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

Initial Release: February 10th, 2026
AMTSO Release: February 23rd, 2026
Version 1.1

Android Malware Detection Test Plan

2026 February · Consumer 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]. Testing Ground Labs (TGL) is solely responsible for the content of this Test Plan.

Table of Contents

Table of Contents 1
1. Introduction 1
2. Scope and Participants 3
3. Methodology 3
4. Participation 4
5. Environment 5
6. Schedule 5
7. Control Procedures 6
8. Scoring Process 6
9. Dispute Process 7
10. Attestations 7

1. Introduction

Android is a mobile operating system developed by Google, built on a modified version of the Linux kernel and other open-source software. It serves as the dominant platform for a vast array of devices from numerous manufacturers, including smartphones, tablets, televisions (Android TV), and automotive systems (Android Auto).

© 2020-2026 Testing Ground Labs | https://www.testingground.io

As of early 2026, Android continues to command the global mobile operating system market with a share fluctuating between 71% and 74%. Its dominance is even more pronounced in key emerging markets across Asia and South America, where market share frequently exceeds 85%. This massive, diverse, and highly fragmented user base — spanning countless device models and price points — makes the Android ecosystem an exceptionally attractive target for cybercriminals. The open nature of the platform, while a catalyst for innovation, simultaneously creates a complex and challenging security environment.

The Android threat landscape has become increasingly organized and aggressive. In 2025 alone, mobile malware targeting Android users surged by over 150%, with adversaries shifting from opportunistic, isolated attacks toward building sustainable, profit-driven criminal enterprises. The primary threats now involve sophisticated, multi-stage campaigns:

- Financial Fraud via Advanced Malware: Cybercriminals deploy highly effective banking trojans — including those from the Android.Banker family, which grew by over 150% in Q1 2025. These threats use overlay attacks to present fake login screens that perfectly mimic legitimate banking applications, and increasingly exploit app virtualization to operate hidden copies of real apps for credential theft.
- Smishing as a Primary Delivery Vector: SMS-based phishing ("smishing") has become a dominant initial attack vector, spiking by 692% between April and May 2025. Users receive deceptive messages masquerading as delivery notifications, tax refunds, or bank alerts, directing them to install spyware or banking trojans.
- Data Espionage and Extortion: Spyware incidents rose by 147% in 2025. Once deployed, these tools operate silently to exfiltrate personal data — including contact lists, photographs, private messages, and real-time GPS location — later monetized through blackmail, identity theft, or sale on darknet markets.
- Contactless Payment Theft: Newer malware strains exploit NFC (Near-Field Communication) technology, effectively turning infected devices into malicious point-of-sale terminals to capture payment card details.
- System-Level Control via Accessibility Services: A prevalent tactic involves tricking users into granting Accessibility Service permissions. Once obtained, malware can automate fraudulent transactions, harvest credentials from any installed application, and actively disable security software.

Systemic risks further compound the threat picture. As of 2025, over 30% of active Android devices run versions that no longer receive security patches, and some low-cost or counterfeit devices arrive pre-loaded with malware. Even official channels such as Google Play are not immune, as attackers continuously refine techniques to bypass platform security controls.

© 2020-2026 Testing Ground Labs | https://www.testingground.io

To protect users against this rapidly evolving landscape, the role of dedicated Android security applications is more critical than ever. Their effectiveness must be continuously and independently evaluated against prevalent, real-world threats. This test is designed to independently assess the detection efficiency of consumer security solutions for the Android platform.

2. Scope and Participants

In this test, Testing Ground Labs (TGL) aims to evaluate the capability of consumer security solutions for the Android OS to detect Android-specific threats collected from diverse sources, as well as to measure their resistance to false positive detections. Upon completion, a certification mark will be awarded to qualifying security solutions based on their performance.

TGL plans to examine consumer security solutions from a range of vendors (Test Subjects). The specific list of Test Subject Vendors and Participants will be confirmed following issuance of the Public Test Notification. The following vendors are currently planned for participation:

Vendor	Software
AhnLab	*AhnLab V3 Mobile Security*
Avast	Avast Mobile Security
Avira	*Avira Antivirus Security for Android*
Bitdefender	Bitdefender Mobile Security for Android
Dr.Web	*Dr.Web Mobile Security Suite*
ESET	ESET Mobile Security
Kaspersky	*Kaspersky Plus for Android*
McAfee	McAfee Mobile Security
NortonLifeLock	*Norton 360 (Norton Mobile Security)*
Total Defense	Total Defense Mobile Security

Note: Specific product versions will be confirmed at the time of testing, following the latest available updates.

