INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-13 14:27 UTC

Android Intrusion Logging Addresses Forensic Gap for High-Risk Users Targeted by Spyware

SECURITY ANALYSIS | MEDIUM | CVSS 7.5

SCC Item ID	SCC-STY-2026-0125
Type	Security Analysis
Severity	MEDIUM
CVSS Base Score	7.5
Affected Products	Android 16 (Google), Chrome on Android, Revolut, Itaú, Nubank (banking call verification), Gemini on Android
Published	2026-05-13T02:55:42
Discovery Source	Rss

Executive Summary

Google has shipped Intrusion Logging as part of Android's Advanced Protection Mode, a capability that stores end-to-end encrypted forensic logs on remote servers, outside the reach of spyware that has already compromised the device. Co-developed with Amnesty International and Reporters Without Borders, the feature directly addresses the forensic destruction problem that has historically allowed commercial spyware operators, including NSO Group and Paragon Solutions, to evade post-incident attribution. Paired with expanded live threat detection, banking call verification, and announced post-quantum cryptography improvements, this update signals that mobile device security is maturing from reactive patching toward proactive forensic resilience, a shift with direct implications for enterprise mobile programs and high-risk user protection policies.

Technical Analysis

The central problem Intrusion Logging solves is well-documented in spyware forensics: once a sophisticated implant achieves kernel-level or privileged access on a device, it can suppress, delete, or falsify local logs. This meant that by the time a forensic investigator, whether from Amnesty International's Security Lab or an enterprise incident response team, examined a suspected Pegasus or Graphite-compromised device, the evidence trail was cold or manipulated. Intrusion Logging routes encrypted forensic telemetry to Google's servers rather than storing it solely on the device. Because the encryption is end-to-end, Google cannot read the logs; only the account holder can. The threat model this counters maps directly to several MITRE ATT&CK Mobile techniques present in this advisory: T1406 (Obfuscated Files or Information), T1636 (Protected User

Data Access), and T1516 (Input Injection), among others. These are the operational fingerprints of commercial spyware campaigns.

The broader 2026 Android security package adds several complementary controls. Post-quantum cryptography improvements, while not tied to an immediate threat, reflect the 'harvest now, decrypt later' concern that intelligence agencies and sophisticated actors represent for communications intercepted today. The expansion of Live Threat Detection, which already covered some stalkerware categories, extends behavioral analysis coverage. OTP hiding addresses a specific on-device interception pattern where malware with accessibility or notification access reads one-time codes before the user sees them, corresponding to T1417 (Input Capture) and T1582 (SMS Control). Banking call verification, announced for integration with Revolut, Itaú, and Nubank, targets social engineering scenarios where attackers impersonate bank representatives while the victim is on a call, a pattern that has driven significant financial fraud losses in Brazil, the UK, and Eastern Europe.

The CWE mapping is instructive for defenders: CWE-359 (Exposure of Private Personal Information), CWE-311 (Missing Encryption of Sensitive Data), and CWE-532 (Insertion of Sensitive Information into Log File) collectively describe the failure modes these controls are designed to close. For security teams running mobile device management programs, the practical implication is that Advanced Protection Mode, previously positioned primarily for individual high-risk users, now carries enterprise-relevant forensic capability that MDM policies should formally address.

Sources: Google Security Blog (T1, 2026); The Hacker News, BleepingComputer, Engadget, AndroidGuys (T3, 2026).

Action Checklist

1. Step 1: Assess exposure, identify which employees in your organization qualify as high-risk users (executives, legal counsel, finance leads, journalists, government liaisons) who are potential commercial spyware targets and are currently using Android devices
2. Step 2: Review controls, audit your MDM or UEM policy to determine whether Advanced Protection Mode is enforced or recommended for high-risk user segments; confirm whether Intrusion Logging can be enabled at the policy level in your MDM platform
3. Step 3: Update threat model, incorporate commercial spyware vendors (NSO Group, Paragon Solutions) as credible threat actors in your mobile threat register, particularly for industries subject to geopolitical targeting: media, NGOs, financial services, government contracting
4. Step 4: Evaluate banking app exposure, if your organization uses Revolut, Itaú, Nubank, or similar banking apps on corporate or BYOD devices, confirm whether banking call verification is available and enabled; review social engineering scenarios in your mobile security awareness program
5. Step 5: Communicate findings, brief leadership on the forensic gap this update closes; frame it as a signal that mobile devices are now a primary spyware delivery surface requiring the same policy rigor as endpoint workstations
6. Step 6: Monitor developments, track Google's rollout timeline for Intrusion Logging across the Android device fleet in your environment; prioritize ensuring high-risk users are running current Android versions

