Keywords: anti-malware; accreditation; assessment; testing; test plan; template; AV-Comparatives; Consumer; 2018 Test Series

AMTSO 2017-2018
Prepared on January 16, 2018

Version 1.4

Independent Tests of Anti-Virus Software

AV-Comparatives Test Plan for the Consumer Product Security Review 2018 Test Series

Sponsored by:
AV-Comparatives (Andreas Clementi, Peter Stelzhammer), AMTSO (John Hawes, Scott Jeffreys)

Abstract:
This Test Plan has been prepared jointly by AV-Comparatives and AMTSO as part of the AMTSO Operational Pilot Implementation of the approved V6.1 Standards. The Plan details the AV-Comparatives testing activities in the Consumer Product Security space for their 2018 Test Series. This document has been developed using AMTSO Test Plan Template Version 1.5 from November 2017.

amtso™
Anti-Malware Testing Standards Organization

www.amtso.org

Table of Contents

AV-Comparatives Consumer Product Security Review 2018 Test Series Test Plan

1. Introduction

The AV-Comparatives Public Consumer Main-Test Series of 2018 consists of the following tests. The dates can be found in the timeline.

- 10x Real-World Protection Tests + FP (false positive) Test, with results published in monthly factsheets and two Overall Real-World Protection Test Reports covering 5 months each
- 2x Performance Tests (1x on low-end machine, 1x on high-end machine)
- 2x Malware Protection Tests (samples are executed) + FP Test
- 1x Malware Removal Test (opt-out possible)
- 1x Summary Report (including awards given for all the year's tests, and product UI reviews)

This Consumer Test Series includes preview reports and the feedback process for missed samples, as well as feedback regarding any bugs we may discover in tested products.

Readers seeking detailed methodology and example reports can examine the following reference material.

- https://www.av-comparatives.org/dynamic-tests/
- https://www.av-comparatives.org/performance-tests/
- https://www.av-comparatives.org/malware-protection-test/
- https://www.av-comparatives.org/removal-tests/
- https://www.av-comparatives.org/summary-reports/

This Test Plan has been structured to follow the AMTSO Test Plan Template and Public Notification Process. Compliance confirmations will take place periodically during 2018.

2. Scope

This Consumer Test Series is designed to examine Consumer Internet Security Suites and/or Antivirus platforms in a variety of practical settings covering scenarios commonly encountered by Consumer users.

3. Methodology and Strategy

Real world protection, performance, malware protection, and malware removal (opt-out option) are all examined during the 2018 Consumer Series. Key elements in the methodology for each individual area are summarized below. For more detailed information, please refer to the previous AV-Comparatives test reports.

Real World Protection Tests

In this test, all protection features of the product can be used to prevent. A suite can step in at any stage of the process – accessing the URL, downloading the file, formation of the file on the local hard drive, file access and file. The false-alarm test in the Whole-Product Dynamic "Real-World" Protection Test consists of two parts: wrongly blocked domains (while browsing) and wrongly blocked files (while downloading/installing). It is necessary to test both scenarios because testing only one of the two above cases could penalize products that focus mainly on one type of protection method, either URL filtering or on-access/behavior/reputation-based file protection. If the user is asked to decide whether a malware sample should be allowed to run, and in the case of the worst user decision system changes are observed, the test case is rated as "user-dependent".

Performance Tests

These tests evaluate the impact of anti-virus software on system performance, as programs running in background – such as real time protection antivirus software – use some percentage of system resources. Taking these tests as reference, users can evaluate their anti-virus protection in terms of system speed (system performance).

The following activities/tests are performed under an up-to-date Windows 10 64-Bit system:

- File copying
- Archiving / unarchiving
- Installing / uninstalling applications
- Launching applications
- Downloading files
- Browsing Websites
- PC Mark 10 Professional Testing Suite

Malware Protection Test

The Malware Protection Test assesses a security program's ability to protect a system against malicious files. Any samples that have not been detected e.g. on-access are executed on the test system, with Internet/cloud access available, to allow features such as behavioral protection to come into play. If a product does not prevent or reverse all the changes made by a particular malware sample within a given time period, that test case is considered to be a miss. This test also contains a false-alarm test.

