TESTING GROUND LABS

Android Malware Detection Test

Enterprise Product

2025 Apr

• • • Celebrating Technology Innovation

Table of Contents

Report version 1.0, published on 2025.06.15, initial version

Chap.1 Background

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

As of mid-2025, Android continues to command the global mobile operating system market with a share fluctuating between 71% and 74%. Its leadership is even more pronounced in key emerging markets across Asia and South America, where its market share often exceeds 85%. This massive, diverse, and fragmented user base, spread across countless device models and price points, makes the Android ecosystem a uniquely attractive and lucrative target for cybercriminals. The open nature of the platform, while a catalyst for innovation, simultaneously creates a complex and challenging security environment.

The threat landscape in 2025 has become more organized and aggressive. In the first half of the year alone, mobile malware targeting Android users surged by 151%, with attackers shifting from isolated scams to building sustainable criminal enterprises. The primary threats to users now involve sophisticated, multi-stage attacks:

Financial Fraud via Advanced Malware: Cybercriminals are deploying highly effective banking trojans, with attacks from families like Android.Banker increasing by over 150% in Q1 2025. These threats use overlay attacks to create fake login screens that perfectly mimic legitimate banking apps. More advanced techniques include app virtualization, where malware runs a counterfeit copy of a real app in a hidden virtual space to capture credentials and one-time passwords without arousing suspicion.

Smishing as a Primary Delivery Vector: SMS-based phishing ("smishing") has become a dominant initial attack vector. Between April and May 2025, smishing attacks spiked by an alarming 692%. Users receive deceptive messages disguised as delivery notifications, tax refunds, or bank alerts, which contain links that lead to the installation of spyware or banking trojans.

Data Espionage and Extortion: Spyware incidents have risen by 147%. These malicious tools, once deployed, operate silently to exfiltrate personal data, including contact lists, photos, private messages, and real-time location. This stolen

information is then monetized through blackmail, identity theft, or by selling it on darknet markets.

Contactless Payment Theft: Newer malware strains are exploiting NFC (Near-Field Communication) technology. An infected phone can be turned into a malicious point-of-sale (POS) device. The malware tricks the user into tapping their own credit or debit card against their phone (e.g., under the guise of verifying the card), allowing the malware to read and steal the card details directly.

System-Level Control through Accessibility Services: A key tactic involves tricking users into granting powerful Accessibility Service permissions. Legitimate by design, these services can read screen content and perform user actions. Once granted, malware can automate fraudulent transactions, steal credentials from any app, and disable security software, gaining nearly complete control over the device.

Underpinning these threats are several systemic risks within the Android ecosystem. OS fragmentation remains a critical issue; as of 2025, over 30% of active devices run outdated Android versions that no longer receive security patches, leaving them vulnerable to well-known exploits. Furthermore, the supply chain is a point of weakness, with some low-cost or counterfeit devices arriving pre-loaded with malware. Even official marketplaces like Google Play are not immune, as attackers continuously find new ways to bypass security checks and publish malicious apps. Google itself regularly issues critical security bulletins to address severe vulnerabilities, some of which could allow for remote code execution without user interaction.

To protect users' systems and data from this highly organized and rapidly evolving threat landscape, the role of dedicated Android security applications is more critical than ever. Their effectiveness must be continuously evaluated against prevalent, real-world threats. This test is designed to independently assess the efficiency of consumer security solutions for the Android OS in detecting and neutralizing the malicious applications that define the current cyber-risk environment.

Chap.2 Test Process & Test Software

This section outlines the methodology used for the test conducted in April 2025. The test environment and procedures were designed to ensure objectivity and reproducibility:

Test Environment:

- A Xiao Mi 8device was used as the primary testing platform.
- Operating System: The device was running a clean installation of Android 14.
- State: Before each test run, the device was reset to a clean, pre-configured backup image to ensure a consistent state and prevent cross-contamination between tests.

Test Procedure:

1. Sample Collection: A comprehensive test set was compiled, consisting of 925 recent, in-the-wild malware samples and 498 legitimate, clean application installers. The malicious samples were gathered from various threat intelligence feeds and online sources, while the clean apps were sourced from the official Google Play Store and other legitimate app stores.
2. Software Installation: Each security application was installed on the test device using its default configuration settings.
3. Signature Updates: Immediately prior to scanning, each security application and its virus definitions were updated to the latest available versions to ensure peak detection capability.
4. Static Analysis (On-Demand Scan): A full file system scan was initiated. All detections of malicious files and any false positives (incorrectly flagged clean files) were recorded.
5. Dynamic Analysis (Behavioral Test): Each malicious sample that was not detected during the static scan was then manually installed and executed. Any behavioral or on-execution detections that occurred at this stage were recorded.
6. False Positive Verification: The clean applications were used for scanning purposes only and were not installed or executed during the test, serving exclusively to measure the false positive rate.

