INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 19:19 UTC

Rokarolla Android Banking Trojan: 137-Command RAT Targets 217 Financial Apps, Defeats Standard Mobile Defenses

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0487
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	217 Android banking and cryptocurrency applications (including 'imagin' banking app); Google Play Protect; Android OS (version range unspecified in source data)
Published	2026-06-16T09:10:17
Discovery Source	Rss

Executive Summary

Zimperium zLabs has documented Rokarolla, an Android banking trojan with a 137-command remote access framework targeting 217 banking and cryptocurrency applications. The malware bypasses Google Play Protect, intercepts SMS one-time passwords, captures PINs, and hijacks clipboard content, giving attackers direct access to mobile banking sessions and cryptocurrency wallets. Organizations with employees or customers using Android mobile banking are exposed through behavior-based attack surfaces that no single patch resolves.

Technical Analysis

Rokarolla is an Android banking trojan documented by Zimperium zLabs (report dated 2026-06-16) carrying a 137-command RAT framework, described by Zimperium as the largest command set catalogued in this malware class. It targets 217 banking and cryptocurrency Android applications, including the 'imagin' banking app. There is no assigned CVE; the attack surface is permission- and behavior-based, not tied to a patchable software vulnerability. Relevant CWEs: CWE-693 (Protection Mechanism Failure), CWE-267 (Privilege Defined With Unsafe Actions), CWE-356 (Product UI Does Not Warn User of Unsafe Actions). MITRE ATT&CK techniques include T1438 (Alternate Network Mediums), T1626 (Abuse Elevation Control Mechanism), T1412 (Capture SMS Messages), T1582 (SMS Control), T1444 (Masquerade as Legitimate Application), T1418 (Software Discovery), T1516 (Input Injection), T1406 (Obfuscated Files or Information), T1417 (Input Capture), T1430 (Location Tracking), T1513 (Screen Capture), and T1411 (User Interface Spoofing). Documented capabilities:

Google Play Protect evasion, lock-screen PIN bypass, SMS OTP interception, clipboard hijacking, screen capture, and UI spoofing. The complete list of 217 targeted applications is enumerated in the Zimperium zLabs advisory; no independently verified C2 infrastructure details or public IOC list are currently circulating in threat intelligence feeds. No patch exists; detection and behavioral controls are the primary defensive layers.

Action Checklist

1. Step 1: Containment, Audit Android devices accessing corporate systems or customer-facing banking services. Enforce Mobile Device Management (MDM) policies that block sideloading and restrict installation to Google Play. Review and tighten which apps are permitted under your mobile application management policy. Reference: CIS Controls v8 2.3 (Address Unauthorized Software), v8 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory).
2. Step 2: Detection, Monitor Mobile Threat Defense (MTD) and MDM telemetry for behavioral indicators: apps requesting Accessibility Service permissions without clear business justification, apps requesting SMS read/send permissions, clipboard access events from non-whitelisted apps, and screen overlay activity. Cross-reference installed app package names against the 217 targeted applications enumerated in the Zimperium zLabs advisory (2026-06-16); request the full package name list directly from Zimperium or via your threat intelligence subscription if not yet published. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS Controls v8 8.2 (Collect Audit Logs), D3-LAM (Local Account Monitoring), D3-SFA (System File Analysis).
3. Step 3: Eradication, No software patch is available; remediation is behavioral. Remove any untrusted or unverified Android applications from managed devices. Revoke and rotate any banking credentials or cryptocurrency wallet access keys on devices showing anomalous permission grants. For compromised devices, perform factory reset before re-enrollment. Reference: D3-CRO (Credential Rotation), NIST AC-2 (Account Management).
4. Step 4: Recovery, After device remediation, re-enable account access only after credential rotation and MFA re-enrollment are confirmed. Monitor transaction logs for the targeted banking and cryptocurrency applications for anomalous activity for a minimum of 30 days post-remediation. Validate MDM enrollment and policy compliance before restoring access to corporate resources. Reference: NIST IR family controls, D3-MFA (Multi-factor Authentication), CIS Controls v8 6.3 (Require MFA for Externally-Exposed Applications).
5. Step 5: Post-Incident, Conduct a mobile security policy review. Evaluate whether your current MDM/MTD stack provides behavioral detection for Accessibility Service abuse, SMS interception, and overlay attacks. Update your mobile application allowlist. Establish a process for ingesting Zimperium zLabs and equivalent vendor threat intelligence on a recurring basis. Reference: CIS Controls v8 7.1 (Establish and Maintain a Vulnerability Management Process), NIST AC-6 (Least Privilege), D3-UAP (User Account Permissions).

