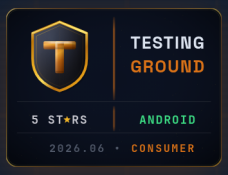
RIGOROUS. REAL. TRUSTED.

Android Malware Detection Test

Independent assessment of 9 consumer security solutions against 1,344 real-world Android malware samples.

TEST PERIOD	REPORT VERSION	PUBLISHED
June 2026	1.0	2026.08.11

9	1,344	500	8
PRODUCTS TESTED	MALWARE SAMPLES	CLEAN APPLICATIONS	5-STAR AWARDS



5-Star Monthly Award · June 2026

8 of 9 tested consumer security products achieved 5-star ratings. Avast, Avira, Kaspersky, and NortonLifeLock achieved a perfect score of 100.00 with zero false positives. Dr.Web achieved a 4-star rating.

© 2020–2026 Testing Ground Labs · www.testingground.io

NAVIGATION

Table of Contents

01 Background

02 Test Process & Software

03 Tested Results

04 Test Summary & Award

05 Compliance

06 Rights & Disclaimer

v1.0 · 2026.08.10	Initial publication of the June 2026 Consumer Android Malware Detection Test report. AMTSO compliance review is currently in progress; this report will be updated once the compliance check is confirmed.

© 2020–2026 Testing Ground Labs · www.testingground.io

CHAPTER 01

Background

Android, Google's mobile operating system built on a modified Linux kernel, remains the world's dominant computing platform — spanning phones, tablets, Android TV, and Android Auto.

Android holds roughly 72% of the global mobile OS market and powers close to 3.9 billion active devices, with penetration above 85% in large emerging markets such as India, Brazil, Indonesia, and Turkey. That scale, combined with device fragmentation and open sideloading, keeps the platform the single most attractive target for mobile-focused cybercrime.

Kaspersky's telemetry for Q1 2026 shows the shift clearly: banking trojans alone made up 52.96% of all detected malicious Android packages, out of more than 306,000 malicious installers identified in the quarter — continuing the roughly 50% quarter-on-quarter growth seen at the end of 2025. Attackers are moving past opportunistic malware toward organized, multi-stage fraud pipelines built to exploit user trust at scale.

FINANCIAL FRAUD VIA ADVANCED MALWARE

Banking trojans remain the single largest category of Android threats. Dr.Web's Q2 2026 telemetry still ranks Android.Banker as the most widespread family despite a quarter-on-quarter dip, accounting for close to a quarter of all malware detections, while Zimperium's 2026 Banking Heist Report puts the year-over-year rise in malware-driven fraudulent transactions at 67%. Modern variants combine overlay screens that mimic legitimate banking apps with app-virtualization and Accessibility Service abuse to capture credentials and one-time passcodes undetected.

NFC RELAY AND CONTACTLESS PAYMENT THEFT

NFC-based fraud has moved from a niche technique to a fast-growing mainstream threat, with relay attacks on smartphones reported to have surged 188% in 2026. Malware built on frameworks such as NFCGate now supports both "direct" schemes, where victims are tricked into tapping a card to an infected phone, and the newer "reverse" scheme, where the infected device is set as the victim's own payment method and used to cash out through ATMs. Trojans like RatOn pair this NFC relay capability with full remote-access and automated-transfer functions, making the fraud difficult to distinguish from a legitimate transaction.

© 2020–2026 Testing Ground Labs · www.testingground.io

SMISHING AS A PRIMARY DELIVERY VECTOR

SMS-based phishing is now a leading initial-access vector on mobile, accounting for roughly 35% of all phishing activity and contributing, together with vishing, to close to a fifth of all breaches. Messages disguised as delivery notifications, tax refunds, or bank alerts continue to be the most effective lure, driving installs of spyware and banking trojans that bypass the scrutiny users apply to email.

DATA ESPIONAGE AND EXTORTION

Spyware remains a persistent, high-impact threat category, with detections continuing to climb through 2025 and into 2026. Once installed, these tools quietly exfiltrate contact lists, photos, private messages, and location data, monetizing it through blackmail, identity theft, or resale on darknet markets.

AI-ASSISTED AND SYSTEM-LEVEL ATTACKS

AI-assisted malware generation is now an established part of the threat landscape, helping attackers produce variants that slip past signature-based detection. Abuse of Android's Accessibility Services remains a favored escalation path: once granted, it lets malware automate fraudulent transactions, harvest credentials across other apps, and disable security software outright. Google reports that Play Protect flagged 27 million malicious sideloaded apps in 2025, more than double the prior year, underscoring how much of the threat still arrives outside the official store.

Device fragmentation compounds all of the above: a substantial share of the active Android install base still runs versions that no longer receive security patches, and counterfeit or pre-loaded devices remain a persistent supply-chain risk in some markets. Against this backdrop, continuous, independent evaluation of consumer security solutions is essential — which is the purpose of this test.

