INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-11 05:54 UTC

TrickMo.C Drops DNS for TON Blockchain: Android Banker Gains Covert C2 and Network Tunneling Capabilities

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0302
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Android devices; banking and cryptocurrency wallet applications; users in France, Italy, and Austria; delivery via TikTok and streaming app impersonation
Published	2026-05-11T05:03:02
Discovery Source	Rss

Executive Summary

A new variant of the TrickMo Android banking trojan has replaced its command-and-control infrastructure with the TON blockchain, making it far more difficult for law enforcement and ISPs to disrupt via traditional DNS sinkholing, domain seizure, or infrastructure takedowns. The malware targets banking and cryptocurrency wallet users in France, Italy, and Austria through fake TikTok and streaming app downloads, stealing login credentials and one-time passcodes. Organizations with mobile-banking-dependent employees or customers in those regions face elevated credential theft risk with no straightforward network-level countermeasure available.

Technical Analysis

TrickMo.C is a new variant of the TrickMo Android banking trojan, tracked by ThreatFabric, that has migrated its C2 channel from traditional DNS-based infrastructure to The Open Network (TON) blockchain overlay. This eliminates the effectiveness of DNS sinkholing, domain seizure, and law enforcement-coordinated takedowns. Core capabilities retained from earlier variants include credential harvesting from banking and crypto wallet applications, OTP interception, and screen capture. New capabilities added in this variant include SSH tunneling, SOCKS5 proxy support, and expanded network reconnaissance commands. Distribution occurs via trojanized APKs impersonating TikTok and streaming applications, sideloaded outside official app stores. Relevant CWEs: CWE-923 (improper restriction of communication channel to intended endpoints), CWE-494 (download of code without integrity check), CWE-295 (improper certificate validation), CWE-287 (improper

authentication). MITRE ATT&CK coverage includes T1481 (web service C2), T1090.003 (multi-hop proxy), T1437.001 (web protocols for C2), T1417 (input capture), T1412 (capture SMS messages), T1660 (phishing via trojanized apps), T1513 (screen capture), T1516 (input injection), T1624 (broadcast receivers for event-triggered execution), and T1571 (non-standard port usage), among others. No CVE identifier is associated with this campaign. No vendor patch applies; the threat vector is sideloaded APKs, not a patched application vulnerability.

Action Checklist

1. Containment: Block installation of APKs from unknown sources on all managed Android devices via MDM policy. If your MDM supports application allowlisting, evaluate and enforce immediately on devices accessing corporate banking or financial applications. Restrict sideloading through Android Enterprise or equivalent policy.
2. Detection: Query MDM and endpoint logs for APKs installed outside Google Play with package names or signing certificates mismatching TikTok's official distribution. Review network logs for connections to TON overlay network endpoints or unusual SOCKS5 and SSH tunnel activity originating from mobile devices. Monitor for unexpected OTP delivery events or authentication anomalies on banking and financial platforms for affected regions (France, Italy, Austria).
3. Eradication: Remove any identified trojanized APKs through MDM remote wipe or selective app removal. Force re-enrollment of devices where sideloading occurred. Revoke and rotate credentials for any accounts accessed from a suspected compromised device, prioritizing banking and crypto wallet credentials.
4. Recovery: Validate that MDM policies blocking unknown-source APK installs are enforced and reporting clean. Monitor affected user accounts for anomalous login activity for a minimum of 30 days post-remediation. Confirm OTP delivery channels are not being intercepted by reviewing authentication logs for unusual OTP consumption patterns.
5. Post-Incident: This variant exposes a gap in mobile device management policy enforcement and user awareness around sideloaded applications. Conduct a review of mobile security policy coverage for personally-owned (BYOD) devices accessing corporate financial systems. Evaluate whether TON blockchain traffic should be added to network monitoring signatures as an anomaly indicator, given its emerging use as a C2 transport.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if any evidence of successful OTP interception or unauthorized banking/crypto transaction is confirmed for users in France, Italy, or Austria, as these jurisdictions trigger GDPR breach notification obligations (72-hour window) and may activate PSD2 fraud reporting requirements for financial institutions.