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to legal, compliance, and executive leadership if any device confirmed or suspected to carry Rokarolla has accessed customer banking sessions, transmitted cryptocurrency wallet keys, or processed PII/PHI — triggering breach notification obligations under GLBA, PCI DSS Requirement 12.10, or applicable state data breach statutes — or if more than five managed devices show Accessibility Service anomalies simultaneously, indicating active campaign targeting rather than isolated infection.
Recovery Notes	Re-enrollment must be gated on confirmed factory reset and clean MDM compliance posture, not merely credential rotation — Rokarolla's 137-command RAT and Accessibility Service persistence mean a device that was not fully reset may re-compromise new credentials within minutes of re-enrollment. Monitor transaction logs for all 217 Rokarolla-targeted banking and cryptocurrency applications accessed from previously affected devices for a minimum of 30 days, with particular attention to small-value probe transactions (a common post-compromise account validation technique) and any wallet address changes. Validate that MFA re-enrollment shifted away from SMS-based OTP to authenticator-app or hardware token methods, since Rokarolla's SMS interception capability directly defeats SMS OTP as a recovery control.
Forensic Artifacts	MDM/MTD Accessibility Service grant logs: timestamps and package names of all apps granted BIND_ACCESSIBILITY_SERVICE on affected devices — Rokarolla requires this permission to perform screen reading, PIN capture, and UI interaction hijacking across the 217 targeted banking apps | Android SMS content provider dump (`adb shell content query --uri content://sms`): captures sent and received SMS records including intercepted OTPs that Rokarolla forwarded to C2, with timestamps to correlate against banking transaction events | Clipboard history from `adb shell dumpsys clipboard` or MDM telemetry: Rokarolla specifically hijacks clipboard content to steal cryptocurrency wallet addresses — clipboard events from non-whitelisted apps are a primary artifact of this attack vector | Outbound network connections and DNS query logs from the device during the suspected infection window: Rokarolla's 137-command RAT requires C2 communication — DNS queries and HTTPS connections to non-banking destinations from within banking app processes (visible via `adb shell dumpsys netstats` or VPN traffic capture) indicate active exfiltration | Installed APK list with install source and install timestamp (`adb shell pm list packages -f -i`): identifies whether Rokarolla was sideloaded (install source will not be com.android.vending / Google Play) and establishes the initial access timeline relative to observed anomalous permission grants

Per-Action IR Details

Step 1: Containment — Audit Android devices accessing corporate systems or customer-facing banking services. Enforce Mobile Device Management (MDM) policies that block sideloading and restrict installation to Google Play. Review and tighten which apps are permitted under your mobile application management policy. Reference: CIS 2.3 (Address Unauthorized Software), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), NIST AC-19 (Access Control For Mobile Devices)

Compensating: Without MDM, use ADB commands across enrolled devices: `adb shell pm list packages -f` to enumerate installed APKs and diff against an approved baseline. For sideload detection, query `adb shell settings get global install_non_market_apps` — a return value of '1' confirms unknown-sources is enabled. Document every device with the Rokarolla-targeted package list from the Zimperium zLabs advisory and flag any match for immediate isolation.

Evidence: Before restricting device access or pushing MDM policy changes that alter device state, capture: (1) full installed package list via `adb shell pm list packages -f` including install source metadata; (2) Accessibility Service grant list via `adb shell settings get secure enabled_accessibility_services`; (3) active SMS listener registrations via `adb shell dumpsys activity broadcasts` filtered for SMS_RECEIVED; (4) MDM enrollment logs showing last check-in time and compliance posture snapshot. These reflect live device state that MDM policy enforcement will overwrite.

Step 2: Detection — Monitor Mobile Threat Defense (MTD) and MDM telemetry for behavioral indicators: apps requesting Accessibility Service permissions without clear business justification, apps requesting SMS read/send permissions, clipboard access events from non-whitelisted apps, and screen overlay activity. Correlate against your application inventory for any of the 217 targeted apps (package list per Zimperium zLabs advisory). Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), D3-LAM (Local Account Monitoring), D3-SFA (System File Analysis).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without MTD, enable Android Debug Bridge logging and run `adb logcat -s AccessibilityService` to surface apps invoking Accessibility APIs in real time. Use `adb shell dumpsys clipboard` to audit clipboard access history. For SMS interception detection, query `adb shell content query --uri content://sms/inbox` and compare timestamps against outbound network connections captured via `adb shell dumpsys netstats`. Cross-reference installed package names against the Zimperium zLabs Rokarolla 217-app target list using a simple bash diff against `adb shell pm list packages`.