Vendor	Software	Version
Dr.Web	Dr.Web Mobile Security Suite	12.9.4(2)
ESET	ESET Endpoint Security	v 5.1.2.0-0
Kaspersky	Kaspersky Endpoint Security	10.54.1.36
Total Defense	Total Defense Mobile Security	3.5.0.4

- Dr.Web Mobile Security Suite is included in Dr.Web Enterprise Security Suite

Chap.3 Tested Result (The test results are shown on the following table)

Vendor	Total Samples	Missed Samples	Detected Samples	Detection Rate	False Positive Counts	Total Score
Kaspersky	925	0	925	100.00%	0	100.00
Total Defense	925	4	921	99.57%	0	99.57
Dr.Web	925	6	919	99.35%	0	99.35
ESET	925	12	913	98.70%	0	98.70

- 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 granted 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

Chap.4 Test Summary & Monthly Award

- Monthly Award:

2025 April	Android Malware Detection Test from Testing Ground Labs
Kaspersky Total Defense Dr.Web ESET	**5 Star Monthly Award 2025 April** **Enterprise Product**

Chap.5 Compliance

This test was made in accordance with the requirements of the AMTSO Testing Protocol Standard v.1.3 https://www.amtso.org/standards/. and is confirmed by AMTSO as the compliant with the Standard.

Chap.6 Rights Statement

Unless otherwise stated, Testing Ground Labs (hereinafter referred to as "TG Labs"), owns the copyright of this report. Without prior written consent of TG Labs, no other organization or individual shall have the right to alter the contents of this report and use it for commercial purposes by any means (including but not limited to transmission, dissemination, reproduction, excerpt, etc.).

Unless otherwise stated, TG Labs shall be the rightful owner of the trademarks and service marks used in the report. Any action of infringing upon the legal rights of TG Labs is prohibited. TG Labs shall have the right to pursue the legal liability of the infringer in accordance with the law.

Chap.7 Disclaimer

Note that before using the report issued by Testing Ground Labs (hereinafter referred to as "TG Labs"), please carefully read and fully understand the terms and conditions of this disclaimer (hereinafter referred to as "Disclaimer"), including the clauses of exclusion or restriction of the liabilities of TG Labs and the limitations of the rights of users. If you have any objection to the terms and conditions of this Disclaimer, you have the right not to use this report, the act of using this report will be regarded as acceptance and the recognition of the terms and conditions of this Disclaimer, so by using this report, you agree to the following terms and conditions:

1. The report is provided by TG Labs, all the contents contained herein are for reference purposes only, and will not be regarded as the suggestion, invitation, or warranty for readers to choose, purchase or use the products mentioned herein. TG Labs will not guarantee the absolute accuracy and completeness of the contents of the report; you should not rely solely on this report, or substitute the viewpoints of the report for your independent judgment. If you have any queries, please consult the relevant departments of the State, and then choose, purchase or use products by your independent judgment.
2. The contents contained herein is the judgment made by TG Labs to the product characteristics as of the date the report was published. In the future, TG Labs will have the right to issue new reports which contain different contents or draw different conclusions, but TG Labs has no obligation or responsibility to update the original report or inform readers of the update of it. In this case, TG Labs will bear no responsibility for readers' loss for using the original report.

3. The report may contain links to other websites, which are provided solely for the readers' convenience. The contents of the linked websites are not any part of this report. Readers shall assume the risks and losses or bear the costs when visiting such websites. TG Labs will not guarantee the authenticity, completeness, accuracy, and legitimacy of the contents of such websites (including but not limited to advertising, products or other information). TG Labs does not accept any liability (direct or indirect) for readers' damages or losses arising from their clicking on or viewing such websites to obtain some information, products, or service.
4. TG Labs may have or will have a business relationship with the companies which produce the products mentioned in this report, but have no obligation to notify readers about it, it doesn't matter if there has already been, or there will be such business relationship in the future.
5. The act of readers' receiving this report is not regarded as the establishment of the business relationship between readers and TG Labs, so there is no customer relationship existing. TG Labs does not accept any legal liability as the readers' customer.
6. The products which are used to be tested as samples by TG Labs are bought through the official channels and legal means, so the report is proper for products bought through the same, not for products bought through unofficial channels and/or illegal means. Therefore, it's the users buying such products that will be responsible for any risk or loss arising there from. TG Labs will not have or accept any liability whatsoever for any such risk or loss.
7. Some trademarks, photos or patterns owned by units or individuals will probably be used in this report, if you think your legal right and interests are infringed, please contact TG Labs promptly, TG Labs will handle the matter as quickly as possible.

TG Labs reserves the right to interpret, modify, and update the Disclaimer.

Attorney: Zhejiang CongDian Law Firm