Recovery Notes	Post-containment, enforce hardware-backed Android attestation (SafetyNet/Play Integrity API) as a condition of banking application access, preventing re-enrollment of rooted or compromised devices that could re-establish TrickMo's TON C2 channel. Monitor all previously affected user accounts across banking and crypto platforms for a minimum of 30 days, specifically watching for low-and-slow credential reuse from credentials harvested before rotation. Given TrickMo.C's use of the TON blockchain as a resilient C2 — a mechanism immune to DNS sinkholing — treat any resumption of TON overlay network traffic from mobile device ranges as an active re-infection indicator requiring immediate device quarantine.
Forensic Artifacts	Trojanized APK file recovered from device storage or MDM inventory — extract SHA-256 hash and compare against TrickMo.C samples indexed on MalwareBazaar; verify APK signing certificate against TikTok's official certificate (available from Play Store APK via apksigner) to confirm trojanization | Android package installer logs at '/data/system/packages.xml' and '/data/system/packages-backup.xml' — these persist install source metadata and timestamps for all installed APKs, including sideloaded ones, and establish the infection timeline even after app removal | Network flow records (NetFlow/IPFIX or firewall session logs) filtered to SOCKS5 (TCP/1080) and SSH (TCP/22) sessions originating from mobile device IP ranges — TrickMo.C's tunneling activity over these protocols is the primary network-layer indicator of active C2 communication via the TON overlay | Authentication platform OTP consumption logs correlated against session device fingerprint — specifically, records where an OTP was delivered to a registered device but consumed by a different IP, user agent, or device ID, indicating on-device interception by TrickMo.C's overlay attack capability | DNS query logs from the organization's recursive resolver or mobile network showing resolution attempts for TON DHT bootstrap nodes or .ton TLD addresses — these queries appear before TrickMo.C establishes its blockchain-based C2 channel and represent the earliest network-visible indicator of infection

Per-Action IR Details

Containment — Block installation of APKs from unknown sources on all managed Android devices via MDM policy. If your MDM supports application allowlisting, enforce it immediately for devices accessing corporate banking or financial applications. Restrict sideloading through Android Enterprise or equivalent policy.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For teams without enterprise MDM: use Android Enterprise Work Profile (free via Google Workspace free tier) to enforce 'Install from Unknown Sources = disabled' at the profile level. Manually audit via ADB: run 'adb shell settings get secure install_non_market_apps' on each enrolled device — a return value of '1' indicates sideloading is enabled and the device is at risk. For BYOD fleets with no MDM, distribute a conditional access policy requiring devices to pass Google Play Protect attestation before connecting to corporate banking portals, enforceable via free Entra ID Conditional Access (P1 license) or equivalent.

Evidence: Before enforcing the MDM block, capture: (1) a full inventory of installed packages on suspect devices via 'adb shell pm list packages -f -i' to identify non-Play-Store origins; (2) APK installer metadata from Android Settings > Apps > [app] > App Info > 'Install Source' to confirm sideload provenance; (3) network connection state at time of containment via 'adb shell netstat -antp' to document any live SOCKS5 or SSH tunnels active from the device before isolation; (4) device enrollment logs from your MDM showing last policy sync timestamp and compliance state — critical for establishing the window of exposure.

Detection — Query MDM and endpoint logs for APKs installed outside Google Play with package names or signing certificates mismatching TikTok's official distribution. Review network logs for connections to TON

overlay network endpoints or unusual SOCKS5 and SSH tunnel activity originating from mobile devices. Monitor for unexpected OTP delivery events or authentication anomalies on banking and financial platforms for affected regions (France, Italy, Austria).

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without SIEM: (1) TikTok's official Play Store signing certificate fingerprint (SHA-256) is publicly documented — extract the certificate from the installed APK using 'apksigner verify --print-certs suspicious.apk' and compare against TikTok's known cert; any mismatch confirms a trojanized package. (2) For TON overlay detection, write a Suricata or Zeek rule matching DNS queries or TLS SNI to known TON bootstrap nodes (publicly listed in the TON documentation); free Zeek on a network tap will surface this without a SIEM. (3) For OTP interception detection, query your SMS gateway or authentication provider's API logs for OTP delivery records where the registered device identifier changed within 24 hours of delivery — this catches SIM-swap-adjacent and on-device OTP theft. MITRE ATT&CK T1437 (Application Layer Protocol) and T1636.003 (Protected User Data: SMS Messages) are the relevant technique references for signature development.

Evidence: Capture before proceeding to eradication: (1) full MDM application inventory export filtered to 'install source != com.android.vending (Google Play)' for all devices with banking app access in France, Italy, and Austria geos; (2) firewall or proxy logs filtered to TCP/UDP sessions on ports 1080 (SOCKS5) and 22 (SSH) originating from mobile device IP ranges — TrickMo.C uses these for tunneling exfiltrated credentials; (3) authentication platform logs (your banking SSO, mobile banking backend, or crypto wallet OAuth provider) showing OTP consumption events correlated against device fingerprint — look for OTPs consumed by a different device or IP than the one that initiated the session; (4) DNS query logs from your recursive resolver or mobile carrier showing lookups for TON DHT bootstrap addresses or .ton TLD resolution attempts.

