INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-12 19:06 UTC

TrickMo Android Banking Trojan Variant Leverages TON C2 and SOCKS5 for Network Pivoting

THREAT CAMPAIGN | **HIGH** | CVSS 7.8

SCC Item ID	SCC-CAM-2026-0308
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.8
Affected Products	Android devices targeted by TrickMo banking trojan; banking, cryptocurrency, and fintech users in France, Italy, and Austria
Published	2026-05-12
Discovery Source	Gemini

Executive Summary

A new TrickMo Android banking trojan variant has been identified using decentralized blockchain infrastructure for command-and-control and SOCKS5 proxy capabilities to route fraudulent transactions through victim devices. Banking, cryptocurrency, and fintech users in France, Italy, and Austria are the primary targets, with the malware harvesting credentials and executing on-device fraud while impersonating legitimate financial applications. The decentralized infrastructure makes traditional takedown efforts ineffective, extending the operational lifespan of this botnet and increasing the risk of undetected fraudulent transactions originating from customer devices.

Technical Analysis

This TrickMo variant introduces two operationally significant capabilities beyond prior documented versions. First, command-and-control communications are routed through The Open Network (TON) blockchain DNS, rendering conventional domain sinkholing and takedown ineffective, the C2 channel is decentralized and has no registrar or hosting provider to engage. Second, infected devices are weaponized as SOCKS5 proxy nodes, enabling threat actors to route fraudulent banking transactions through victim devices, bypassing geolocation-based fraud controls that financial institutions rely on. The malware retains TrickMo's established capability set: overlay attacks against banking and cryptocurrency applications, accessibility service abuse for on-device fraud (ODF), screen capture, and keylogging. Relevant CWE classifications: CWE-506 (embedded malicious code), CWE-267 (privilege abuse via accessibility services), CWE-200 (credential and data exposure),

CWE-923 (improper restriction of communication channel). MITRE ATT&CK techniques mapped include T1583.006 (Web Services for C2 via TON), T1055 (process injection), T1417 (input capture/keylogging), T1418 (application discovery), T1625 (hijack execution flow), T1090.003 (multi-hop proxy via SOCKS5), T1521 (encrypted channel), and T1437 (application layer protocol abuse). No CVE identifier is associated with this campaign. Prior variant documentation is available from Cleafy, ThreatFabric, and Zimperium. [Internal rollup reference: Tech Jack Solutions published a TrickMo.C campaign summary on 2026-05-11.] Patch status: no vendor patch applicable, this is a malware campaign, not a software vulnerability.

Action Checklist

1. Step 1: Containment. Note: This is a malware campaign, not a software vulnerability. Patching will not remove this threat; device wipe is required for full remediation. Block TON blockchain DNS resolution at the network perimeter; TON uses .ton TLD and custom DNS resolvers (e.g., 8.8.8.8 over port 53 to ton-aware resolvers). Identify and isolate any enrolled Android devices showing anomalous SOCKS5 outbound traffic on non-standard ports. Alert mobile device management (MDM) teams to flag side-loaded or unknown APKs on corporate and BYOD Android devices.
2. Step 2: Detection. Query mobile threat defense (MTD) and EDR tools for accessibility service grants to non-system applications on Android devices. Review firewall and proxy logs for SOCKS5 proxy traffic patterns on ports 1080, 9050, or custom ports from Android device IP ranges. Look for overlay activity indicators: applications requesting SYSTEM_ALERT_WINDOW or BIND_ACCESSIBILITY_SERVICE permissions. Check for DNS queries to TON-associated resolvers or .ton domains. IOC patterns include outbound connections to TON DNS resolvers and unexplained SOCKS5 tunnels originating from mobile device segments.
3. Step 3: Eradication. For confirmed infected devices: perform a factory reset; do not rely on antivirus removal alone given accessibility service persistence mechanisms. Revoke any active banking or financial application sessions associated with confirmed infected devices. Notify affected financial institutions of compromised devices to allow transaction review and session invalidation. Remove side-loaded APKs and enforce Google Play Protect or MDM application allowlisting.
4. Step 4: Recovery. Re-enroll wiped devices through MDM with a verified clean baseline before returning to production. Confirm banking application sessions have been re-established with fresh authentication. Monitor reinstated devices for 30 days for recurrence of SOCKS5 outbound traffic or anomalous accessibility service grants. Validate that fraud controls at financial institution partners have been notified and geolocation anomalies for affected accounts are under enhanced review.
5. Step 5: Post-Incident. This campaign exposes three control gaps: absence of mobile threat defense on BYOD and corporate Android devices, lack of network-layer visibility into SOCKS5 traffic from mobile segments, and insufficient monitoring of Android accessibility service abuse. Implement MTD tooling with behavioral detection. Add TON DNS resolver blocking to DNS security policy. Evaluate whether BYOD devices accessing financial or corporate applications require enrolled MDM with application vetting as a prerequisite.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately if any confirmed TrickMo-infected device has accessed corporate financial systems, banking APIs, or credential stores, or if transaction anomalies are detected at partner financial institutions — GDPR Article 33 requires breach notification to supervisory authorities within 72 hours if personal financial data was exfiltrated from users in France, Italy, or Austria.
Recovery Notes	Re-enrolled devices must pass Android SafetyNet or Play Integrity attestation and MDM compliance checks before corporate resource access is restored; do not trust antivirus clean results alone given TrickMo's accessibility service persistence. Monitor re-enrolled devices for 30 days with daily firewall log checks for SOCKS5 outbound traffic on ports 1080, 9050, or non-standard high ports from mobile device IP ranges, and weekly ADB accessibility service audits for the first two weeks. Coordinate with financial institution fraud teams to maintain enhanced transaction monitoring on affected accounts for a minimum of 60 days, as TrickMo's on-device fraud execution may have staged unauthorized transactions that clear on delayed settlement cycles.
Forensic Artifacts	Android ADB 'dumpsys accessibility' output from infected device — documents active BIND_ACCESSIBILITY_SERVICE grants to TrickMo's impersonator APK, which is the primary persistence and overlay execution mechanism for this variant | Firewall/proxy session logs showing SOCKS5 handshake traffic (TCP to ports 1080, 9050, or custom ports) from Android device IP ranges — documents TrickMo's use of the victim device as a SOCKS5 proxy node for routing fraudulent banking transactions through victim IP addresses to evade geolocation fraud controls | DNS resolver query logs for .ton TLD lookups and outbound DNS queries to non-standard resolver IPs — documents TrickMo's C2 beacon pattern via TON blockchain decentralized infrastructure, which is the distinguishing IOC of this specific variant | Extracted TrickMo impersonator APK AndroidManifest.xml — documents declared permissions (BIND_ACCESSIBILITY_SERVICE, SYSTEM_ALERT_WINDOW, RECEIVE_SMS, READ_SMS) and the list of targeted financial application package names used for overlay injection against banking, crypto, and fintech apps in FR/IT/AT | Financial institution transaction logs for the 30-day pre-eradication window on affected accounts — documents on-device fraud execution where TrickMo intercepted and manipulated banking sessions, with fraudulent transactions appearing as legitimate authenticated activity originating from the victim device's IP

