Keywords: anti-malware; compliance; assessment; testing; test plan; Testing Ground Labs; Android Detection

Initial Release: August 10th, 2023
Published: August 14th, 2023

Version 1.1

Android Malware Detection Test Plan 2023 August (enterprise product)

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 [2.4]. TGL is solely responsible for the content of this Test Plan.

Table of Contents

TGL Android Malware Detection Test

1. Introduction

Android is a mobile operating system developed by Google. It is based on a modified version of the Linux kernel and other open-source software, and is designed primarily for touchscreen mobile devices such as smartphones and tablets. In addition, Google has further developed Android TV for televisions, Android Auto for cars, and Wear OS for wrist watches, each with a specialized user interface. Variants of Android are also used on game consoles, digital cameras, PCs and other electronics. Android's smartphone share will hover with around 85% throughout the forecast. Volumes are expected to grow at a five-year compound annual growth rate (CAGR) of 1.7% with shipments approaching 1.36 billion in 2023. Android maintained its position as the leading mobile operating system worldwide in September 2023, controlling the mobile OS market with a close to 70 percent share. Google's Android and Apple's iOS jointly possess over 99 percent of the global market share. Overall this is a positive sign that consumers are seeing the benefits of moving to a slightly more premium device than they likely previously owned.

Aside from the clear advantages to build mobile devices on Android, the platform also introduces numerous security risks to the platform users. Among them the following malicious activities:

1. Send messages to "premium service" SMS numbers that cost extra money.
2. Send your personal information to unknown parties.
3. Turn your phone into a part of a botnet so others can execute commands remotely for nefarious purposes, such as spam, DDOS attack, and more.
4. Non-authorized persons September monitor your phone calls and text messages.
5. Open you to blackmail, if something embarrassing can be found and sent elsewhere.
6. Trick you into entering financial information, such as account number, birth date, and more.
7. Even stuff on your PC if you connect your PC to your smartphone.

Clearly, to protect user's system and the data from the listed threats and the others, Android-based security applications exist and their efficiency is to be evaluated regularly against the permanently evolving threats.

This test is designed to independently assess the efficiency of enterprise security solutions for Android OS on detecting currently spread malicious mobile apps.

2. Scope and Participants

In this test Testing Ground Labs plans to reveal capabilities of enterprise security solutions for Android OS to detect Android threats, collected from different sources, as well as to check their resistance to False Positives. As a result of the test, certification mark will be granted to security solutions depending on their results. Testing Ground Labs plans to examine enterprise security solutions for Android OS from the following companies (Test Subjects). Specific Test Subject Vendors and Participants will be determined after the Public Test Notification has been issued.

Vendor	Software
Dr.Web	*Dr.Web Essential Security Suite*
ESET	*ESET Endpoint Security for Android*
Kaspersky	*Kaspersky Endpoint Security*
Total Defense	*Total Defense Premium Internet Security for SMB*

3. Methodology

Detailed process is as follows.

1. Several Android based mobile devices are prepared and backup images are created then. Platform: Android 12 on XiaoMi 8.
2. Collect about 1000-2000 malware samples and 300-500 different clean android applications installers, and deliver them in a mixed set to the internal storage of mobile devices. The malware is collected from multiple sources (including China region-based ones), clean apps are taken from Google AppStore and other legitimate app stores.
3. Install selected security applications on the physical mobile devices in default configuration.
4. Update the security applications and their antivirus bases.
5. Run full scan of the collection by the security application. Malware detection and false positive rates are recorded.
6. Install each missed malicious sample and then run each application, detection (if happened) will be recorded.
7. Installation process against clean apps will not be executed.

4. Participation

Testing Ground Labs chooses security solutions of interest to include into this test. Additionally, any vendor September submit request to participate in the test. Testing of either security solution (both chosen by Testing Ground Labs and submitted by a Vendor directly) is free of charge to the Vendor. Every Vendor will be provided with the feedback process, which means that the test lab will share test results with Vendors and they will have chance to investigate the results and submit disputes in case of any.