Eradication — Remove any identified trojanized APKs through MDM remote wipe or selective app removal. Force re-enrollment of devices where sideloading occurred. Revoke and rotate credentials for any accounts accessed from a suspected compromised device, prioritizing banking and crypto wallet credentials.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without enterprise MDM remote-wipe capability: (1) use ADB selective uninstall 'adb shell pm uninstall -k --user 0 ' to remove the trojanized TikTok/streaming APK without full device wipe, preserving forensic data on the device if needed; (2) for credential rotation on banking and crypto platforms without an IAM system, generate a priority list from your MDM application inventory of all accounts authenticated from compromised devices within the past 30 days and push mandatory password resets via each platform's admin console — crypto wallet seed phrases must be treated as fully compromised and wallet migration initiated; (3) disable TOTP/SMS OTP seeds for affected accounts and reissue — TrickMo.C's OTP interception means existing TOTP or SMS second factors on compromised devices are untrusted.

Evidence: Before issuing remote wipe or app removal commands: (1) pull a full application data backup via 'adb backup -apk -obb -all -f device_backup__.adb' while device is still accessible — this preserves the malicious APK, its data directory, and any staged exfiltration files for forensic analysis; (2) extract shared preferences and SQLite databases from the TrickMo APK's data directory (typically '/data/data//') if rooted access or an MDM with deep inspection is available — these may contain harvested credentials, intercepted OTPs, or C2 configuration referencing TON bootstrap endpoints; (3) document the full list of accounts authenticated from the device across all banking and crypto platforms before revoking — required for downstream breach notification scoping.

Recovery — Validate that MDM policies blocking unknown-source APK installs are enforced and reporting clean. Monitor affected user accounts for anomalous login activity for a minimum of 30 days post-remediation. Confirm OTP delivery channels are not being intercepted by reviewing authentication logs for unusual OTP consumption patterns.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a dedicated monitoring platform: (1) schedule a daily cron job or PowerShell task to export MDM compliance reports and diff against a known-good baseline — any device reappearing as non-compliant within 30 days indicates re-infection or policy bypass; (2) configure your banking platform's admin alert (most major online banking admin consoles offer free anomaly email alerts) to flag logins from new device fingerprints, new geolocations, or out-of-band OTP consumption for the affected French, Italian, and Austrian user accounts; (3) for crypto wallet accounts, enable on-chain transaction monitoring using free tools such as Etherscan alerts or equivalent per-chain notification services to catch unauthorized outbound transfers that may result from pre-rotation credential theft not yet acted upon by the threat actor.

Evidence: During recovery validation, retain and review: (1) MDM compliance audit trail showing policy enforcement timestamps and device re-enrollment events — gaps between wipe and re-enrollment are windows where a device could reconnect to TON C2; (2) authentication platform logs covering the full 30-day monitoring window, specifically filtering on accounts flagged during eradication for any session initiated without the newly issued MFA credential — this detects credential reuse from pre-rotation theft; (3) network flow data for mobile device subnets showing any resumption of SOCKS5/SSH tunnel activity, which would indicate re-infection or a previously undetected device.

Post-Incident — This variant exposes a gap in mobile device management policy enforcement and user awareness around sideloaded applications. Conduct a review of mobile security policy coverage for personally-owned (BYOD) devices accessing corporate financial systems. Evaluate whether TON blockchain traffic should be added to network monitoring signatures as an anomaly indicator, given its emerging use as a C2 transport.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: For teams without a dedicated threat intelligence platform: (1) subscribe to free OSINT feeds tracking TrickMo IOCs — abuse.ch ThreatFox and MalwareBazaar both index TrickMo samples and C2 indicators at no cost; create a weekly review task to check for new TrickMo.C package hashes or TON bootstrap node updates; (2) write a free Suricata or Snort rule matching the TON DHT handshake pattern (documented in open TON protocol specs) and deploy on your network perimeter — this converts the post-incident finding into an active detection; (3) develop a 15-minute user awareness module specifically addressing fake TikTok and streaming app sideloading, targeting employees in France, Italy, and Austria who use mobile banking — this directly addresses the TrickMo.C delivery vector rather than generic phishing awareness.

