INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 19:18 UTC

Rokarolla Android Trojan Combines Banking Fraud with Full Device Takeover via Fake TikTok and Chrome Apps

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0485
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Android devices; trojanized fake TikTok and Chrome applications (sideloaded)
Published	2026-06-16T13:32:32
Discovery Source	Rss

Executive Summary

A newly identified Android trojan called Rokarolla is spreading through fake TikTok and Chrome applications distributed outside official app stores. The malware steals banking credentials and grants attackers full remote control over infected devices. Organizations permitting personal devices to access corporate systems face meaningful risk of credential theft and lateral movement into enterprise environments.

Technical Analysis

Rokarolla is an Android mobile implant delivered via trojanized APKs mimicking TikTok and Google Chrome, likely distributed through third-party stores or phishing-delivered links. The malware abuses Android Accessibility Services to perform overlay attacks and keylogging (CWE-506: Embedded Malicious Code; CWE-267: Improper Privilege Management; CWE-272: Least Privilege Violation). Confirmed MITRE ATT&CK mobile techniques include: T1444 (Masquerade as Legitimate Application), T1417 (Input Capture), T1429 (Capture Audio), T1421 (System Network Connections Discovery), T1430 (Location Tracking), T1418 (Software Discovery), T1404 (Exploit OS Vulnerability), T1476 (Deliver Malicious App via Other Means), and T1631 (Accessibility Service Abuse). Capabilities span banking credential harvesting, persistent surveillance, and remote device takeover. No CVE has been assigned; no NVD or CISA KEV entry exists for this campaign. Source confidence is medium, single RSS-sourced item, secondary corroboration not confirmed at analysis time. The Dark Reading source URL requires human validation before citing as primary reporting.

Action Checklist

1. Step 1: Containment, Enforce MDM policy blocking sideloaded APKs on all BYOD and corporate-managed Android devices immediately. Restrict installation sources to Google Play only. Identify any enrolled devices that have installed applications named 'TikTok' or 'Chrome' from sources other than official stores and quarantine those devices from corporate network access pending inspection. Reference: NIST AC-19 (Access Control for Mobile Devices), CIS 2.3 (Address Unauthorized Software).
2. Step 2: Detection, Query MDM telemetry for Android devices with applications installed outside official app store channels. Look for accessibility service grants to applications that are not system-approved. Review corporate SSO, VPN, and email gateway logs for authentication events originating from Android device user-agents, cross-referenced against known-clean device inventory (NIST AU-6, CIS 8.2). Behavioral indicators include: unexpected accessibility service activations, screen overlay permissions granted to TikTok or Chrome lookalike package names, anomalous outbound network connections from mobile device IPs to unknown C2 infrastructure.
3. Step 3: Eradication, Factory reset any confirmed-infected devices before re-enrolling into MDM. Do not attempt partial remediation; persistent implants with device administrator or accessibility access survive standard uninstall attempts. Rotate all corporate credentials that may have been entered on infected devices, including VPN credentials, SSO tokens, email passwords, and any banking or financial application credentials (NIST AC-2, D3-CRO: Credential Rotation). Revoke and reissue active session tokens for affected accounts.
4. Step 4: Recovery, Verify re-enrolled devices pass MDM compliance checks before restoring corporate access. Enable continuous monitoring for accessibility service abuse and unknown package installation events going forward. Review authentication logs for the 30 days preceding detection for signs of account compromise using credentials that may have been harvested (NIST AU-11, AU-6). Monitor for lateral movement indicators from IP ranges associated with affected devices.
5. Step 5: Post-Incident, Audit BYOD policy against NIST AC-19 and CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.4 (Require MFA for Remote Network Access). Require MFA for all corporate application access from mobile devices to limit credential-theft impact. Implement application allowlisting on managed Android devices (CIS 2.1, CIS 2.3). Conduct targeted awareness training on risks of sideloading applications. Document gaps identified during this incident and update mobile device security policy accordingly.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and the CISO immediately if any evidence confirms that Rokarolla successfully harvested corporate SSO, VPN, or email credentials and those credentials were used to authenticate to enterprise systems — this constitutes a breach of corporate infrastructure with potential regulatory notification obligations under applicable data protection law (e.g., GDPR, CCPA, state breach notification statutes) if employee or customer PII was accessible via the compromised accounts.

