INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:39 UTC

Perseus Android Malware Breaks New Ground by Scanning Note-Taking Apps for Passwords and Recovery Phrases

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0067
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Android 13+; Google Keep, Evernote, Microsoft OneNote, Samsung Notes, Xiaomi Notes, ColorNote, Simple Notes; financial institutions in Turkey, Italy, Poland, Germany, and France; nine cryptocurrency platforms
Published	2026-03-21

Executive Summary

Perseus is a newly identified Android banking trojan targeting financial institutions across Turkey, Italy, Poland, Germany, and France, as well as nine cryptocurrency platforms. Distributed through fake IPTV applications, it introduces a capability not seen in prior Cerberus-lineage malware: automated scanning of popular note-taking apps including Google Keep, Evernote, and Microsoft OneNote to extract passwords, cryptocurrency wallet recovery phrases, and financial credentials stored in plaintext. Organizations with BYOD or corporate-liable device programs face elevated risk, as employees routinely store sensitive credentials in consumer note apps that lack enterprise data protection controls.

Technical Analysis

Perseus derives from the Cerberus/Phoenix Android banking trojan codebase and targets Android 13 and later. Initial delivery is via trojanized IPTV applications distributed outside the Google Play Store. The malware abuses Android Accessibility Services to perform overlay attacks against targeted banking and cryptocurrency applications, intercept keystrokes, and read screen content across running apps. The distinguishing capability is a note-scanning module that enumerates content from Google Keep, Evernote, Microsoft OneNote, Samsung Notes, Xiaomi Notes, ColorNote, and Simple Notes, extracting credentials and cryptocurrency seed phrases stored in unprotected notes. Exfiltrated data is transmitted to attacker-controlled infrastructure. Relevant CWEs: CWE-926 (Improper Export of Android Application Components), CWE-927 (Use of Implicit Intent for Sensitive Communication), CWE-312 (Cleartext Storage of Sensitive Information). MITRE ATT&CK for Mobile techniques

include T1513 (Screen Capture), T1418 (Software Discovery), T1444 (Masquerade as Legitimate Application), T1629.003 (Impair Defenses: Disable or Modify Tools), T1417 (Input Capture), T1409 (Stored Application Data), T1429 (Capture Audio), T1516 (Input Injection), T1406 (Obfuscated Files or Information), T1421 (System Network Connections Discovery), and T1627 (Execution Guardrails). No CVE has been assigned. Attribution to a named threat actor has not been confirmed as of March 2026 per ThreatFabric reporting. No vendor patch addresses Perseus directly, as this is a malware family rather than a patched vulnerability; mitigations are configuration and policy-based.

Action Checklist

1. Step 1, Immediate: Issue guidance to employees with BYOD or corporate-liable Android devices prohibiting storage of passwords, recovery phrases, or financial credentials in consumer note-taking applications (Google Keep, Evernote, OneNote, Samsung Notes, Xiaomi Notes, ColorNote, Simple Notes).
2. Step 2, Immediate: Block sideloading of applications on managed Android devices via MDM policy; enforce Google Play Protect and restrict installation sources to the official Play Store.
3. Step 3, Detection: Review MDM and endpoint telemetry for Android devices running apps with Accessibility Service permissions granted to non-system, non-approved applications; flag and investigate anomalies.
4. Step 4, Assessment: Inventory BYOD and corporate-liable Android devices running Android 13 or later; identify any devices with the targeted note-taking apps (Google Keep, Evernote, OneNote, Samsung Notes, Xiaomi Notes, ColorNote, Simple Notes) installed and assess whether sensitive data is stored in those apps.
5. Step 5, Communication: Notify security operations, mobile device management administrators, and relevant HR or legal stakeholders about the campaign scope; if your organization has users in Turkey, Italy, Poland, Germany, or France, elevate priority accordingly.
6. Step 6, Long-term: Enforce enterprise-grade credential storage policy requiring password managers with encryption at rest (e.g., 1Password, Bitwarden) in place of consumer note apps; update BYOD acceptable use policy to explicitly prohibit plaintext credential storage; review mobile threat defense (MTD) tooling coverage for Accessibility Service abuse detection.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm or law enforcement if any device is confirmed to have Perseus indicators (Accessibility Service permissions to malicious app, note app data exfiltration, network traffic to known C2), or if your organization has users in the five targeted regions (Turkey, Italy, Poland, Germany, France) and cannot validate device inventory within 48 hours.