Evidence: This step is read-only telemetry collection and does not alter live state — no destructive precapture required before analysis. However, preserve the following as point-in-time snapshots before any subsequent containment or eradication action: (1) MTD/MDM alert logs including Accessibility Service grant events, overlay permission grants (SYSTEM_ALERT_WINDOW), and SMS READ/SEND permission grants with timestamps; (2) clipboard access audit trail from MDM telemetry or `adb shell dumpsys clipboard`; (3) outbound network connection log from the device (DNS queries and HTTPS destinations) correlated against Rokarolla C2 IOCs from the Zimperium advisory; (4) full `adb shell dumpsys package` output for any app matching the 217-app target list.

Step 3: Eradication — No software patch is available; remediation is behavioral. Remove any untrusted or unverified Android applications from managed devices. Revoke and rotate any banking credentials or cryptocurrency wallet access keys on devices showing anomalous permission grants. For compromised devices, perform factory reset before re-enrollment. Reference: D3-CRO (Credential Rotation), NIST AC-2 (Account Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without enterprise MDM remote-wipe capability, guide device owners through manual factory reset via Android Settings > General Management > Reset > Factory Data Reset. Before reset, use `adb backup -apk -all -f pre_reset_backup.ab` to preserve a forensic APK archive for later YARA analysis. For credential rotation without a PAM tool, generate a revocation checklist per affected banking app: revoke API tokens via each bank's developer portal, invalidate active sessions via the app's account security page, and issue new credentials out-of-band. For cryptocurrency wallets, transfer funds to a freshly generated wallet address on a clean device before revoking the compromised wallet keys.

Evidence: Rokarolla can intercept SMS OTPs and capture PINs via keylogging through Accessibility Service abuse — meaning credentials rotated over a still-compromised device are immediately re-captured. Before revoking or rotating any credential: (1) acquire a full memory dump if device is rooted or via MDM forensic agent to capture in-memory session tokens and clipboard contents (Rokarolla's 137-command RAT may hold active banking session state in memory); (2) export `adb shell dumpsys activity` to capture foreground app and active intent state; (3) capture

outbound network traffic via `adb shell tcpdump` or a VPN-based traffic capture to document any exfiltration in progress; (4) screenshot or export the Accessibility Service grant list and overlay permission list as the factory reset will destroy this evidence. Only after this capture is confirmed complete should credential revocation and device reset proceed.

Step 4: Recovery — After device remediation, re-enable account access only after credential rotation and MFA re-enrollment are confirmed. Monitor transaction logs for the targeted banking and cryptocurrency applications for anomalous activity for a minimum of 30 days post-remediation. Validate MDM enrollment and policy compliance before restoring access to corporate resources. Reference: NIST IR family controls, D3-MFA (Multi-factor Authentication), CIS 6.3 (Require MFA for Externally-Exposed Applications).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), NIST AC-12 (Session Termination), NIST AC-2 (Account Management)

Compensating: Without a SIEM to monitor transaction logs, establish a manual review cadence: export banking transaction logs weekly (via bank API or CSV download from the institution's admin portal) and diff against pre-incident baseline transaction patterns. For cryptocurrency wallets, set up free blockchain explorer alerts (e.g., Etherscan or Blockchair notification APIs) on the previously compromised wallet addresses to detect any residual unauthorized transfers. Verify MDM re-enrollment compliance using `adb shell dumpsys device_policy` and confirm `install_non_market_apps` returns '0' and Accessibility Service list contains only approved system entries.

Evidence: Recovery actions that restore access or re-enroll devices alter authentication state. Before restoring any account access: (1) confirm via MDM compliance report that the re-enrolled device has no packages matching the Rokarolla 217-app target list; (2) verify the Accessibility Service grant list is clean (`adb shell settings get secure enabled_accessibility_services` returns only system defaults); (3) confirm no residual Rokarolla C2 network destinations appear in DNS or firewall logs for the 48 hours post-factory-reset; (4) validate that the new MFA enrollment was performed on the freshly reset device, not re-linked to the same SMS number Rokarolla was intercepting — consider hardware token or authenticator-app MFA to prevent re-interception.