Recovery Notes	Re-enrollment into MDM must require passing Google Play Protect device attestation and an explicit MDM compliance check confirming Unknown Sources is disabled before any corporate network access is restored — do not rely on the device owner's attestation alone. Conduct a 30-day elevated monitoring period post-recovery, specifically watching for authentication anomalies from the affected user accounts (new MFA device enrollments, password resets, access from unfamiliar geographies or IP ranges) that would indicate Rokarolla's credential harvest is being operationalized by the threat actor from external infrastructure. If the organization permits banking or financial application access on BYOD devices, notify affected users to contact their financial institutions directly, as Rokarolla's primary capability is banking credential theft that extends beyond the corporate environment.
Forensic Artifacts	Android APK signing certificate fingerprint of the fake TikTok or Chrome package — extracted via 'apksigner verify --print-certs ' or 'adb shell dumpsys package | grep -A5 signatures' — will not match Google LLC or ByteDance certificate fingerprints from legitimate Play Store builds, providing definitive confirmation of trojanized application | Android accessibility service binding records — captured via 'adb shell dumpsys accessibility' and 'adb shell settings get secure enabled_accessibility_services' — Rokarolla's overlay and remote control capabilities require BIND_ACCESSIBILITY_SERVICE permission which leaves a persistent record of the malicious package name bound as an accessibility provider | Device administrator enrollment records — captured via 'adb shell dumpsys devicepolicy' before factory reset — Rokarolla requests Device Admin privileges to block removal; the presence of the fake TikTok or Chrome package name in the device admin list is a high-confidence indicator of active Rokarolla infection | Outbound network connection logs from MDM, VPN gateway, or on-device 'adb shell netstat' / 'adb shell ss -tunp' output captured before device isolation — Rokarolla's RAT component maintains persistent C2 sessions; unique destination IPs, ports, and TLS SNI values in these captures constitute actionable C2 infrastructure indicators for threat intelligence sharing and blocklisting | Corporate SSO, VPN, and email gateway authentication logs for the 30-day window preceding detection, filtered on Android user-agent strings from enrolled device IDs — Rokarolla harvests credentials entered on the device and may have enabled silent authentication to corporate services; anomalous successful authentications from the infected device during off-hours or from unexpected geographic locations corroborate active credential abuse

Per-Action IR Details

Step 1: Containment — Enforce MDM policy blocking sideloaded APKs on all BYOD and corporate-managed Android devices immediately. Restrict installation sources to Google Play only. Identify any enrolled devices that have installed applications named 'TikTok' or 'Chrome' from sources other than official stores and quarantine those devices from corporate network access pending inspection. Reference: NIST AC-19 (Access Control for Mobile Devices), CIS 2.3 (Address Unauthorized Software).

NIST Phase: Containment

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

Controls: NIST AC-19 (Access Control for Mobile Devices), NIST AC-3 (Access Enforcement), CIS 2.3 (Address Unauthorized Software)

Compensating: For teams without enterprise MDM: use Android Debug Bridge (ADB) to enumerate installed packages on enrolled devices — run 'adb shell pm list packages -f -i' and grep for package names that mimic com.zhiliaoapp.musically (TikTok) or com.android.chrome but originate from non-Play sources. Cross-reference against known-good Play Store APK signing certificate hashes using apksigner or apktool. Enforce a manual attestation process requiring device owners to confirm installation sources before VPN credentials are issued.

Evidence: Before quarantining devices, capture: (1) MDM device detail reports showing installed application package names, version codes, and installation sources for any 'TikTok' or 'Chrome' named apps; (2) ADB output of 'adb shell

dumpsys package ' to extract signing certificate, declared permissions, and installation timestamp; (3) Network flow logs from the corporate perimeter/VPN concentrator showing outbound connections from the device's IP prior to isolation, to identify C2 beaconing patterns unique to Rokarolla before the device is quarantined and live network state is destroyed.

Step 2: Detection — Query MDM telemetry for Android devices with applications installed outside official app store channels. Look for accessibility service grants to applications that are not system-approved. Review corporate SSO, VPN, and email gateway logs for authentication events originating from Android device user-agents, cross-referenced against known-clean device inventory (NIST AU-6, CIS 8.2). Behavioral indicators include: unexpected accessibility service activations, screen overlay permissions granted to TikTok or Chrome lookalike package names, anomalous outbound network connections from mobile device IPs to unknown C2 infrastructure.

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 a SIEM: (1) Pull Android device logs via ADB using 'adb shell dumpsys accessibility' to list all active accessibility services — any entry referencing a TikTok or Chrome lookalike package is a high-confidence indicator of Rokarolla's overlay/RAT component. (2) Run 'adb shell settings get secure enabled_accessibility_services' to enumerate granted accessibility service bindings. (3) Export VPN and SSO authentication logs to CSV and run a manual grep or PowerShell 'Select-String' against known-clean device IDs to surface authentication events from unrecognized or unenrolled Android user-agents. (4) Use Wireshark or tcpdump on the VPN gateway interface to capture and inspect outbound traffic from flagged mobile IPs for DNS lookups or TLS SNI values associated with unknown infrastructure.