Malware Removal Test (optional)

This test focuses only on the malware removal/cleaning capabilities. The main question is if the products are able to successfully remove malware from an already infected system. The test is aimed to typical home users.

4. Participation

Opt-Out Policy : All the above-mentioned tests (except the Malware Removal Test) are mandatory, and part of the Public Consumer Main-Test Series. It is not possible to withdraw

from any test once an application to participate in the Main-Test Series has been accepted.

Conflict of Interest Disclosure : No known conflicts of interest exist at this time. Post-test consultancy services are available to all tested companies for a fee.

Funding : Products that we consider of key interest to our readers are included in our tests at no cost to the vendor, but to get the same post-test consultancy services, the feedback process, the preview process, the marketing use of logos/awards, as well as links to your web pages on our website, etc. like the other participating vendors, the same fee applies (i.e. same equal opportunity is given). The fee for the services is available upon request. Additional information regarding test funding can be found at the following link.

https://www.av-comparatives.org/funding/

5. Environment

Physical Configuration : The systems are non-physical systems, identical and fully patched Microsoft Windows 10 64-bit (English) systems with active internet/cloud access.

The performance and Malware Removal Tests are done on a physical machine with an Intel Core i5-6200U CPU, 8GB of RAM and SSD hard disks. If the security product gives an option to enable PUA, this option will be enabled.

Sample Relevance : AV-Comparatives aims to use visible and relevant malicious websites/malware that currently present a risk to ordinary users. Every potential test-case to be used in the test is run and analysed on a clean machine without antivirus software, to ensure that it is a suitable candidate. If the malware meets these criteria, the test-case is added to the list to be tested with security products. Any test cases which turn out not to be appropriate are excluded from the test set. Potentially Unwanted Applications (PUA) will be excluded from the test.

Geographic Limitations : Samples used in the AV-Comparatives 2018 Consumer Security Product Test Series will not include any known regional or geographic bias.

Curation Process : AV-Comparatives only use samples that have been analysed by either in-house automated sandbox systems or manually. Details regarding this process can be found at the following web site.

http://weblog.av-comparatives.org/sample-quality/

Please note that AV-Comparatives does maintain intellectual property associated with their collection process and does not disclose those details regarding their internal procedures.

Distribution of Test Data : Missed samples (binaries/hashes) and false alarms from tests included in the Public Main-Test Series are only provided as a post consultancy service after the test is completed.

6. Schedule

Start Date Range : Applications for the Consumer Test Series 2018 were due by December 10th, 2017. Testing is expected to begin on February 1st, 2018.

Test Duration and Calculated End Date : The Test Series is anticipated to cover the entirety of 2018 and the milestones section enumerates the individual tests and associated reporting.

Milestones : Arranged by quarters, the listing of tests and deliverables from the 2018 Consumer Test Series will be as follows.

Q1'2018

- Real-World Protection Test 02/18 (including FP test), results released on the 15th of March
- Real-World Protection Test 03/18 (including FP test), results released on the 15th of April
- Malware Protection Test 03/18 (including FP test), results released 15th of April
- Malware removal test, ongoing February to October, results released in November

Q2'2018

- Real-World Protection Test 04/18 (including FP test), results released on the 15th of May
- Performance Test 04/18, results released in May/June
- Real-World Protection Test 05/18 (including FP test), results released on the 15th of June
- Real-World Protection Test 06/18 (including FP test), results released on the 15th of July
- Malware removal test, ongoing February to October, results released in November

Q3'2018

- July: Release of Real-World Protection Test half-year report (including FP test)
- Real-World Protection Test 07/18 (including FP test), results released on the 15th of August
- Real-World Protection Test 08/18 (including FP test), results released on the 15th of September
- Real-World Protection Test 09/18 (including FP test), results released on the 15th of October
- Malware Protection Test 09/18 (including FP test), results released 15th of October
- Malware removal test, ongoing February to October, results released in November

Q4'2018

- Malware removal test, ongoing February to October, results released in November
- Performance Test 09/18, results released October/November
- Real-World Protection Test 10/18 (including FP test), results released on the 15th of November

• Real-World Protection Test 11/18 (including FP test), results released on the 15th of December
• December: Release of Real-World Protection Test half-year report (including FP test); , results released on the 15th of December
• December/January: Release of Summary Report

Communications : Variations by four weeks or more from this published schedule will cause AV-Comparatives to provide schedule updates to participants in the 2018 Consumer Test Series.

