Anti-Virus Comparative

Retrospective/Proactive test

Heuristic and behavioural protection
against new/unknown malicious software

Language: English
March 2013
Last revision: 16th August 2013

www.av-comparatives.org

Contents

1. Introduction

This test report is the second part of the March 2013 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).

The products used the same updates and signatures that they had on the 28th February 2013. This test shows the proactive protection capabilities that the products had at that time. We used 1,109 new, unique and very prevalent malware samples that appeared for the first time shortly after the freezing date. The size of the test-set has also been reduced to a smaller set containing only one unique sample per variant, in order to enable vendors to peer-review our results in a timely manner. The following products were tested:

- AhnLab V3 Internet Security 8.0
- avast! Free Antivirus 8.0
- AVIRA Antivirus Premium 2013
- Bitdefender Anti-Virus Plus 2013
- BullGuard Antivirus 2013
- Emsisoft Anti-Malware 7.0
- eScan Anti-Virus 14.0
- ESET NOD32 Antivirus 6.0
- F-Secure Anti-Virus 2013

- Fortinet FortiClient 5.0
- G DATA AntiVirus 2013[2]
- Kaspersky Anti-Virus 2013
- Kingsoft Internet Security 2013
- Microsoft Security Essentials 4.2
- Panda Cloud Free Antivirus 2.1.1
- Tencent QQ PC Manager 7.4
- ThreatTrack Vipre Antivirus 2013

At the beginning of the year, we gave the vendors the opportunity to opt out of this proactive test. AVG, McAfee, Qihoo, Sophos and Trend Micro decided not to take part in the test, as their products rely heavily on the cloud, and would (so they believe) therefore very probably score poorly against completely new malware in a test without a cloud connection.

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, with-

---

[1] http://www.av-comparatives.org/wp-content/uploads/2013/03/avc_fdt_201303_en.pdf

[2] The tested version of **G DATA** (2013) was based on the Avast and Bitdefender engines. G DATA 2014 is based on the Bitdefender engine and a new in-house engine; the results in this report of G DATA 2013 are not applicable to G DATA 2014.

out 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 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.

What about the cloud? Even several weeks later, a number of the malware samples used were still not detected by some cloud-dependent products, even when their cloud-based features were available. Consequently, we consider it 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[3]. This time we based our decisions on the following scheme:

	Proactive Detection/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

---

[3] 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/2013/03/avc_fp_mar2013.pdf

Very few false alarms (0-2):	Microsoft
Few false alarms (3-15):	Fortinet, Kaspersky, AVIRA, Bitdefender, BullGuard, ESET, F-Secure, Avast, Kingsoft, Tencent
Many false alarms (over 15):	AhnLab, GDATA 2013, eScan, Panda, Vipre, Emsisoft

A small behavioural false-alarm test using the 100 most downloaded/common software packages released in February did not bring up any additional false alarms.