Evidence: This is a detection step; however, capture and preserve before any device interaction: (1) MDM telemetry snapshot of all enrolled Android devices including app inventory, permission grants, and accessibility service states at time of detection — this is volatile if the device is remotely wiped or reset; (2) VPN/SSO authentication logs for the 30-day window preceding detection, specifically filtering on Android user-agent strings that do not match enrolled device IDs; (3) 'adb shell dumpsys activity permissions' output showing which packages hold BIND_ACCESSIBILITY_SERVICE and SYSTEM_ALERT_WINDOW (screen overlay) permissions, as Rokarolla relies on both for credential harvesting and UI manipulation; (4) Network connection state from the device via 'adb shell netstat' or 'adb shell ss -tunp' before any isolation action to capture live C2 connection endpoints.

Step 3: Eradication — Factory reset any confirmed-infected devices before re-enrolling into MDM. Do not attempt partial remediation; persistent implants with device administrator or accessibility access survive standard uninstall attempts. Rotate all corporate credentials that may have been entered on infected devices, including VPN credentials, SSO tokens, email passwords, and any banking or financial application credentials (NIST AC-2, D3-CRO: Credential Rotation). Revoke and reissue active session tokens for affected accounts.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-12 (Session Termination)

Compensating: For teams without automated credential rotation tooling: (1) Manually invalidate all active SSO sessions via the identity provider admin console (e.g., force sign-out all sessions in Azure AD, Okta, or Google Workspace for affected users); (2) Revoke VPN certificates or pre-shared keys associated with affected device IDs; (3) Use 'adb shell wipe data' or MDM remote wipe command to perform factory reset — do NOT attempt to uninstall Rokarolla manually, as it requests device administrator privileges during installation that block standard removal; (4) Document all credentials entered on each affected device during the confirmed infection window by interviewing the device owner, then reset each credential individually with forced re-authentication on a clean device.

Evidence: CRITICAL — volatile evidence must be captured BEFORE factory reset, credential rotation, or session revocation: (1) Full logical backup of the device via ADB ('adb backup -apk -shared -all -f device_backup.ab') to

preserve installed APK artifacts, app data directories, and shared storage for forensic analysis; (2) 'adb shell dumpsys devicepolicy' to document all active Device Administrator bindings — Rokarolla's persistence mechanism specifically abuses Android Device Admin API to prevent removal; (3) 'adb shell dumpsys package ' to capture full package metadata including install timestamp, signing certificate fingerprint, declared permissions, and granted runtime permissions; (4) Network capture (pcap) from the device or upstream gateway of all active connections from the device IP before isolation — Rokarolla's RAT component maintains persistent C2 sessions that will reveal C2 infrastructure when captured live; (5) Screenshot or screen recording of active accessibility services, overlay permissions, and device admin list via 'adb shell screencap' before wipe destroys this state.

Step 4: Recovery — Verify re-enrolled devices pass MDM compliance checks before restoring corporate access. Enable continuous monitoring for accessibility service abuse and unknown package installation events going forward. Review authentication logs for the 30 days preceding detection for signs of account compromise using credentials that may have been harvested (NIST AU-11, AU-6). Monitor for lateral movement indicators from IP ranges associated with affected devices.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-11 (Audit Record Retention), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AC-17 (Remote Access), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Without enterprise SIEM for lateral movement monitoring: (1) Run a PowerShell script against Active Directory or the identity provider to identify any new MFA enrollment, password reset, or privileged role assignment events for affected accounts during and after the infection window — 'Get-AzureADAuditSignInLogs' or equivalent; (2) Query VPN concentrator logs manually for authentication events from IP ranges that were associated with the infected devices post-isolation to detect credential reuse from attacker-controlled infrastructure; (3) Use osquery on corporate endpoints to detect any new login sessions or remote authentication events associated with the compromised usernames: 'SELECT * FROM last WHERE username = ""'; (4) Enforce a re-enrollment MDM compliance policy that requires Google Play Protect attestation and prohibits 'Unknown Sources' installation before network access is restored.

Evidence: Before restoring corporate access to re-enrolled devices: (1) Confirm factory reset completion by verifying the device serial number against MDM re-enrollment records — a device that was not fully wiped may retain Rokarolla's Device Admin binding in a secondary user profile or work profile partition; (2) Retain the 30-day authentication log window from SSO, VPN, and email gateway for post-recovery threat hunting — Rokarolla's credential harvesting of banking and SSO credentials may enable delayed account takeover attempts from attacker infrastructure after the device is remediated; (3) Document the IP addresses associated with affected devices during the infection window and add them to a watchlist for correlation against future authentication attempts, as attackers may reuse harvested credentials from external IPs not associated with the original device.