Recovery Notes	Post-containment, conduct a 30-day forensic review: (1) retain full device forensics (APK extraction, logcat, SQLite databases from note apps) for devices where credentials may have been exposed; (2) mandate credential rotation for all financial and crypto accounts whose recovery phrases or passwords may have been stored in note apps; (3) conduct a post-incident review per NIST 800-61r3 §4.3 to document root cause (lack of MTD, weak policy), gaps in detection, and preventive measures (e.g., password manager rollout success, policy update effectiveness). Schedule lessons-learned session 2 weeks post-eradication with security operations, MDM, and affected business units.
Forensic Artifacts	Android MDM enrollment and policy application logs (timestamps, device IDs, policy versions) | Accessibility Service permission grant logs from affected devices (via ADB: dumpsys accessibility or MDM telemetry) | Note-taking app databases and cache files (/data/data/com.google.android.keep/*, /data/data/com.evernote.android.*, etc.) extracted via ADB pull | Android system logs (logcat, dumped via ADB) from flagged devices spanning 7–30 days prior to detection, filtered for app launch events and data access patterns | Network traffic captures (PCAP) from affected devices showing exfiltration attempts to unusual IP addresses or domains (use network monitor or MTD logs)

Per-Action IR Details

Step 1 — Immediate: Issue guidance to employees with BYOD or corporate-liable Android devices prohibiting storage of passwords, recovery phrases, or financial credentials in consumer note-taking applications (Google Keep, Evernote, OneNote, Samsung Notes, Xiaomi Notes, ColorNote, Simple Notes).

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (organizational readiness and security awareness)

Controls: NIST 800-53 AT-2 (awareness and training), NIST 800-53 AC-2 (account management), CIS 2.4 (user account management)

Compensating: Draft a one-page mobile credential hygiene notice citing specific app names and distribute via email with read-receipt tracking; ask managers to confirm receipt by team members. Include a simple credential checklist (What NOT to store: passwords, 2FA backup codes, seed phrases; Where to store instead: approved password manager or hardware wallet).

Evidence: Capture baseline inventory of note-taking apps installed on enrolled devices before issuing guidance (via MDM query or manual audit log). Document email distribution timestamp and read-receipt data to prove awareness communication was sent. Preserve any employee responses or remediation confirmations.

Step 2 — Immediate: Block sideloading of applications on managed Android devices via MDM policy; enforce Google Play Protect and restrict installation sources to the official Play Store.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (containment), NIST 800-53 SI-7 (software, firmware, and information integrity)

Controls: NIST 800-53 CM-5 (access restrictions for change), NIST 800-53 SI-7 (software integrity), CIS 4.1 (hardware and firmware inventory), CIS 4.12 (application whitelisting)

Compensating: If MDM is unavailable, manually audit all enrolled devices for non-Play Store app sources: navigate to Settings > Apps > Special App Access > Install Unknown Apps and screenshot each app with permission enabled. Create a signed IT policy directive requiring users to disable Unknown Sources; validate compliance via one-time manual verification and subsequent monthly spot checks documented in a shared spreadsheet.

Evidence: Export MDM policy change log with timestamp and affected device count before applying the policy. Capture baseline of devices with Unknown Sources enabled (screenshot or MDM report). After policy deployment, query MDM for devices still non-compliant and retain policy application logs (device enrollment ID, policy version, application timestamp). Document any policy enforcement failures.