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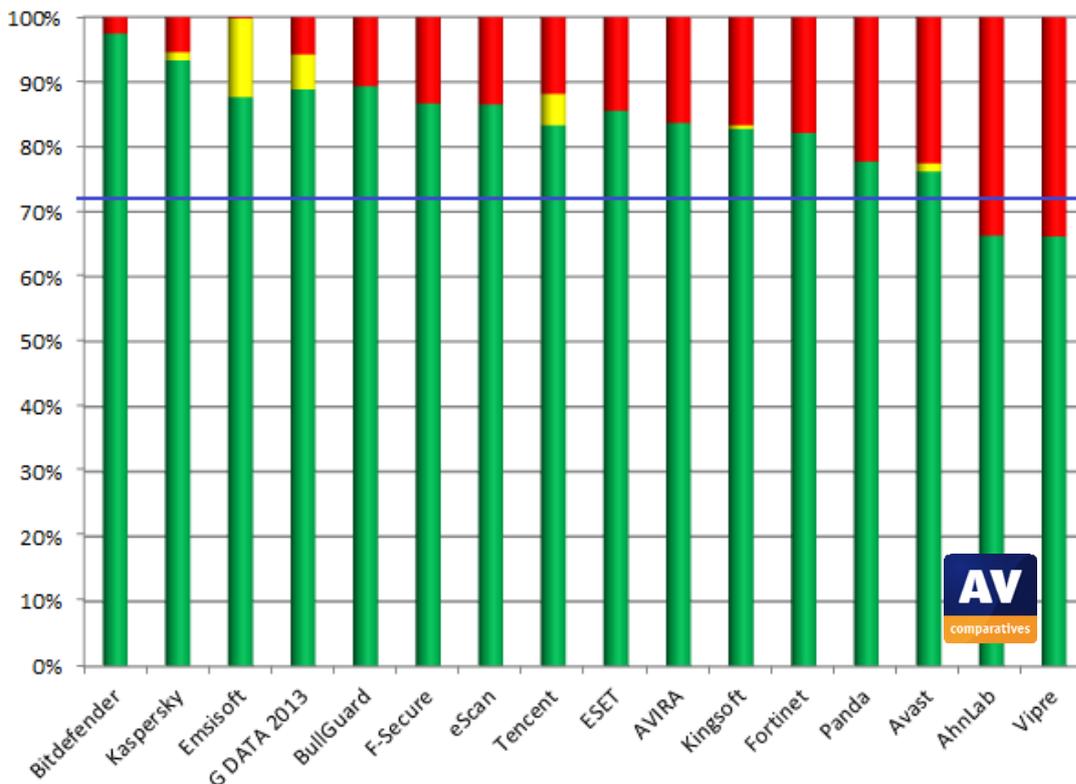
Key:
Green = blocked/protected
Yellow = user dependent
Red = not blocked/compromised
The blue line indicates the results of Microsoft Security Essentials

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 very prevalent malware appeared in-the-field (1,109 malware samples):

	Blocked	User dependent[4]	Compromised	Proactive Protection Rate	False Alarms	Cluster
Bitdefender	1081	-	28	**97%**	few	1
Kaspersky	1035	14	60	**94%**	few	1
Emsisoft	972	134	3	**94%**	many	1
G DATA 2013	985	60	64	**92%**	many	1
BullGuard	991	-	118	**89%**	few	1
F-Secure	961	-	148	**87%**	few	1
eScan	960	-	149	**87%**	many	1
Tencent	924	54	131	**86%**	few	1
ESET	949	-	160	**86%**	few	1
AVIRA	928	-	181	**84%**	few	1
Kingsoft	918	6	185	**83%**	few	1
Fortinet	911	-	198	**82%**	few	1
Panda	862	-	247	**78%**	many	2
Avast	845	14	250	**77%**	few	2
Microsoft	795	-	314	**72%**	very few	2
AhnLab	736	-	373	**66%**	many	3
Vipre	734	-	375	**66%**	many	3

---

[4] 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[5] are for the results reached in the proactive/retrospective test:

AWARDS	PRODUCTS
ADVANCED+ ★★★ HEURISTIC / BEHAVIOURAL TEST AUG 2013	Bitdefender Kaspersky BullGuard F-Secure Tencent ESET AVIRA Kingsoft Fortinet
ADVANCED ★★ HEURISTIC / BEHAVIOURAL TEST AUG 2013	Emsisoft* G DATA 2013* eScan* Avast
STANDARD ★ HEURISTIC / BEHAVIOURAL TEST AUG 2013	Panda*
TESTED HEURISTIC / BEHAVIOURAL TEST AUG 2013	AhnLab* Vipre*
NOT INCLUDED[6]	*AVG* *McAfee* *Qihoo* *Sophos* *Trend Micro*

*: 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 therefore out-of-competition.

---

[5] 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 therefore out-of-competition.

[6] As those products are included in our yearly public test-series, they are listed even though these vendors decided not to be included in retrospective tests as they rely heavily on cloud-connectivity.

7. Copyright and Disclaimer

This publication is Copyright © 2013 by AV-Comparatives e.V. ®. 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 e.V., prior to any publication. AV-Comparatives e.V. 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 e.V. 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 e.V. is an Austrian Non-Profit Organization.

AV-Comparatives e.V. (August 2013)