Step 5: Post-Incident — Audit BYOD policy against NIST AC-19 and CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.4 (Require MFA for Remote Network Access). Require MFA for all corporate application access from mobile devices to limit credential-theft impact. Implement application allowlisting on managed Android devices (CIS 2.1, CIS 2.3). Conduct targeted awareness training on risks of sideloading applications. Document gaps identified during this incident and update mobile device security policy accordingly.

NIST Phase: Post Incident

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

Controls: NIST AC-19 (Access Control For Mobile Devices), NIST AC-7 (Unsuccessful Logon Attempts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without a formal GRC platform: (1) Conduct a structured lessons-learned meeting within 5 business days of containment; document the gap between existing BYOD policy and the actual MDM enforcement state that allowed Rokarolla-infected devices to reach corporate SSO and VPN; (2) Produce a one-page sideloading

risk brief specifically referencing the Rokarolla campaign's use of fake TikTok and Chrome APKs as the delivery vector — this is more effective awareness training than generic phishing content; (3) Manually audit the MDM enrollment database to confirm that 'Unknown Sources' installation is blocked at the policy layer, not just recommended in user-facing documentation; (4) Add Rokarolla-associated package name patterns and signing certificate hashes (obtained from forensic capture in Step 3) to the MDM application blocklist as a detection-in-depth measure for future reinfection attempts.

Evidence: No live volatile evidence is at risk in this phase. Preserve for post-incident record: (1) All forensic artifacts collected during Steps 1–4 (APK backups, accessibility service dumps, network captures, authentication logs) — retain per AU-11 requirements for the organization-defined retention period; (2) The MDM compliance audit report from Step 4 re-enrollment verification, documenting which devices failed compliance checks and why; (3) A complete record of all credentials rotated and sessions revoked in Step 3, with timestamps, for regulatory or HR purposes if the incident involves PII or financial data exposure.

Detection Guidance

Primary detection surface is MDM and endpoint telemetry. Query for: (1) Android applications with package names resembling 'com.tiktok', 'com.google.chrome', or close variants that were not installed from Google Play Store, compare package signing certificates against known-good hashes. (2) Accessibility service grants to any non-system, non-approved application, flag immediately for review. (3) Screen overlay permission grants on devices accessing corporate resources. On the network side, review DNS and proxy logs for connections to unknown or newly registered domains originating from mobile device segments. VPN and zero-trust access logs should be reviewed for authentication anomalies from Android user-agents. SIEM correlation rule: alert on [MDM event: accessibility_service_enabled] AND [MDM event: package_source = unknown] on any device with active corporate session. No confirmed IOCs (hashes, C2 domains, IPs) are available in the sourced reporting at this time, monitor threat intelligence feeds for Rokarolla-specific indicators as reporting matures. Source confidence for this campaign remains medium; adjust detection priority as corroboration emerges.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`No confirmed IOCs available at time of analysis`	No C2 domains, IP addresses, or file hashes for Rokarolla have been confirmed in sourced reporting. Monitor threat intelligence feeds for updates as campaign reporting matures.	LOW

Framework Mappings

MITRE-ATTACK

- **T1429** — Audio Capture
- **T1421** — System Network Connections Discovery
- **T1476**
- **T1418** — Software Discovery
- **T1631** — Process Injection

- **T1417** — Input Capture
- **T1430** — Location Tracking
- **T1404** — Exploitation for Privilege Escalation
- **T1444**

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SR-2** — Supply Chain Risk Management Plan

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1429	Audio Capture	Collection
T1421	System Network Connections Discovery	Discovery
T1476		
T1418	Software Discovery	Discovery
T1631	Process Injection	Defense-Evasion
T1417	Input Capture	Collection
T1430	Location Tracking	Collection

Technique ID	Technique Name	Tactic
T1404	Exploitation for Privilege Escalation	Privilege-Escalation
T1444		

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/endpoint-security/rokarolla-android-trojan	T3
Oversecured detects dangerous vulnerabilities in the TikTok Android ...	https://oversecured.com/blog/oversecured-detects-dangerous-vulnerab...	T3
Aura on Instagram: "A newly discovered Android malware campaign ...	https://www.instagram.com/reel/DY-AzmJFbgm/	T3
TikTok was found to be bypassing Android's built-in protections and ...	https://www.reddit.com/r/privacy/comments/i826fz/tiktok_was_found_t...	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

Generated 2026-06-16 19:18 UTC by TJS Security Command Center