Step 3 — Detection: Review MDM and endpoint telemetry for Android devices running apps with Accessibility Service permissions granted to non-system, non-approved applications; flag and investigate anomalies.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (detection and analysis), NIST 800-53 AU-12 (audit generation)

Controls: NIST 800-53 SI-4 (information system monitoring), NIST 800-53 AU-2 (audit events), CIS 8.5 (log all access to audit trails)

Compensating: Manually audit devices via ADB (Android Debug Bridge) if MDM lacks granular permission visibility: `adb shell settings get secure enabled_accessibility_services` on each enrolled device. Create a baseline spreadsheet of expected system accessibility services (e.g., Samsung Voice Assistant, system UI); any third-party app with Accessibility Service permission is an anomaly. Query monthly and flag new entries. Store results in a timestamped audit log with device serial number, app name, package ID, and grant date if available.

Evidence: Capture baseline Accessibility Service permissions report from MDM or ADB before investigation begins. Preserve MDM logs showing permission grant events (timestamp, app package name, device ID). Extract APK files of flagged third-party apps for static analysis (strings, manifest inspection). Preserve device system logs (logcat) from flagged devices for 30 days post-detection to correlate with data exfiltration patterns.

Step 4 — Assessment: Inventory BYOD and corporate-liable Android devices running Android 13 or later; identify devices with any of the seven targeted note-taking apps installed and assess whether sensitive data is stored in those apps.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1.2 (analysis), NIST 800-53 CM-8 (information system component inventory)

Controls: NIST 800-53 CM-8 (information system component inventory), NIST 800-53 SA-4 (acquisition process), CIS 1.1 (hardware inventory)

Compensating: If MDM lacks app inventory visibility, issue a compliance form to all mobile device users requesting: (1) Android OS version (Settings > About Phone > Android Version), (2) installed note-taking apps (Settings > Apps > See All Apps, filter by 'Keep', 'Note', 'Evernote', 'OneNote', 'ColorNote', 'Simple'), (3) sensitive data stored in those apps (yes/no/unknown). Collect responses in a shared spreadsheet with device owner, device IMEI, and submission date. Follow up non-responders within 5 business days with escalation to their manager.

Evidence: Preserve MDM app inventory queries (export date, device count, app distribution report). Document the compliance form template, distribution date, and response tracking. For devices identified with target apps: screenshot the app's note content folders (without capturing credentials), document file paths, note modification dates. Retain device serial numbers, OS versions, and user identity for all flagged devices.

Step 5 — Communication: Notify security operations, mobile device management administrators, and relevant HR or legal stakeholders about the campaign scope; if your organization has users in Turkey, Italy, Poland, Germany, or France, elevate priority accordingly.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (tools and resources) and §4.1 (post-incident activities: lessons learned)

Controls: NIST 800-53 IR-4 (incident handling), IR-6 (incident reporting), CIS 5.2 (incident response procedures)

Compensating: Draft a formal incident communication memo (to: CISO, SOC Manager, MDM Admin, Legal, HR) with subject 'Perseus Android Malware Campaign — Immediate Action Required'. Include: (1) threat summary (2-3 sentences), (2) affected regions and user count in your organization, (3) immediate mitigation steps assigned to each team with due dates, (4) escalation criteria (any device with Perseus indicators = immediate isolation), (5) contact for questions. Distribute via secure email with read-receipt tracking and document delivery. Schedule 24-hour follow-up check-in call with CISO.

Evidence: Retain the memo template, distribution list, timestamps, and read receipts. Document attendance or notes from any follow-up briefings. Preserve email chains showing acknowledgment from each stakeholder group. If legal/HR provide guidance (e.g., GDPR notification requirements), archive those directives.

Step 6 — Long-term: Enforce enterprise-grade credential storage policy requiring password managers with encryption at rest (e.g., 1Password, Bitwarden) in place of consumer note apps; update BYOD acceptable use policy to explicitly prohibit plaintext credential storage; review mobile threat defense (MTD) tooling coverage for Accessibility Service abuse detection.