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if MVT analysis of a high-risk user's Android device returns positive indicators matching NSO Group or Paragon Solutions IOCs, if a high-risk user reports an unexpected or suspicious call from a number spoofing Revolut, Itaú, or Nubank, or if your organization operates in a sector (media, NGO, financial services, government contracting) with a documented history of geopolitical targeting by commercial spyware operators — any of these conditions triggers potential breach notification obligations under GDPR, CCPA, or sector-specific regulations if PII or privileged communications were accessed.
Recovery Notes	If a commercial spyware compromise is confirmed on an Android device, do not attempt to remediate the device in place — Pegasus and Graphite implants with SELinux bypass capability can survive factory reset on some firmware versions; the device must be physically replaced and the compromised device preserved as forensic evidence under chain of custody per NIST IR-4. Enable Intrusion Logging on the replacement device immediately upon enrollment, and request the encrypted log archive from Google for the compromised device if it was running Android 16 with APM active at any point during the suspected compromise window. Monitor the replacement device and all accounts the compromised device had access to (email, banking apps, VPN credentials) for at least 90 days, as Pegasus operators have demonstrated persistence through credential harvesting that survives device replacement.
Forensic Artifacts	MVT (Mobile Verification Toolkit) analysis output: run 'mvt-android check-backup' or 'mvt-android check-adb' against the device using the latest Amnesty IOC list (github.com/mvt-project/mvt/blob/main/iocs); positive hits on known Pegasus or Paragon Graphite domains, process names (e.g., bh, bridgehead, liblgplayer.so), or network indicators are the primary forensic confirmation of commercial spyware compromise | Android Intrusion Logging encrypted archive (Android 16 + APM only): if the device was enrolled in Advanced Protection Mode prior to compromise, request the tamper-resistant log package from Google — this is the only forensic artifact that survives on-device destruction by a root-level spyware implant and is the specific gap this feature closes | Android device backup via 'adb backup -all -f device_backup.ab' captured before any remediation: preserves app data, notification history, and call logs that MVT can parse for spyware indicators including unauthorized Revolut, Itaú, or Nubank data access, which is relevant to the banking call verification social engineering vector in this advisory | Network traffic capture from the device's last known connection point (corporate Wi-Fi access point logs, firewall NetFlow, or Wireshark capture on a monitored network): Pegasus C2 infrastructure has used domains mimicking legitimate services; Amnesty-published network IOCs should be used to query DNS query logs and firewall connection logs for the device's MAC address or assigned IP during the suspected compromise window | Google Account and Chrome on Android audit logs: request Google Account activity export (myaccount.google.com/data-and-privacy) for the high-risk user — Chrome browsing history, location history, and app activity logs may contain evidence of zero-click exploit delivery via a malicious link or browser-based exploit chain, which is a documented Pegasus delivery vector on Android; Chrome on Android is explicitly named as an affected application in this advisory

Per-Action IR Details

Step 1: Assess exposure — identify which employees in your organization qualify as high-risk users (executives, legal counsel, finance leads, journalists, government liaisons) who are potential commercial spyware targets and are currently using Android devices

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and identifying assets requiring elevated protection prior to an incident

Controls: NIST IR-4 (Incident Handling) — build handling capability scoped to mobile spyware threat actors including NSO Group and Paragon Solutions, NIST RA-2 (Security Categorization) — categorize high-risk user devices separately given elevated targeting likelihood by commercial spyware operators, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — enumerate all Android devices held by high-risk personnel with OS version, MDM enrollment status, and APM eligibility

Compensating: Export your MDM device inventory (Jamf, Intune, or Google Workspace Admin SDK devices.list API) to a spreadsheet; cross-reference against your HR role taxonomy to flag executive, legal, finance, and government liaison accounts. If no MDM exists, run 'adb devices' inventory script across enrolled devices or distribute a Google Form to high-risk users requesting device model and Android version. Takes under 2 hours for a 2-person team on a sub-500-user org.

