Anti-Virus Comparative

Retrospective/Proactive test

Heuristic and behavioural protection
against new/unknown malicious software

Language: English
March 2015
Last revision: 26th June 2015

www.av-comparatives.org

Contents

1. Introduction 3

2. Description 3

3. False-alarm test 5

4. Test Results 5

5. Summary results 6

6. Awards reached in this test 7

7. Copyright and disclaimer 8

1. Introduction

This test report is the second part of the March 2015 test[1]. The report is delivered several months later due to the large amount of work required, deeper analysis, preparation and dynamic execution of the retrospective test-set. This type of test is performed only once a year and includes a behavioural protection element, where any malware samples are executed, and the results observed. Although it is a lot of work, we usually receive good feedback from various vendors, as this type of test allows them to find bugs and areas for improvement in the behavioural routines (as this test evaluates specifically the proactive heuristic and behavioural protection components). Feedback from users (especially corporate users) indicates that they appreciate the findings from this type of test.

The products used the same updates and signatures that they had on the 3rd March 2015. This test shows the proactive protection capabilities that the products had at that time. We used 1,463 new and relevant (i.e. prevalent malware files and families) malware samples that appeared for the first time shortly after the freezing date. The following 12 products were tested:

- Avast Free Antivirus 2015
- Bitdefender Internet Security 2015
- BullGuard Internet Security 2015
- 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
- Microsoft Security Essentials 4.7
- ThreatTrack Vipre Internet Security 8.0

This test is an optional part of our public main test-series, that is to say, manufacturers can decide at the beginning of the year whether they want their respective products to be included in the test. The test is currently done as part of the public main-test series only if a minimum number of vendors choose to participate in it.

Readers may be interested to see a summary and commentary of our test methodology which was published by PC Mag two years ago: http://securitywatch.pcmag.com/security-software/315053-can-your-antivirus-handle-a-zero-day-malware-attack

2. Description

Many new malware samples appear every day, which is why it is important that antivirus products not only provide new updates, as frequently and as quickly as possible, but also that they are able to detect such threats in advance with generic/heuristic techniques; failing that, with behavioural protection measures. Even if nowadays most antivirus products provide daily, hourly or cloud updates, without proactive methods there is always a time-frame where the user is not reliably protected. The aim of this test is to evaluate the proactive detection and protection rates in this time-frame (without cloud). The data shows how good the proactive heuristic/generic detection and behavioural protection capabilities of the scanners were in detecting new threats used in this test. The design and scope

[1] http://www.av-comparatives.org/wp-content/uploads/2015/04/avc_fdt_201503_en.pdf

of the test mean that only the heuristic/generic detection capability and behavioural protection capabilities were tested (offline). Additional protection technologies (which are dependent on cloud-connectivity) and infection vectors are considered by AV-Comparatives in e.g. Whole-Product Dynamic ("Real-World") Protection Tests and other tests, but are outside the scope of the Retrospective/Proactive Tests.

We included in the retrospective test-set only new malware that was very prevalent in-the-field shortly after the freezing date. Samples which were not detected by the heuristic/generic detection capabilities of the products were then executed in order to see if behaviour-blocking features would stop them. In several cases, we observed that behaviour blockers only warned about some dropped malware components or system changes, without protecting against all the malicious actions performed by the malware; such cases were not counted as a block. As behaviour blockers only come into play after the malware is executed, a certain risk of being compromised remains (even when the security product claims to have blocked/removed the threat). Therefore, it is preferable that malware be detected before it is executed, by e.g. the on-access scanner using heuristics. This is why behaviour blockers should be considered a complement to the other features of a security product (multi-layer protection), and not a replacement.