Evidence: For the lessons-learned record and to support BYOD policy revision: (1) compile the full timeline of device non-compliance events from MDM logs showing when sideloading policies were absent or unenforced — this establishes the policy gap duration for risk documentation; (2) retain all IOC artifacts collected during detection and eradication (trojanized APK hashes, TON endpoint addresses, anomalous authentication records) and contribute to a sector ISAC (FS-ISAC for financial sector, given France/Italy/Austria banking targeting) to support broader community defense; (3) document whether any BYOD devices were involved that fell outside MDM policy scope — the count and access level of unmanaged BYOD devices touching banking systems is the primary metric for scoping the residual risk

and justifying a formal BYOD mobile security policy revision.

Detection Guidance

Detection options are limited at the network layer due to TON blockchain C2; focus on endpoint and behavioral signals. On managed Android devices, use MDM logs to identify APKs installed from sources outside Google Play, flag any package claiming to be TikTok or a streaming service that was not installed via the official store. At the network layer, look for SOCKS5 proxy traffic or SSH tunnel establishment originating from mobile devices, particularly to non-corporate endpoints. Monitor authentication logs on banking portals and financial platforms for users in France, Italy, and Austria for credential stuffing patterns or OTP exhaustion. MITRE T1481 (web service C2 via TON), T1090.003 (multi-hop proxy), T1412 (SMS capture), and T1417 (input capture) are the highest-signal techniques to hunt against. Behavioral indicators include: unexpected accessibility service grants on Android devices, apps requesting SMS read permissions that are not messaging applications, and anomalous screen capture activity. No public IOC list (hashes, IPs, domains) has been published at time of writing; monitor ThreatFabric's threat research directly for updated indicators as they become available.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`TON blockchain overlay (no specific domain)`	TrickMo.C routes C2 traffic through the TON blockchain network; no seized or sinkholeable domain exists. Check ThreatFabric research for updated IOCs.	LOW
HASH	`Not publicly confirmed in available sources`	No APK hashes confirmed in tier-3 source reporting at time of writing. Retrieve from ThreatFabric's published TrickMo.C analysis.	LOW

Framework Mappings

MITRE-ATTACK

- **T1646** — Exfiltration Over C2 Channel
- **T1513** — Screen Capture
- **T1516** — Input Injection
- **T1632.001** — Code Signing Policy Modification
- **T1521** — Encrypted Channel
- **T1219** — Remote Access Tools
- **T1409** — Stored Application Data
- **T1571** — Non-Standard Port
- **T1417** — Input Capture
- **T1660** — Phishing

- **T1509** — Non-Standard Port
- **T1437** — Application Layer Protocol
- **T1437.001** — Web Protocols
- **T1481** — Web Service
- **T1638** — Adversary-in-the-Middle
- **T1412**
- **T1090.003** — Multi-hop Proxy
- **T1624** — Event Triggered Execution

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures

NIST-800-53R5

- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-4** — System Monitoring

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **3.10** — Encrypt Sensitive Data in Transit
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1646	Exfiltration Over C2 Channel	Exfiltration
T1513	Screen Capture	Collection
T1516	Input Injection	Defense-Evasion
T1632.001	Code Signing Policy Modification	Defense-Evasion
T1521	Encrypted Channel	Command-And-Control
T1219	Remote Access Tools	Command-And-Control
T1409	Stored Application Data	Collection
T1571	Non-Standard Port	Command-And-Control
T1417	Input Capture	Collection
T1660	Phishing	Initial-Access
T1509	Non-Standard Port	Command-And-Control
T1437	Application Layer Protocol	Command-And-Control
T1437.001	Web Protocols	Command-And-Control
T1481	Web Service	Command-And-Control
T1638	Adversary-in-the-Middle	Collection
T1412		
T1090.003	Multi-hop Proxy	Command-And-Control
T1624	Event Triggered Execution	Persistence

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/trickmo-android-bank...	T3
Microsoft Finds Vulnerability Exposing Millions of Android Crypto ...	https://www.securityweek.com/microsoft-finds-vulnerability-exposing...	T3

Source	URL	Tier
New trojan wave targets crypto wallets and banking apps - MSN	https://www.msn.com/en-us/news/technology/new-trojan-wave-targets-c...	T3
Android Malware Targets Banking and Crypto Apps - Binance	https://www.binance.com/en/square/post/316369894177505	T3
Android API exposure, Acrobat zero-day, Bitcoin Depot attack	https://cisoseries.com/cybersecurity-news-android-api-exposure-acro...	T3

Generated 2026-05-11 05:54 UTC by TJS Security Command Center