Evidence: Before conducting the role-based exposure assessment, capture the current Android OS version distribution across your fleet (MDM device report or Google Admin Console > Devices > Mobile & Endpoints). Document which devices are NOT on Android 16 — these are the devices where Intrusion Logging is unavailable and the forensic gap exploited by Pegasus and Graphite spyware still exists. Preserve this baseline inventory as a dated snapshot; it establishes pre-remediation exposure scope if a retrospective investigation is later needed.

Step 2: Review controls — audit your MDM or UEM policy to determine whether Advanced Protection Mode is enforced or recommended for high-risk user segments; confirm whether Intrusion Logging can be enabled at the policy level in your MDM platform

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Acquiring tools and configuring systems to support incident detection and evidence collection before an incident occurs

Controls: NIST SI-4 (System Monitoring) — extend monitoring policy explicitly to Android endpoints for high-risk users to capture the tamper-resistant Intrusion Logging telemetry introduced in Android 16, NIST CM-6 (Configuration Settings) — enforce Advanced Protection Mode and Intrusion Logging as a baseline configuration requirement for high-risk user device profiles in MDM policy, CIS 4.6 (Securely Manage Enterprise Assets and Software) — manage Android device configuration through MDM version-controlled policy profiles, including APM enforcement for designated user groups, CIS 8.2 (Collect Audit Logs) — Intrusion Logging under Android Advanced Protection Mode is the only mechanism that stores forensic logs outside the reach of on-device spyware such as Pegasus or Paragon's Graphite; enabling it is the audit log collection action for this threat

Compensating: If your MDM platform (Intune, Jamf Pro, VMware Workspace ONE) does not yet expose an Advanced Protection Mode toggle in policy profiles, enforce it manually: distribute a step-by-step enrollment guide to high-risk users directing them to Settings > Security & Privacy > Advanced Protection. Validate compliance by querying MDM device compliance reports or, without MDM, by requesting a screenshot of the APM status screen from each high-risk user. Track completion in a shared spreadsheet with a date-stamped confirmation column.

Evidence: Pull your MDM's current Android device compliance report before making any policy changes — this documents the pre-hardening baseline. Export the full policy profile applied to high-risk user device groups and preserve it as a versioned artifact. If Intrusion Logging was previously disabled or unconfigured, this baseline establishes the forensic gap window: the period during which commercial spyware operators such as NSO Group could have compromised a device and destroyed on-device forensic artifacts without any tamper-resistant log capture in place.

Step 3: Update threat model — incorporate commercial spyware vendors (NSO Group, Paragon Solutions) as credible threat actors in your mobile threat register, particularly for industries subject to geopolitical targeting: media, NGOs, financial services, government contracting

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Developing and maintaining threat intelligence resources and updating IR plans to reflect current adversary capability

Controls: NIST RA-3 (Risk Assessment) — formally document NSO Group (Pegasus) and Paragon Solutions (Graphite) as threat actors in the organizational risk register with assessed likelihood calibrated to your industry sector, NIST IR-8 (Incident Response Plan) — update the mobile IR plan to include zero-click spyware delivery scenarios (iMessage, WhatsApp, and browser-based zero-click chains used by Pegasus) as named incident categories, NIST SI-5 (Security Alerts, Advisories, and Directives) — subscribe to Amnesty International Security Lab and Citizen Lab advisories, which have historically provided the earliest public attribution of Pegasus and Graphite campaigns

Compensating: Add the following free threat intel sources to a weekly review rotation: Amnesty International Security Lab GitHub (github.com/AmnestyTech/investigations), Citizen Lab reports (citizenlab.ca/category/research), and MITRE ATT&CK Mobile matrix — specifically T1424 (Process Discovery), T1417 (Input Capture), T1516 (Input Injection), and T1513 (Screen Capture), which map to documented Pegasus and Graphite capabilities. Create a simple threat actor card in your risk register for each vendor covering: known zero-click delivery vectors, targeted sectors, and known IOC types (process names, network infrastructure patterns documented by Amnesty).

Evidence: Before updating the threat model, retrieve and preserve the latest Amnesty International Security Lab Mobile Verification Toolkit (MVT) IOC lists (available at github.com/mvt-project/mvt) — these contain domain, process, and network indicators associated with confirmed Pegasus and Paragon deployments. Also retrieve the most recent Citizen Lab report relevant to your sector. These serve as the evidentiary basis for the threat actor additions to your risk register and establish the intelligence cutoff date for your model update.