© 2020–2026 Testing Ground Labs · www.testingground.io

CHAPTER 02

Test Process & Test Software

This section outlines the methodology behind the June 2026 test, designed to keep results objective and reproducible.

TEST DEVICE	OPERATING SYSTEM
Samsung Galaxy S22	**Android 14**
MALWARE SAMPLES	CLEAN APPLICATIONS
1,344 in-the-wild	**500 installers**

TEST ENVIRONMENT

- A Samsung Galaxy S22 was used as the primary testing platform.
- The device was running a clean installation of Android 14.
- 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.

© 2020–2026 Testing Ground Labs · www.testingground.io

TEST PROCEDURE

1. **Sample Collection:** A comprehensive test set was compiled, consisting of 1,344 recent, in-the-wild malware samples and 500 legitimate, clean application installers gathered from threat intelligence feeds and verified sources.
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 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 and any false positives were recorded.
5. **Dynamic Analysis (Behavioral Test):** Each malicious sample not detected during the static scan was manually installed and executed. Behavioral or on-execution detections were recorded.
6. **False Positive Verification:** Clean applications were scanned only — not installed or executed — serving exclusively to measure the false positive rate.

TESTED PRODUCTS — SOFTWARE & VERSIONS

© 2020–2026 Testing Ground Labs · www.testingground.io

VENDOR	SOFTWARE	VERSION
AhnLab	AhnLab V3 Mobile Security	`3.14.0.2(Build 4313)`
Avast	Avast Mobile Security	`26.11.1.260616601`
Avira	Avira Antivirus Security for Android	`7.32.0 build No. 260611311`
Dr.Web	Dr.Web Security Space for Android	`12.9.11(2)`
ESET	ESET Mobile Security	`v. 11.2.7.0-15`
Kaspersky	Kaspersky for Android	`11.132.4.15652`
McAfee	McAfee Mobile Security	`10.6.1.8`
NortonLifeLock	Norton 360 (Norton Mobile Security)	`26.10.1.260610581`
Total Defense	Total Defense Mobile Security	`16.4.3`

© 2020–2026 Testing Ground Labs · www.testingground.io

CHAPTER 03

Tested Results

Android Malware Detection Rate — Consumer Products

June 2026 · Testing Ground Labs · Total Samples: 1,344

© 2020–2026 Testing Ground Labs · www.testingground.io

VENDOR	TOTAL	MISSED	DETECTED	DETECTION RATE	FALSE POSITIVES	FINAL SCORE
Avast	1344	0	1344	100.00%	0	100.00
Avira	1344	0	1344	100.00%	0	100.00
Kaspersky	1344	0	1344	100.00%	0	100.00
NortonLifeLock	1344	0	1344	100.00%	0	100.00
ESET	1344	1	1343	99.93%	0	99.93
Total Defense	1344	1	1343	99.93%	0	99.93
McAfee	1344	2	1342	99.85%	0	99.85
AhnLab	1344	7	1337	99.48%	0	99.48
Dr.Web	1344	31	1313	97.69%	0	97.69

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

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

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

© 2020–2026 Testing Ground Labs · www.testingground.io

CHAPTER 04

Test Summary & Monthly Award

Of the 9 tested products in the June 2026 Android Malware Detection Test from Testing Ground Labs, 8 achieved 5-star ratings and 1 achieved a 4-star rating across 1,344 malware samples. No product recorded any false positives among the 500 clean applications. Avast, Avira, Kaspersky, and NortonLifeLock achieved a perfect score of 100.00.

★★★★★ 5-Star Monthly Award — June 2026

Avast	Avira	Kaspersky	NortonLifeLock
ESET	Total Defense	McAfee	AhnLab
Dr.Web			

Gold highlight = 5-star rating (Final Score 98.00 — 100.00). Avast, Avira, Kaspersky, and NortonLifeLock achieved a Perfect Score (100.00) with zero false positives. Dr.Web achieved a 4-star rating (95.00 — 97.99) this cycle.

Products achieving 5-star and 4-star ratings are entitled to display the corresponding Testing Ground Labs Monthly Award badge on their marketing materials, subject to the Rights Statement set out in this report. The Certified Consumer badge will be issued once AMTSO compliance confirmation for this test cycle is complete (see Chapter 05).

© 2020–2026 Testing Ground Labs · www.testingground.io

CHAPTER 05

Compliance

This test was conducted in accordance with the AMTSO Testing Protocol Standard v.1.3 (https://www.amtso.org/standards/). AMTSO compliance confirmation for this cycle is in progress; once complete, this report will be updated with the confirmed "Compliant" badge and the Certified Consumer marketing badge.

© 2020–2026 Testing Ground Labs · www.testingground.io

CHAPTER 06

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.

CHAPTER 07

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.
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.
3. The report may contain links to other websites provided solely for the readers' convenience. The contents of linked websites are not part of this report. 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.
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.

© 2020–2026 Testing Ground Labs · www.testingground.io

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