By design, the test does not make use of cloud services. In the time needed for the entire test procedure, it is possible that most of the samples would be blacklisted by vendors' signatures or cloud services, meaning that the results would not reflect true proactive protection. In last year's test, it took several weeks before all the malware samples used had been covered by some of the participants' cloud services. This year the situation was better (due to the inclusion of mainly quite prevalent malware files / families), but in some few cases it still took some weeks till all malware samples used were finally detected by some cloud-dependent products, even when their cloud-based features were available. Consequently, it has to be considered as a marketing excuse if retrospective tests - which test the proactive protection against new malware - are criticized for not being allowed to use cloud resources. This is especially true considering that in many corporate environments the cloud connection is disabled by the company policy, and the detection of new malware coming into the company often has to be provided (or is supposed to be provided) by other product features. Cloud features are very (economically) convenient for security software vendors and allow the collection and processing of large amounts of metadata. However, in most cases (not all) they still rely on blacklisting known malware, i.e. if a file is completely new/unknown, the cloud will usually not be able to determine if it is good or malicious.

The awards are given by the testers after consulting a number of statistical methods, including hierarchical clustering[2]. We based our decisions on the following scheme:

	Proactive Protection Rates			
	Under 50%	Cluster 3	Cluster 2	Cluster 1
None - Few FP	tested	STANDARD	ADVANCED	ADVANCED+
Many FP	tested	tested	STANDARD	ADVANCED
Very many FP	tested	tested	tested	STANDARD
Crazy many FP	tested	tested	tested	tested

[2] http://en.wikipedia.org/wiki/Hierarchical_clustering

3. False alarm test

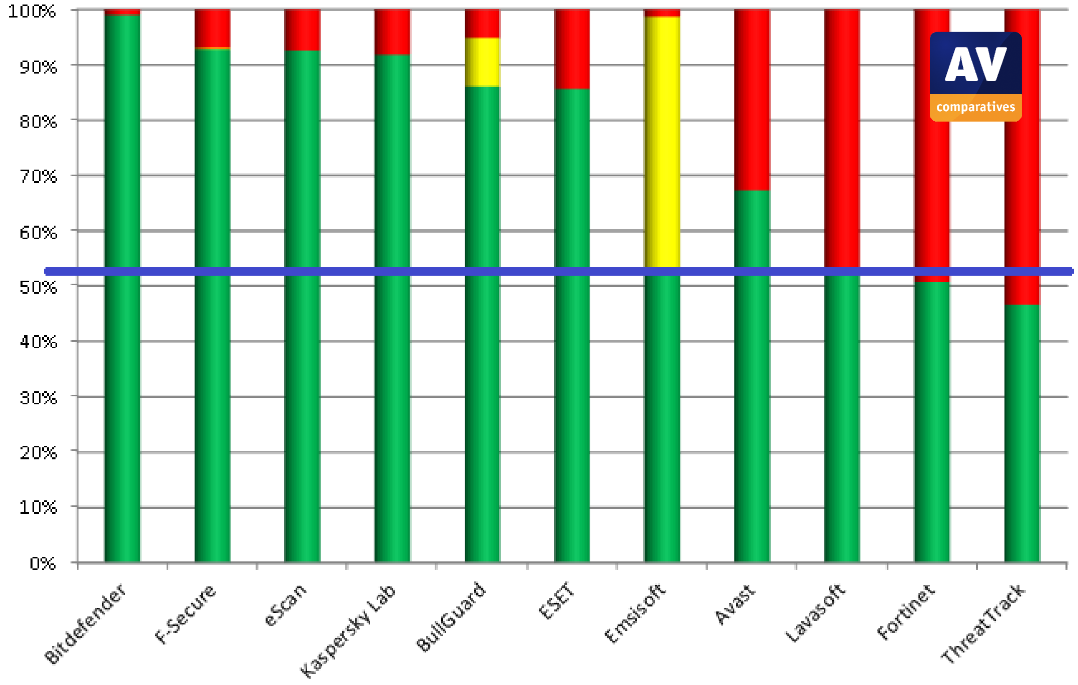
To better evaluate the proactive detection capabilities, the false-alarm rate has to be taken into account too. A false alarm (or false positive [FP]) occurs when an antivirus product flags an innocent file as infected. False alarms can sometimes cause as much trouble as real infections.
The false-alarm test results were already included in the March test report. For details, please read the report, available at http://www.av-comparatives.org/wp-content/uploads/2015/04/avc_fps_201503_en.pdf