Step 4: Evaluate banking app exposure — if your organization uses Revolut, Itaú, Nubank, or similar banking apps on corporate or BYOD devices, confirm whether banking call verification is available and enabled; review social engineering scenarios in your mobile security awareness program

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: User awareness training and establishing preventive controls for known social engineering attack vectors

Controls: NIST IR-2 (Incident Response Training) — update mobile security awareness training to include vishing and fraudulent banking call scenarios targeting Revolut, Itaú, and Nubank users, which are enabled by spyware-assisted caller ID spoofing and credential interception, NIST SC-8 (Transmission Confidentiality and Integrity) — verify that banking call verification features in Revolut, Itaú, and Nubank are active, as these represent the application-layer integrity control for voice-channel social engineering enabled by Pegasus-class spyware, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — inventory which high-risk users have Revolut, Itaú, or Nubank installed on corporate or BYOD devices to scope the social engineering attack surface

Compensating: Manually verify banking call verification status for Revolut (Settings > Security > Revolut Phone Number Verification), Itaú, and Nubank by requesting users to walk through the setting with a team member or via screen share. Develop a one-page awareness brief specific to the spyware-assisted vishing scenario: attacker compromises device via zero-click spyware, intercepts or spoofs banking calls, then conducts fraudulent wire transfer or credential harvesting. Distribute to all high-risk users identified in Step 1. No SIEM required — this is a human-layer control.

Evidence: If a high-risk user reports a suspicious banking call or unexpected transaction, the forensic evidence to capture immediately includes: (1) the call log from the Android dialer (Settings > Call History export or adb backup), (2) notification history accessible via adb shell dumpsys notification, which may show spoofed banking app notifications injected by spyware, and (3) MVT analysis output targeting Revolut, Itaú, or Nubank process invocations in the Android backup, which can surface unauthorized access to banking app data stores by a Pegasus-class implant.

Step 5: Communicate findings — brief leadership on the forensic gap this update closes; frame it as a signal that mobile devices are now a primary spyware delivery surface requiring the same policy rigor as endpoint workstations

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned communication and policy improvement driven by new threat intelligence, applied here proactively before a confirmed incident

Controls: NIST IR-6 (Incident Reporting) — brief leadership on the threat intelligence basis for this policy change, including the historical forensic gap that allowed Pegasus and Graphite operators to evade post-incident attribution on

Android devices prior to Intrusion Logging, NIST IR-8 (Incident Response Plan) — update the IR plan to formally classify commercial spyware compromise of a mobile device as a Tier 1 incident category requiring the same escalation path as a confirmed endpoint compromise, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — present the Android 16 Intrusion Logging capability as a vulnerability management gap closure, specifically the gap that commercial spyware operators have exploited to destroy forensic artifacts on compromised Android devices

Compensating: Prepare a one-page executive brief using a concrete recent case: reference the 2024 Paragon Solutions Graphite campaign targeting WhatsApp users on Android (reported by Citizen Lab, February 2025) as the specific threat model. Quantify the forensic gap: prior to Android 16 Intrusion Logging, a Pegasus or Graphite implant with root or SELinux bypass could delete its own artifacts, leaving investigators with no on-device evidence — MVT analysis would return inconclusive results. Frame Intrusion Logging as closing this specific gap. No budget required for this step; the brief itself is the deliverable.

Evidence: The supporting evidence for the leadership brief should include: the dated baseline inventory from Step 1 (showing current exposure), the MDM policy gap documented in Step 2 (showing APM is not yet enforced), and a reference to at least one confirmed Citizen Lab or Amnesty report documenting forensic destruction by the specific spyware operators named (NSO Group, Paragon Solutions). These three artifacts together demonstrate existing exposure, current control gap, and adversary capability — the minimum evidentiary standard for a credible risk briefing.

Step 6: Monitor developments — track Google's rollout timeline for Intrusion Logging and post-quantum cryptography across the Android device fleet in your environment; prioritize Android 16 upgrade paths for high-risk users

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Using lessons learned and threat intelligence to drive sustained improvement in detection and protection capability

