INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-17 08:04 UTC

Rokarolla Android Banking Trojan Targets 217 Financial Apps via Fake Chrome and TikTok Installers

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0498
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Android OS; 217 banking and cryptocurrency applications (specific app list unspecified in available source data); Google Chrome and TikTok impersonated as delivery lures
Published	2026-06-16T16:04:11
Discovery Source	Rss

Executive Summary

A newly identified Android banking trojan called Rokarolla is spreading through fake Google Chrome and TikTok app installers, targeting 217 banking and cryptocurrency applications. Once installed, it exploits Android's accessibility features to take near-complete control of a device, capturing credentials, intercepting communications, and bypassing built-in protections including Google Play Protect. Organizations with employees using Android devices for mobile banking, corporate finance apps, or cryptocurrency management face direct risk of credential theft and unauthorized financial transactions.

Technical Analysis

Rokarolla is an Android banking trojan distributed via trojanized APKs impersonating Google Chrome and TikTok, delivered through social-engineering-driven sideloading outside the Google Play Store. The malware abuses Android Accessibility Services (MITRE T1476) to achieve device takeover, executing overlay attacks (T1516) against 217 targeted banking and cryptocurrency applications. A 137-command C2 framework (per initial reporting) provides operators with capabilities including keylogging (T1417), SMS/call interception (T1412, T1582), screen capture (T1513), location tracking (T1430), and app data collection (T1418). The malware actively disables Google Play Protect (T1629.003) to suppress detection and uses obfuscated payloads (T1406). It masquerades as legitimate applications (T1444) and employs phishing overlays to harvest credentials (T1411). No CVE identifier is associated with this campaign. CWE mappings cited in source data include CWE-926 (Improper Export of Android Application Components), CWE-927 (Use of Implicit Intent for

Sensitive Communication), and CWE-276 (Incorrect Default Permissions); CWE-1021 (Improper Restriction of Rendered UI Layers) may more precisely describe the overlay mechanism, though confidence on exact CWE alignment is medium without access to the full technical report. No patch is available; mitigation is behavioral and configuration-based. Attribution is unestablished as of 2026-06-16. Primary source is BleepingComputer (T3); full technical details of the 217 targeted apps and complete command list are not independently verified from primary sources in this analysis.

Action Checklist

1. Step 1: Containment, Enforce Mobile Device Management (MDM) policy blocking sideloading of APKs from unknown sources on all Android devices with access to corporate banking, finance, or cryptocurrency applications. If MDM is not deployed, provide immediate guidance to employees to disable 'Install unknown apps' in Android settings.
2. Step 2: Detection, Review MDM and endpoint telemetry for Android devices showing Accessibility Service grants to non-system applications, unexpected APK installations named after Chrome or TikTok, and Google Play Protect disabled status. Query mobile threat defense (MTD) platforms for behavioral indicators: apps requesting Accessibility permissions, overlay draw permissions (SYSTEM_ALERT_WINDOW), and SMS read/send permissions in combination. No confirmed IOC hashes or C2 infrastructure are available from primary sources in this analysis.
3. Step 3: Eradication, On confirmed infected devices, perform a factory reset; do not attempt partial removal, as Accessibility Service abuse enables persistence and may resist standard uninstall. Remove any APKs installed from outside the Google Play Store. Re-enroll devices under MDM with enforced app allowlisting (CIS 2.3) before returning to service.
4. Step 4: Recovery, After re-enrollment, verify Google Play Protect is active and returning clean status. Require credential rotation (D3-CRO) for any banking, finance, or cryptocurrency accounts accessed from affected devices. Confirm MFA (D3-MFA) is enforced on all financial application accounts per CIS 6.3. Monitor account activity on targeted financial platforms for 30 days post-remediation.
5. Step 5: Post-Incident, Conduct a mobile security policy gap review against CIS 5.4 (restrict administrator privileges) and CIS 6.3 (require MFA for externally-exposed applications). Evaluate deployment of a Mobile Threat Defense solution if not present. Update security awareness training to specifically address APK sideloading risks and fake app installer lures. Review NIST AC-17 (Remote Access) and AC-19 (Access Control for Mobile Devices) compliance for mobile devices accessing corporate financial systems.

Detection Guidance

Detection focus areas: (1) MDM/UEM platforms, alert on any Android device with Google Play Protect disabled, Accessibility Service grants to non-system or non-whitelisted apps, or APK installs from sources outside Google Play. (2) Mobile Threat Defense (MTD) behavioral indicators, look for apps simultaneously holding Accessibility Service, SYSTEM_ALERT_WINDOW (overlay), READ_SMS, and RECEIVE_SMS permissions; this combination is a high-confidence indicator of banking trojan behavior. (3) Network monitoring, watch for unusual outbound connections from Android devices to uncategorized or newly registered domains, particularly over non-standard ports, which may indicate C2 activity from the 137-command framework. (4) Financial platform monitoring, alert on login attempts or transactions from Android devices flagged by MDM as non-compliant or

recently re-enrolled. No confirmed C2 IP addresses, domains, or APK file hashes are available from primary sources in this analysis; update detection rules as IOCs are released by the research community. D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) techniques apply for on-device forensic review.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Not available — no confirmed C2 URLs reported in primary sources as of 2026-06-16`	C2 infrastructure for Rokarolla's 137-command framework has not been publicly disclosed in available source material	LOW
HASH	`Not available — no confirmed APK file hashes reported in primary sources as of 2026-06-16`	Malicious APKs masquerade as Google Chrome and TikTok installers; specific hashes not independently verified	LOW

Framework Mappings

MITRE-ATTACK

- **T1444**
- **T1412**
- **T1516** — Input Injection
- **T1476**
- **T1417** — Input Capture
- **T1418** — Software Discovery
- **T1582** — SMS Control
- **T1406** — Obfuscated Files or Information
- **T1629.003** — Disable or Modify Tools
- **T1411**
- **T1513** — Screen Capture
- **T1430** — Location Tracking

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

NIST-800-53R5

- **SI-4** — System Monitoring

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1444		
T1412		
T1516	Input Injection	Defense-Evasion
T1476		
T1417	Input Capture	Collection
T1418	Software Discovery	Discovery
T1582	SMS Control	Impact
T1406	Obfuscated Files or Information	Defense-Evasion
T1629.003	Disable or Modify Tools	Defense-Evasion
T1411		
T1513	Screen Capture	Collection
T1430	Location Tracking	Collection

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-rokarolla-androi...	T3
Cybersecurity News - Western Illinois University	https://www.wiu.edu/cybersecuritycenter/cybernews.php	T1
May 2025 - Google Online Security Blog	https://security.googleblog.com/2025/05/	T3
Vulnerability in TikTok Android app could lead to one-click account ...	https://www.microsoft.com/en-us/security/blog/2022/08/31/vulnerabil...	T1
Google patches Android remote takeover bug - Risky Bulletin	https://news.risky.biz/risky-bulletin-google-patches-android-remote...	T3

Generated 2026-06-17 08:04 UTC by TJS Security Command Center