

011 010110 101 01011101 010 001 011010

01 110 101 011 011 0



Android Malware Detection Test

Enterprise Product

2025 Dec

••• Celebrating Technology Innovation

Table of Contents

P1

Background

P3

Test Process &
Test Software

P5

Tested Result

P6

Test Summary &
Monthly Award

P7

Compliance

P7

Rights Statement

P7

Disclaimer

Report version 1.0, published on 2026.02.10, initial version

Report version 2.0, published on 2026.02.23, 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 enterprise 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 December 2025. The test environment and procedures were designed to ensure objectivity and reproducibility:

Test Environment:

- A Samsung S22 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 1241 recent, in-the-wild malware samples and 495 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.
2. Software Installation: Each security application was installed on the test device using its default configuration settings.
3. Signature Updates: Prior to each scan, 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.

<i>Vendor</i>	<i>Software</i>	<i>Version</i>
<i>Dr.Web</i>	<i>Dr.Web Mobile Security Suite</i>	<i>12.9.8(2)</i>
<i>ESET</i>	<i>ESET Endpoint Security</i>	<i>v 6.2.6.0-0</i>
<i>Kaspersky</i>	<i>Kaspersky Endpoint Security</i>	<i>10.56.1.11</i>
<i>Total Defense</i>	<i>Total Defense Mobile Security</i>	<i>16.3.9</i>

- *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)

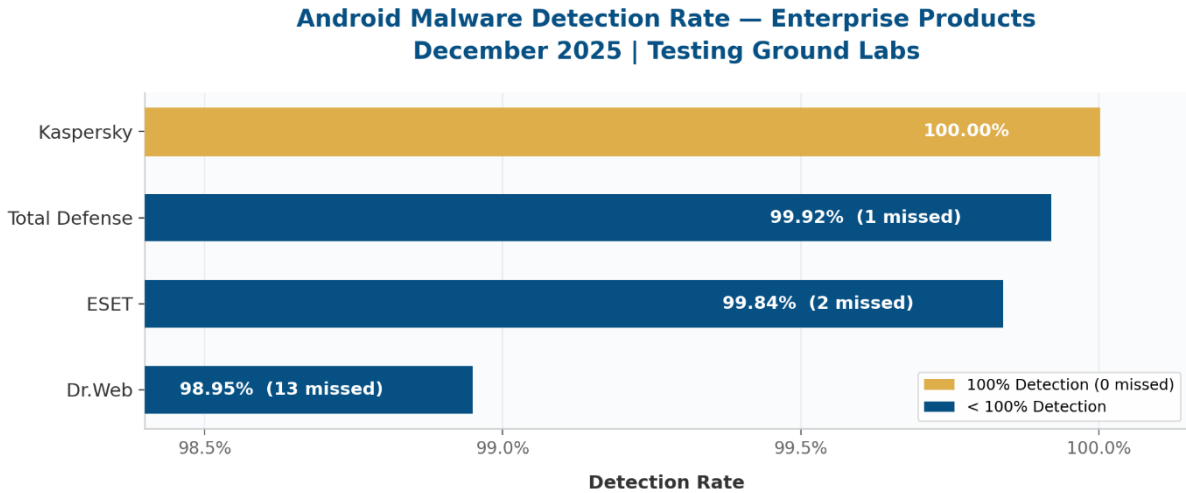
Vendor	Total Samples	Missed Samples	Detected Samples	Detection Rate	False Positive Counts	Total Score
Kaspersky	1241	0	1241	100.00%	0	100.00
Total Defense	1241	1	1240	99.92%	0	99.92
ESET	1241	2	1239	99.84%	0	99.84
Dr.Web	1241	13	1228	98.95%	0	98.95

- For each security solution, a Final Score is calculated once the full test is performed:
Final Score = (Detection %) *100 - 0.2*FP
- Based on the Final Score, the corresponding rating is assigned 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

Chap.4 Test Summary & Monthly Award

- Monthly Award:



Total Samples: 1,241 | All products tested with 0 false positives | Source: Testing Ground Labs

2025 December	Android Malware Detection Test from Testing Ground Labs
<p><i>Kaspersky</i></p> <p><i>Total Defense</i></p> <p><i>ESET</i></p> <p><i>Dr.Web</i></p>	<p>5 Star Monthly Award 2025 December</p> <p>Enterprise Product</p> 

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

Before using this report issued by Testing Ground Labs (hereinafter "TG Labs"), please read and understand the following terms and conditions (the "Disclaimer") carefully, including provisions that limit or exclude TG Labs' liability and that restrict the rights of users. Use of this report constitutes acceptance of, and agreement to, all terms and conditions set forth herein.

1. The report is provided by TG Labs, all contents are provided for reference purposes only and shall not be construed as a recommendation, invitation, or warranty to choose, purchase, or use any products mentioned herein. TG Labs does not guarantee the absolute accuracy or completeness of the report's contents; readers should not rely solely on this report or substitute its findings

for their own 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. TG Labs reserves the right to issue future reports containing different content or conclusions and is under no obligation to update this report or notify readers of any such updates. 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 assume all risks and costs associated with visiting such websites. TG Labs makes no representations regarding the authenticity, accuracy, completeness, or legality of content on linked websites (including but not limited to advertising, products or other information). TG Labs accepts no liability, direct or indirect, for any damages or losses arising from readers' access to or reliance on such linked websites.
4. TG Labs may have existing or future business relationships with companies whose products are mentioned in this report, but is under no obligation to disclose such relationships to readers, regardless of whether such relationships exist at present or may arise in the future.
5. Receipt of this report does not constitute the formation of any business or client relationship between the reader and TG Labs. TG Labs does not accept any legal liability as the readers' customer.
6. All products tested by TG Labs were procured through official and lawful channels. The findings of this report apply only to products obtained through equivalent channels, and not to products acquired through unofficial or unlawful means. Any risks or losses arising from the use of products obtained through such channels are the sole responsibility of the user. TG Labs accepts no liability in connection with such risks or losses.
7. This report may reference trademarks, images, or intellectual property owned by third parties. If you believe your rights have been infringed, please contact TG Labs promptly, TG Labs will handle the matter as quickly as possible.

TG Labs reserves the right to interpret, amend, and update this Disclaimer at any time.

Attorney: Zhejiang CongDian Law Firm