Controls: NIST SI-2 (Flaw Remediation) — prioritize Android 16 upgrade paths for high-risk users as a formal flaw remediation action, given that Intrusion Logging and post-quantum cryptographic protections against long-term Pegasus traffic interception are only available on Android 16, NIST SI-5 (Security Alerts, Advisories, and Directives) — establish a standing subscription to Google Android security bulletins and Amnesty International Security Lab releases to track Intrusion Logging feature availability by device model and carrier, CIS 7.3 (Perform Automated Operating System Patch Management) — enforce automated or MDM-pushed OS upgrade tracking for Android 16 availability on high-risk user devices, with manual escalation for devices where OEM or carrier delays block the upgrade, CIS 7.2 (Establish and Maintain a Remediation Process) — document a risk-accepted exception for any high-risk user device that cannot be upgraded to Android 16 within 30 days, with compensating controls (MDM-enforced app restrictions, network segmentation) formally recorded

Compensating: Create a tracking spreadsheet with columns: device model, current Android version, Android 16 OEM availability date (sourced from the manufacturer's update schedule), MDM enrollment status, and APM/Intrusion Logging enabled flag. Review and update monthly. For devices that cannot reach Android 16 due to OEM end-of-support, escalate to a device replacement recommendation for the specific high-risk user. Subscribe to the Android Security Bulletin RSS feed (android.googleblog.com) and Amnesty Tech GitHub releases (github.com/AmnestyTech) using a free RSS reader — no SIEM required for this monitoring track.

Evidence: Maintain a version-controlled record of which Android devices in your high-risk user population have reached Android 16 and have Intrusion Logging active (captured from MDM compliance reports). This record serves as the forensic readiness baseline: if a future Pegasus or Graphite compromise is suspected, investigators using MVT can request the Intrusion Logging encrypted archive from Google's servers for enrolled devices, but only if the feature was active at the time of the suspected compromise. Gap periods — dates when the device was not on Android 16 or APM was not enabled — must be documented as forensic blind spots in any retrospective investigation.

Detection Guidance

Intrusion Logging is itself a detection mechanism, but security teams should understand what it produces and how to operationalize it. If a high-risk user's device is suspected of compromise, the encrypted logs stored server-side can be retrieved and analyzed for anomalous process activity, privilege escalation attempts, and data exfiltration patterns. Teams should establish a pre-incident process for enrolling high-risk users in Advanced Protection Mode before a suspected compromise occurs, not after, since post-compromise enrollment may not capture earlier activity.

For broader behavioral hunting relevant to the MITRE techniques in this story: monitor for applications requesting accessibility service permissions without clear user-initiated justification (T1417, T1516); audit notification listener permissions across managed devices for apps that should not have them, a common OTP interception vector (T1582); look for anomalous background data usage from apps during low-activity periods, which can indicate covert telemetry exfiltration (T1437); and review location permission grants for apps that do not have a functional need for precise location (T1430).

For enterprises using MAM or MDM platforms, review whether your platform exposes threat detection telemetry from Android's Live Threat Detection API. If not, this is a gap worth raising with your MDM vendor. Logs to prioritize: device enrollment anomalies, app installation events outside managed channels, permission change events, and any alerts generated by Google Play Protect in managed profiles.

Framework Mappings

MITRE-ATTACK

- **T1444**
- **T1406** — Obfuscated Files or Information
- **T1430** — Location Tracking
- **T1417** — Input Capture
- **T1636** — Protected User Data
- **T1437** — Application Layer Protocol
- **T1582** — SMS Control
- **T1512** — Video Capture
- **T1521** — Encrypted Channel
- **T1516** — Input Injection

NIST-800-53R5

- **SI-2** — Flaw Remediation
- **SC-13** — Cryptographic Protection
- **SI-4** — System Monitoring

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1444		
T1406	Obfuscated Files or Information	Defense-Evasion
T1430	Location Tracking	Collection
T1417	Input Capture	Collection
T1636	Protected User Data	Collection
T1437	Application Layer Protocol	Command-And-Control
T1582	SMS Control	Impact
T1512	Video Capture	Collection
T1521	Encrypted Channel	Command-And-Control
T1516	Input Injection	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/android-adds-intrusion-logging-fo...	T3
What's New in Android Security and Privacy in 2026 - Google Blog	https://blog.google/security/whats-new-in-android-security-privacy-...	T1
Google Announces Upcoming Security Tools For Android, Including ...	https://www.engadget.com/2169750/google-announces-upcoming-security...	T3

Source	URL	Tier
Google Android 17: New Security Features for 2026 - AndroidGuys	https://androidguys.com/news/android-announces-2026-security-update...	T3
Android 17 to expand banking scam call and privacy protections	https://www.bleepingcomputer.com/news/security/android-17-to-expand...	T3

Generated 2026-05-13 14:27 UTC by TJS Security Command Center