which products have a lower time-to-detect rate, i.e. 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.

[3] http://www.amtso.org/feature-settings-check-cloud-lookup.html

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. As we have reduced the size of the test-set by removing some further old software files, we have also reduced the threshold levels for false positives (i.e. the "Many" category starts at 11 instead of 16). Further adaptions may be done in future.

	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

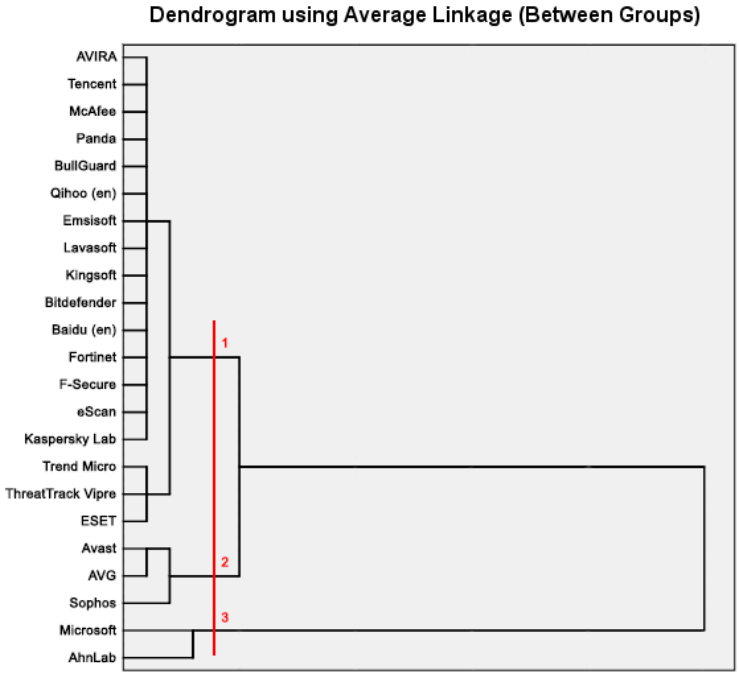
Total detection rates (clustered in groups):

Please consider also the false alarm rates when looking at the file detection rates below[4].

1.	Kaspersky Lab	99.8%
2.	F-Secure, eScan, Baidu (en), Fortinet	99.6%
3.	Emsisoft, Bitdefender, Lavasoft, Kingsoft², BullGuard, Qihoo (en)	99.5%
4.	McAfee, Panda	99.3%
5.	AVIRA, Tencent	99.2%
6.	Trend Micro	99.0%
7.	ThreatTrack Vipre	98.9%
8.	ESET	98.8%
9.	Sophos	98.3%
10.	Avast	97.7%
11.	AVG	97.5%
12.	Microsoft	90.0%
13.	AhnLab	89.0%

The test-set used contained 125977 recent/prevalent samples[5] from last few weeks/months.

Hierarchical Cluster Analysis



This dendrogram shows the results of the cluster analysis[6]. 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.

[4] Tests of some additional products have been commissioned by IT publications, and although they are not included in this report, for some of them (G DATA, Symantec, ...) results can be requested using the following link or can be read in the printed magazines. http://bit.ly/1lj0MWo

[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.uga.edu/software/pdf/clusterTutorial.pdf

False positive (false alarm) test

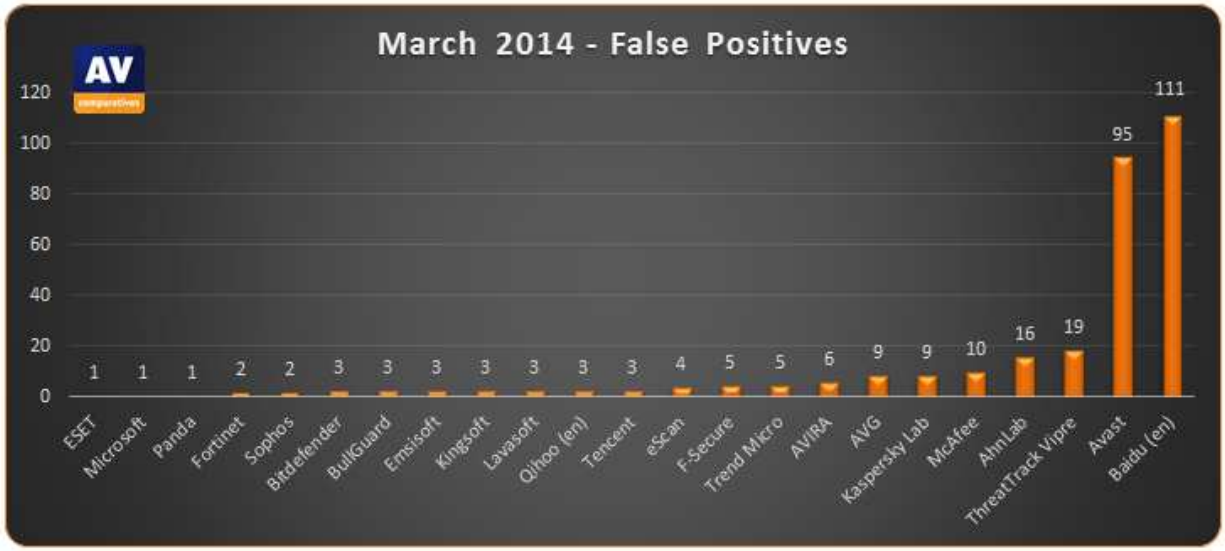
In order to better evaluate the quality of the file detection capabilities (distinguish good files from malicious files) of anti-virus products, we provide a false alarm test. False alarms can sometimes cause as much trouble as a real infection. Please consider the false alarm rate when looking at the 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, Microsoft, Panda	1	very few FPs
2.	Fortinet, Sophos	2	
3.	Bitdefender, BullGuard, Emsisoft, Kingsoft, Lavasoft, Qihoo, Tencent	3	
4.	eScan	4	few FP's
5.	F-Secure, Trend Micro	5	
6.	AVIRA	6	
7.	AVG, Kaspersky Lab	9	
8.	McAfee	10	
9.	AhnLab	16	many FP's
10.	ThreatTrack Vipre	19	
11.	Avast	95	very many FP's
12.	Baidu	111	crazy many FP's

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/2014/04/avc_fps_201403_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]
AV comparatives ADVANCED+ ★★★ FILE DETECTION TEST MAR 2014	✓ Kaspersky Lab ✓ F-Secure ✓ eScan ✓ Fortinet ✓ Emsisoft ✓ Bitdefender ✓ Lavasoft ✓ BullGuard ✓ Qihoo (en) ✓ McAfee ✓ Panda ✓ AVIRA ✓ Tencent ✓ Trend Micro ✓ ESET
AV comparatives ADVANCED ★★ FILE DETECTION TEST MAR 2014	✓ ThreatTrack Vipre* ✓ Sophos ✓ AVG
AV comparatives STANDARD ★ FILE DETECTION TEST MAR 2014	-
AV comparatives TESTED FILE DETECTION TEST MAR 2014	✓ Baidu (en)* ✓ Avast* ✓ AhnLab*

*: 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.
Kingsoft is not included in the awards page as the tested product was a non-final version using a different third-party engine.

Copyright and Disclaimer

This publication is Copyright © 2014 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 2014)