NIST Phase: Recovery

Reference: NIST 800-61r3 §4 (post-incident activities), NIST 800-53 AC-2 (account management), IA-5 (authentication)

Controls: NIST 800-53 IA-5 (authentication — password management), NIST 800-53 SC-13 (cryptographic protection), NIST 800-53 IR-6 (incident reporting, post-incident review), CIS 4.5 (password policy enforcement), CIS 5.2 (incident response procedures)

Compensating: Deploy Bitwarden (free, open-source password manager) enterprise trial for 90 days: (1) host Bitwarden Server on-premises or use Bitwarden Cloud; (2) issue org policy requiring all employees to migrate credentials from note apps by end of trial; (3) conduct monthly spot-checks using ADB to verify note apps are empty of credentials (per Step 3 methodology); (4) update BYOD Acceptable Use Policy explicitly stating 'No plaintext storage of credentials in note-taking, email, or messaging apps'; (5) require digital signature acknowledgment from all users. For MTD: evaluate free alternatives (e.g., Zimperium, Lookout free tiers) for Accessibility Service abuse alerts or implement manual monthly audits per Step 3.

Evidence: Archive the updated BYOD policy with version control and effective date. Preserve Bitwarden deployment logs, user enrollment counts, and migration completion reports. Document MTD evaluation matrix (tools evaluated, cost, feature comparison). Retain signed user acknowledgments of updated policy. Store baseline and post-deployment Accessibility Service permission reports to measure compliance improvement.

Detection Guidance

No confirmed IOCs (hashes, domains, IPs) have been released in available public reporting as of this analysis; detection must rely on behavioral indicators. In MDM and MTD platforms, alert on: (1) Accessibility Service grants to applications not on an approved allowlist, particularly apps installed outside the Play Store; (2) applications with package names or certificates not matching known-good IPTV or streaming applications that request Accessibility, Overlay, or Device Admin permissions; (3) high-frequency screen content reads or cross-app content access events from non-system processes. In network monitoring, look for anomalous outbound HTTPS traffic from Android devices to newly registered or low-reputation domains, particularly from applications that should not have network activity. On devices using Android Enterprise with work profiles, verify that note-taking apps in the personal profile cannot access work-profile data. Organizations using SIEM with MDM integration (e.g., Microsoft Sentinel with Intune, Splunk with Jamf) should query for Accessibility Service enable events on unmanaged or recently enrolled devices. Source: ThreatFabric Perseus analysis (March 2026).

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not available`	No C2 domains have been published in available public reporting as of this analysis. Monitor ThreatFabric and BleepingComputer for updates.	LOW

Type	Value	Context	Confidence
HASH	`Not available`	No sample hashes have been published in available public reporting as of this analysis. Check ThreatFabric threat intelligence feeds for sample releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T1513** — Screen Capture
- **T1418** — Software Discovery
- **T1444**
- **T1629.003** — Disable or Modify Tools
- **T1417** — Input Capture
- **T1409** — Stored Application Data
- **T1429** — Audio Capture
- **T1516** — Input Injection
- **T1406** — Obfuscated Files or Information
- **T1421** — System Network Connections Discovery
- **T1627** — Execution Guardrails

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1513		
T1418		
T1444		
T1629.003		
T1417		

Technique ID	Technique Name	Tactic
T1409		
T1429		
T1516		
T1406		
T1421		
T1627		

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-perseus-android-...	T3
Perseus: DTO malware that takes notes - Threat Fabric	https://www.threatfabric.com/blogs/perseus-dto-malware-that-takes-n...	T3
Perseus Android Malware Steals User Notes and Enables Full ...	https://www.cryptika.com/perseus-android-malware-steals-user-notes-...	T3
New Android malware is built to scan your notes for sensitive details	https://tech.yahoo.com/cybersecurity/articles/android-malware-built...	T3
Perseus Android Trojan Reads Your Notes Apps - AnonHaven	https://anonhaven.com/en/news/perseus-android-trojan-notes-2026/	T3

Generated 2026-03-29 18:39 UTC by TJS Security Command Center