3. Methodology

The following detailed procedure governs the conduct of this test:

1. Device preparation: Physical Android test devices are factory reset and provisioned with clean backup images to guarantee a consistent, uncontaminated baseline for each test run. Platform: Android 14 on Samsung Galaxy S22.
2. Sample collection: Approximately 1,000–2,000 recent, in-the-wild Android malware samples and 300–500 legitimate clean application installers are assembled into a mixed test set and transferred to the internal storage of the test devices. Malicious samples are sourced from multiple threat intelligence feeds (including China-region sources); clean applications are sourced from the official Google Play Store and other legitimate app stores.
3. Software installation: Each security application under evaluation is installed on the test device using its factory-default configuration settings, without any manual tuning or optimization.
4. Definition updates: Immediately prior to testing, each security application and its associated virus definitions are updated to the latest available versions to ensure peak detection capability.
5. Static analysis (on-demand scan): A full file-system scan is initiated. All detections of malicious files and any false positives (incorrectly flagged clean files) are recorded.
6. Dynamic analysis (behavioral test): Each malicious sample not detected during the static scan is then manually installed and executed on the device. Any behavioral or on-execution detections are recorded at this stage.
7. False positive verification: Clean application samples are used for scan-based false positive rate measurement only; they are not installed or executed during the test.

4. Participation

Testing Ground Labs selects security solutions of interest for inclusion in each test cycle. Additionally, any vendor may submit a request to participate. Testing of both TGL-selected and vendor-submitted solutions is provided free of charge. All participating vendors will be given access to a structured feedback process, allowing the test lab to share results with vendors and providing an opportunity to investigate sub-optimal outcomes and submit disputes where warranted.

Opt-Out Policy: If any vendor provides sufficient justification for why Testing Ground Labs should not include their product in an upcoming or ongoing test, TGL will review the request and make a corresponding decision.

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

Funding: This test is conducted free of charge. Vendors seeking post-test services or additional support may contact TGL directly. Use of test results — including reference to or direct use of the test

report or certification seals — is permitted only under a marketing rights agreement between Testing Ground Labs and the relevant vendor.

5. Environment

Physical Configuration: Android 14 on Samsung Galaxy S22 with 128 GB internal storage. The device is restored to a clean backup image prior to each individual test run to prevent cross-contamination.

Sample Relevance: Malicious and non-malicious Android application installers are collected by the Testing Ground Labs threat intelligence system over the preceding two months. Malicious samples are sourced from multiple threat feeds, including China-region sources. Non-malicious (clean) applications are used exclusively to measure false positive detection rates. Candidates for legitimate sample testing include newly released applications gathered from multiple public app stores, including but not limited to the Google Play Store.

Curation Process: All malicious and legitimate application samples are independently verified by Testing Ground Labs prior to inclusion in the test set.

Distribution of Test Data: Malicious and non-malicious samples associated with sub-optimal results are shared with the relevant vendor upon completion of the full test. TGL does not share one vendor's data with other vendors. Any security vendor whose product was tested may request the hash values of their missed samples or false positives.

6. Schedule

Start Date Range: Test configuration is scheduled to begin on February 23rd, 2026, with test commencement forecast for the same date.

Test Duration and Calculated End Date: Active testing is scheduled to conclude by February 28, 2026. The Final Test Report is anticipated during the week of March 17, 2026.

Milestones: Interim schedule milestones are listed in the table below.

Index	Test Activity	Start Date / Range	Dependencies
1	*Test Commencement*	*February 23, 2026*	—

Index	Test Activity	Start Date / Range	Dependencies
2	Confirm Vendor Configuration Feedback	Feb 23 – Feb 24, 2026	—
3	*Milestone 1 — Preliminary Results*	*February 27, 2026*	*(1), (2)*
4	Milestone 2 — Test Report First Edition (End of Testing Period)	March 3, 2026	(3)
5	*Feedback and Dispute Resolution — Retests as Needed*	*March 10, 2026*	*(3)*
6	Milestone 3 — Issue Final Report (End Date for Test)	March 17, 2026	(5)

Communications: All participants will be notified promptly in the event that 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 security solutions will be granted full access to their respective cloud reputation services and other online features during the test, replicating real-world end-user conditions.

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

Updates: Any configuration information required for product definition updates to occur during the Testing Period must be disclosed by the Participant in advance.

8. Scoring Process

For each security solution, a Final Score is calculated upon completion of the full test using the following formula:

$$\text{Final Score} = (\text{Detection \%}) \times 100 - 0.2 \times \text{FP}$$

Based on the Final Score, the corresponding rating is awarded to each participating security solution in accordance with the table 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 for additional details and timing. The general dispute process proceeds as follows:

1. Testing Ground Labs provides each vendor with the results pertaining exclusively to their own security solution, including hash values associated with any sub-optimal results.
2. The vendor responds within eight business days, providing fact-based disagreements with any sub-optimal results, if applicable.
3. Testing Ground Labs reviews the submission and communicates its decision, confirming whether each 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 may 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-TP189]

© 2020-2026 Testing Ground Labs | https://www.testingground.io