Risks and Risk Management : No risks are known at this time.

7. Control Procedures

Connectivity Validation : Each Product will be tested with full internet access. Connectivity details should be defined by the Tester. A means for confirming whether a Product's Cloud connectivity or other features are functioning can be provided by the Vendor if the Vendor has a tool for that purpose.

Logging : Instructions to enable logging within a Participant's Product should be provided by the Vendor. E-Mailing the process to your AV-Comparatives contact is sufficient.

Updates : Given that testing will take place over the course of 2018, version information might change as various components are updated. AV-Comparatives will allow products to be updated as part of the natural product update cycles. In particular for the Real World Testing Environment, every morning, any available security software updates are downloaded and installed, and a new base image is made for that day. Before each test case is carried out, the products have some time to download and install newer updates which have just been released, as well as to load their protection modules (which in several cases takes some minutes). If a major signature update for a product is made available during the day, but fails to download/install before each test case starts, the product will at least have the signatures that were available at the start of the day. This replicates the situation of an ordinary user in the real world.

8. Dependencies

Participant Actions : Participating vendors are required to inform AV-Comparatives which publicly available product version should be included in the test series. The same major product type (e.g. Internet Security, paid Antivirus, free Antivirus) and configuration will be used throughout the Consumer Main-Test Series.

9. Scoring Process

All tests, including the Whole-Product Dynamic Real-World Protection Test and Performance Tests, allow for Triple-Star, Double-Star, and Single-Star awards to be earned by any individual product. Note that each individual test award is given only for the scope of that single test in the test series. Statistical methods (usually clustering analysis) are used to determine the awards. Examples and details about scoring processes for each test type can be found in previous reports.

10. Dispute Process

The AV-Comparatives feedback system provides participating vendors with details of their respective product's missed samples, false positives, metadata, and so forth via WebGUI and API.
AV-Comparatives gives as part of its post consultancy services each vendor the possibility to review their missed samples and FPs AFTER the test using AV-Comparatives' Feedback System. Any dispute from a participant must be accompanied by an element of proof, or evidence that the dispute is legitimate, rather than just the participant's statement of disagreement. We continuously verify our test set during the open feedback time. The final decision whether a dispute is accepted or declined is taken solely by AV-Comparatives.

11. Attestations

I understand and agree that I am submitting this Test Plan, and the following Attestations, on behalf of the entity listed below, and I represent and warrant that I have authority to bind such entity to these Attestations. All references to "I" or "me" or similar language refer to such entity. I represent and warrant that the following Attestations are true, to the best of my knowledge and belief, and each of the following commitments will be upheld to the best of my ability.

1. I will provide public notification on the AMTSO website covering my obligation for notification of a Public Test, regardless of whether a potential Participant is in actual receipt of such notification prior to the Commencement Date of a Test. (Section 1, Section 4, Section 6)

2. All products included in this Test will be analyzed fairly and equally. (Section 2, Section 3, Section 5)

3. I will disclose any anticipated or known imbalance or inequity in the Test design to all Participants in the Test. (Section 2, Section 3)

4. Although I may charge for participation in a Test, I will not charge any additional fees for a Test Participant to be "Voluntary" under the Standards. (Section 4)

5. I will disclose any material conflicts of interest or other information that could materially impact the reliability of the Test. (Section 4)

6. I will disclose how the Test was funded. (Section 4)

I hereby affirm, to the best of my knowledge and belief that this Test Plan complies with the AMTSO Testing Standards, as of the date hereof.

Signature: /s/ Andreas Clementi
Name: Andreas Clementi
Test Lab: AV-Comparatives
AMTSO test ID: AMTSO-PP1-TP203