Keywords: application; assessment; testing; test plan; template; mobile; security

Test Plan Creation Date : December 18, 2023
Review and ID Assigned : December 21, 2023
AMTSO Publication : January 2, 2024

Version 1.2

AV-TEST Test Plan for MacOS Consumer Security Product Testing for 2024

Authored by:
AV-TEST (Erik Heyland, Marcel Wabersky)

AMTSO Standard Compliance Statement
This Test has been designed to comply with the Anti-Malware Testing Standards Organization, Inc. ("AMTSO") Testing Protocol Standard for the Testing of Anti-Malware Solutions, Version [1.3] (the "Standard"). This Test Plan has been prepared using the AMTSO Test Plan Template and Usage Directions, Version [2.5]. AV-TEST is solely responsible for the content of this Test Plan.

Table of Contents

1. Introduction

Due to the increasing number of threats being released and spreading through the internet, the risk of infection is higher than ever. In the past, new malware apps were released every few days, but now there are several thousand new threats per day. As of December 2023, AV-TEST has already recognized around 1 million new MacOS malware samples for the year 2023.

Infections caused by MacOS malware can result in financial and private data losses, as well as damaged hardware. A Banking-Trojan can steal credit data, while a Backdoor may provide unwanted access to the device, and Ransomware can prevent normal device usage.

The purpose of an anti-malware product is to protect users from such threats at all times. AV-TEST aims to demonstrate how the malware detection rate and resource usage of anti-malware products can be measured. Our AV-TEST method enables us to determine which Anti-Malware products provide effective protection without causing battery life disruption.

2. Scope and Participants

The AV-TEST MacOS Consumer Security Product Test evaluates security applications that target MacOS consumers to determine their ability to protect devices against malicious attacks. The test includes different scenarios to measure the products' detection rates, their reaction to clean samples, and their impact during normal device operation.

The list of vendors and participants will be determined after the Public Test Notification has been issued.

We select products to test based on the size of their user-base, relevance to the market, or other significance to our readers. In each case, we use the most recent and widely-used product and version available for the appropriate platform.

All products are downloaded prior to the test from their main source or from a source provided by the vendor. During the test, the products' signatures are updated, and also product version updates are possible.

3. Methodology and Strategy

AV-TEST will follow the methodology provided by the URL below.
https://www.av-test.org/en/about-the-institute/test-procedures/test-modules-under-MacOS-protection/
https://www.av-test.org/en/about-the-institute/test-procedures/test-modules-under-MacOS-usability/
https://www.av-test.org/en/about-the-institute/test-procedures/test-modules-under-MacOS-performance/

4. Participation

AV-TEST selects security solutions for inclusion in this test based on requests from the press, social media, or any other relevant aspect. Vendors can also submit a request to participate in the test.

Opt-Out Policy: If any vendor provides a valid reason why their product should not be included in an ongoing or upcoming test, AV-TEST will thoroughly review the request and make an informed decision.

Conflict of Interest Disclosure: There are currently no conflicts of interest. We offer technical and marketing services to vendors upon request for a fee.

Funding: The testing is funded by vendors who have an agreement with AV-TEST to participate. We reserve the right to include additional products in our tests at no cost to the vendor. Participants receive additional technical and marketing services. Being a participant also grants the right to use seals if awarded by AV-TEST according to AV-TEST's Brand Guidelines and Terms and General Terms and Conditions.

5. Environment

Physical Configuration:Device used for all test cases:

Physical devices: Physical devices: mac mini 2018 and 2022 with Intel i5 and 8 or 16 GB RAM
OS: MacOS with the latest build

Sample Relevance: The prevalent malware category includes recent malware applications, no older than 10 days prior to the test. The samples cover several relevant malware families.

In the real-world test category, each sample is tested on the day of its discovery by AV-TEST.

The false positive test set includes both static and dynamic samples used by average consumers, excluding those that pose a threat to device security, such as rooting tools. The test is divided into false positive testing and dynamic cases from the MacOS Store and software from third-party stores.

Geographic Limitations: This test has no geographic limitations.

Curation Process: Only malicious or clean samples that have been validated by AV-TEST's in-house systems or manually analyzed samples are used.

Distribution of Test Data: After the test, participants will receive their own results or the results of all vendors in an Excel sheet based on their agreement with AV-TEST. The test results will indicate whether a test case was detected by on-demand or on-access scan.

6. Schedule

Start Date Range, Test Duration, Calculated End Date:
MacOS Consumer Security Product Testing will be conducted six times a year, starting in January, March, May, July, September, and November. Prior to each test run, a detailed schedule will be sent to the vendors participating in the test via email. This email will include the start date, estimated end date, and other relevant information.

Milestones: Interim schedule milestones are listed below.

AV-TEST MacOS Consumer Security Product Testing Schedule			
Index	**Test Activity**	**Start Date Range**	**Dependencies**
1	*Test Commencement*	*Every odd month, Detailed start date announced by e-mail*	
2	*End of Testing Period and Preliminary Results*	*Bi-monthly test cycle*	*(1)*
3	*Dispute-Phase*	*Seven days announced by e-mail after each month*	*(2)*
4	*Feedback and Dispute Resolution Time – Retests as Needed*		*(2), (3)*
5	*Final Report – End Date for Test*	*After disputes have been solved of the second month*	*(4)*

Communications: Prior to a test run, a detailed schedule is sent to the vendors participating. We will notify all tested vendors if there are significant deviations from this schedule.

Risks and Risk Management: No risks are currently known.

7. Control Procedures

Connectivity Validation: At the beginning of each test case, we ensure and check internet connectivity.

Logging: The products operate using the default settings. If requested by the participant, additional logging can be enabled.

Updates: All products are updated using online updates before the start of the test.

8. Dependencies

Participant and Test Subject Vendors Required Actions: Test vendors can contact AV-TEST to request inclusion, exclusion, or respond to an invitation.

9. Scoring Process

AV-TEST will follow the scoring provided under the section Certification in the methodology.

https://www.av-test.org/en/about-the-institute/certification/

10. Dispute Process

After receiving their test results, participants may dispute individual test cases using AV-TEST's online dispute system.

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/ Marcel Wabersky

Name: Marcel Wabersky

Test Lab: AV-TEST

AMTSO Test ID: AMTSO-LS1-TP105