Opt-Out Policy: If any Vendor manages to supply sufficient reason as to why Testing Ground Labs should not include their products in an upcoming or on-going test, Testing Ground Labs will review this request and make the correspondent decision.

Conflict of Interest Disclosure: No known conflicts of interest exist at this time.

Funding: This test is free of charge. Any Vendor who would like to get post-test service or any other extra service, can email us. Results (reference or direct use of the test report or seals) would be allowed to use only in case of marketing rights agreement between Testing Ground Labs and the interested Vendor.

5. Environment

Physical Configuration: Android 12 on XiaoMi 8 with 128 GB internal storage

Sample Relevance: Malicious and non-malicious android installers are collected by Testing Ground Labs threat collection system during the past 2 months. The malware is collected from multiple sources (including China region-based ones). Non-malicious (clean) apps are used to check the level of false positive detection. Candidates for legitimate sample testing include newly released applications collected by multiple public app stores (including but not limited to Google AppStore).

Curation Process: Malicious and legitimate applications are independently verified by Testing Ground Labs.

Distribution of Test Data: Malicious and non-malicious apps data with non-optimal results are provided to vendor once the full test is complete. Testing Ground Labs does not share data on one vendor with other vendors. Any security vendor whose product was tested, September request hashes of their missed samples/false positives.

6. Schedule

Start Date Range: Test configuration is scheduled to begin on 10th August, 2023 and the Test commencement is forecast for 18th August, 2023

Test Duration and Calculated End Date: The final Test Report is anticipated during the week of September 9, 2023.

Milestones: Interim schedule milestones are listed below.

Sample Schedule Summary for Test Project

Index	Test Activity	Start Date Range	Dependencies
1	*Test Commencement*	*August 18 2023*	
2	*Confirm Vendor Configuration Feedback*	*August 14 2023 – August 18 2023*	
3	*Milestone 1 – Preliminary Results*	*August 25 2023*	*(1), (2)*
4	*Milestone 2 – Test Report First Edition – End of Testing Period*	*August 28 2023*	*(3)*
5	*Feedback and Dispute Resolution Time – Retests as Needed*	*September 4 2023*	*(3)*
6	*Milestone 3 – Issue Final Report – End Date for Test*	*September 9 2023*	*(5)*

Communications: All Participants will be notified when the schedule changes by two weeks or more.

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

7. Control Procedures

Connectivity Validation: All the security solutions in the test will be granted access to their cloud reputation and other services, which is the way how it works for end-users in real life.

Logging: Instructions for enabling logging within the Product must be provided by the Participant upon request to Testing Ground Labs.

Updates: Any configuration information needed for product updates to take place during the Testing Period should be disclosed by the Participant.

8. Scoring Process

For each security solution, a Final Score is calculated once the full test is performed:

Final Score = (Detection %)*100 - 0.2*FP

Basing on the Final Score, the correspondent rating is grated to each participating security solution, in accordance with the tab below:

final score	monthly award
98.00 - 100.00	5-star rating
95.00 - 97.99	4-star rating
90.00 - 94.99	3-star rating

9. Dispute Process

The dispute process runs for eight business days commencing from the end of the test. Refer to Section 6 covering the Test Schedule for additional details and timing. The general Dispute Process works as follows.

1. Testing Ground Labs provides Vendors with results their security solution with hash values associated with any sub-optimal results.

2. Vendor responds within eight business days to Testing Ground Labs, providing fact-based disagreements with any sub-optimal results, in case of any.

3. Testing Ground Labs responds with decision, if the dispute is accepted or denied.

10. 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 September charge for participation in a Test, I will not charge any additional fees for a vendor to be a test subject 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/

Name: Jeffrey Wu

Test Lab: Testing Ground Labs

AMTSO Test ID: [AMTSO-LS1-TP085]