Very few false alarms (0-1):	Microsoft, ESET
Few false alarms (2-10):	Fortinet, Bitdefender, Kaspersky Lab
Many false alarms (over 10):	Emsisoft, BullGuard, eScan, F-Secure, Lavasoft, ThreatTrack Vipre
Very many false alarms (over 50):	Avast

A small behavioural false-alarm test using 100 most downloaded/common software packages released in February did not bring up any additional false alarms. The false-alarm test carried out for the March 2015 Real-World Protection Test produced largely similar false alarm rates to those for the File-Detection Test shown above.

4. Test Results

The table below shows the proactive protection capabilities of the various products. The awards given (see page 7 of this report) consider not only the protection rates against new malware, but also the false alarm rates.



Key:
Green = blocked/protected
Yellow = user dependent
Red = not blocked/compromised
The blue line indicates the results of Microsoft Security Essentials

5. Summary results

The results show the proactive (generic/heuristic/behavioural) protection capabilities of the various products against new malware. The percentages are rounded to the nearest whole number.

To know how these antivirus products perform with updated signatures and cloud connection against prevalent malware files, please have a look at our File Detection Tests of March and September. To find out about real-life online protection rates provided by the various products, please have a look at our ongoing Whole-Product Dynamic "Real-World" Protection tests. Readers should look at the results and decide on the best product for them based on their individual needs. For example, laptop users who are worried about infection from e.g. infected flash drives whilst offline should pay particular attention to this Proactive test.

Below you can see the proactive protection results over our set of new and prevalent malware files/families appeared in-the-field (1,463 malware samples):

	Blocked	User dependent[3]	Compromised	Proactive Protection Rate	False Alarms	Cluster
Bitdefender	1448	-	15	**99%**	few	1
F-Secure	1358	3	102	**93%**	many	1
eScan	1354	-	109	**93%**	many	1
Kaspersky Lab	1343	-	120	**92%**	Few	1
BullGuard	1259	129	75	**90%**	many	1
ESET	1253	-	210	**86%**	very few	1
Emsisoft	777	667	19	**76%**	many	2
Avast	985	-	478	**67%**	very many	2
Lavasoft	781	-	682	**53%**	many	3
Microsoft	772	-	691	**53%**	very few	3
Fortinet	742	-	721	**51%**	few	3
ThreatTrack	682	-	781	**47%**	many	-

[3] User-dependent cases were given a half credit. Example: if a program blocks 80% of malware by itself, plus another 20% user-dependent, we give it 90% altogether, i.e. 80% + (20% x 0.5).

6. Awards reached in this test

The following awards are for the results reached in the proactive/behavioural test:

AWARDS	PRODUCTS
AV comparatives ADVANCED+ ★★★ HEURISTIC / BEHAVIOURAL TEST MAR 2015	Bitdefender Kaspersky Lab ESET
AV comparatives ADVANCED ★★ HEURISTIC / BEHAVIOURAL TEST MAR 2015	F-Secure* eScan* BullGuard*
AV comparatives STANDARD ★ HEURISTIC / BEHAVIOURAL TEST MAR 2015	Emsisoft* Fortinet
AV comparatives TESTED HEURISTIC / BEHAVIOURAL TEST MAR 2015	Avast* Lavasoft* ThreatTrack Vipre

*: these products got lower awards due to false alarms

Microsoft security products are not included in the awards page, as their out-of-box protection is (optionally) included in the operating system and is currently considered out-of-competition.

7. Copyright and Disclaimer

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 no representative of AV-Comparatives can he held liable for the accuracy of the test results. 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 (June 2015)