Step 5: Post-Incident — Conduct a mobile security policy review. Evaluate whether your current MDM/MTD stack provides behavioral detection for Accessibility Service abuse, SMS interception, and overlay attacks. Update your mobile application allowlist. Establish a process for ingesting Zimperium zLabs and equivalent vendor threat intelligence on a recurring basis. Reference: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), NIST AC-6 (Least Privilege), D3-UAP (User Account Permissions).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Without a commercial MTD platform, implement free behavioral detection using Android Enterprise work profile restrictions to block Accessibility Service grants for non-whitelisted apps by policy. Subscribe to Zimperium zLabs RSS or email alerts (free tier available) and the CISA Known Exploited Vulnerabilities catalog for Android campaign updates. Maintain a YARA rule set targeting Rokarolla APK characteristics (string patterns from the Zimperium advisory) and run scans against new APKs using `yara rokarolla_rules.yar ` before allowlisting. Document lessons learned in a one-page after-action report covering: detection gap (how long was the trojan active before detection), coverage gap (which of the 217 targeted apps are in active use by employees or customers), and policy gap (what MDM controls were absent that would have blocked Accessibility Service abuse).

Evidence: Post-incident review requires preserving the forensic record from all prior phases before systems are returned to full operational status. Retain: (1) pre-reset APK backups from compromised devices for YARA analysis and potential submission to VirusTotal or Zimperium for IOC enrichment; (2) MDM and MTD telemetry logs covering the full incident window with Accessibility Service grant events, overlay permission events, and SMS permission events timestamped for dwell-time calculation; (3) network logs documenting C2 communication patterns (destination IPs, domains, ports, and payload sizes) to feed into threat intelligence platform or share with Zimperium zLabs for campaign

tracking; (4) the before-and-after application inventory diff showing which of the 217 Rokarolla-targeted apps were present on affected devices.

Detection Guidance

Primary detection relies on behavioral telemetry from Mobile Threat Defense platforms and MDM solutions. Key behavioral indicators to hunt: (1) Android apps granted Accessibility Service permissions that are not whitelisted enterprise tools - Accessibility abuse is the primary mechanism for PIN capture, UI spoofing, and input injection (T1417, T1411, T1516); (2) apps holding SMS READ/SEND permissions that are not the designated corporate messaging application, flag for OTP interception (T1412, T1582); (3) clipboard access events from apps without clear business need (T1417); (4) screen capture or recording activity initiated outside known approved apps (T1513); (5) applications exhibiting masquerading behavior, icon or label matching legitimate banking apps but with differing package names (T1444); (6) obfuscated or packed APKs loaded outside the managed app store (T1406). In MDM/MTD dashboards, create alerts for any device granting Accessibility Service to a newly installed app. As the Zimperium zLabs advisory is published, cross-reference the 217 targeted app package names; request expedited access via your threat intelligence subscription if the list is not immediately available. No confirmed C2 IP/domain indicators are available in current source data; network-layer blocking cannot substitute for behavioral detection. Reference: D3-LAM, D3-SFA, NIST AU-2, NIST AU-6, CIS Controls v8 8.2.

Framework Mappings

MITRE-ATTACK

- **T1438**
- **T1626** — Abuse Elevation Control Mechanism
- **T1412**
- **T1582** — SMS Control
- **T1444**
- **T1418** — Software Discovery
- **T1516** — Input Injection
- **T1406** — Obfuscated Files or Information
- **T1417** — Input Capture
- **T1430** — Location Tracking
- **T1513** — Screen Capture
- **T1411**

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

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SI-4** — System Monitoring
- **IR-5** — Incident Monitoring

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1438		
T1626	Abuse Elevation Control Mechanism	Privilege-Escalation
T1412		
T1582	SMS Control	Impact
T1444		
T1418	Software Discovery	Discovery
T1516	Input Injection	Defense-Evasion
T1406	Obfuscated Files or Information	Defense-Evasion
T1417	Input Capture	Collection
T1430	Location Tracking	Collection
T1513	Screen Capture	Collection
T1411		

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/new-rokarolla-android-malware-ste...	T3
What information on your phone should banking apps have access to?	https://www.reddit.com/r/Banking/comments/1susjw2/what_information_...	T3

Source	URL	Tier
Security vulnerabilities are common in bank mobile apps	https://www.prosightfa.org/insights/security-vulnerabilities-are-co...	T3
Use Google Play Protect to help keep your apps safe & your data ...	https://support.google.com/googleplay/answer/2812853?hl=en	T3
What's New in Android Security and Privacy in 2026 - Google Blog	https://blog.google/security/whats-new-in-android-security-privacy-...	T1

Generated 2026-06-16 19:19 UTC by TJS Security Command Center