Per-Action IR Details

Step 1: Containment — Block TON blockchain DNS resolution at the network perimeter; TON uses .ton TLD and custom DNS resolvers (e.g., 8.8.8.8 over port 53 to ton-aware resolvers). Identify and isolate any enrolled Android devices showing anomalous SOCKS5 outbound traffic on non-standard ports. Alert mobile device management (MDM) teams to flag side-loaded or unknown APKs on corporate and BYOD Android devices.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SI-3 (Malicious Code Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 2.3 (Address Unauthorized Software)

Compensating: On pfSense or OPNsense, add a DNS blocklist entry for known TON DNS resolver IPs (e.g., 159.69.212.228 and 185.244.149.14 used by ton.sh/adnl) and create a firewall rule blocking outbound TCP/UDP port 1080 and 9050 from the mobile device VLAN. Use Pi-hole with a custom blocklist for .ton TLD and TON resolver IPs. Run 'tcpdump -i eth0 port 1080 or port 9050' on the network gateway to capture SOCKS5 handshake traffic from Android device subnet ranges. Use Wireshark display filter 'tcp.port == 1080 && ip.src == ' to identify SOCKS5 CONNECT requests.

Evidence: BEFORE isolating devices, capture: full packet capture (PCAP) of SOCKS5 negotiation traffic from the mobile device segment to document the proxy destination IPs and ports used by TrickMo for transaction routing; DNS query logs from your recursive resolver showing .ton domain lookups or queries forwarded to TON-aware resolvers (look for unusual resolver IPs in outbound UDP/53 traffic); MDM enrollment records and last-known APK inventory for the device to establish a baseline for comparison; firewall session logs showing established outbound connections from Android device IPs on non-standard ports to identify C2 infrastructure before blocking cuts the connection.

Step 2: Detection — Query mobile threat defense (MTD) and EDR tools for accessibility service grants to non-system applications on Android devices. Review firewall and proxy logs for SOCKS5 proxy traffic patterns on ports 1080, 9050, or custom ports from Android device IP ranges. Look for overlay activity indicators: applications requesting SYSTEM_ALERT_WINDOW or BIND_ACCESSIBILITY_SERVICE permissions. Check for DNS queries to TON-associated resolvers or .ton domains. IOC patterns include outbound connections to TON DNS resolvers and unexplained SOCKS5 tunnels originating from mobile device segments.

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: Without MTD: use Android Debug Bridge (ADB) on enrolled devices — run 'adb shell dumpsys accessibility' to enumerate all active accessibility services and flag any non-system package names (anything not under com.android, com.google, or your MDM vendor namespace). Run 'adb shell dumpsys package | grep permission' to check SYSTEM_ALERT_WINDOW and BIND_ACCESSIBILITY_SERVICE grants for suspicious APKs. For network detection without a SIEM, run this Wireshark/tshark filter on the network tap: 'tshark -i eth0 -Y "tcp.dstport == 1080 or tcp.dstport == 9050" -T fields -e ip.src -e ip.dst -e tcp.dstport' and cross-reference source IPs against your Android device DHCP lease table. Use the open-source Sigma rule for SOCKS5 proxy abuse (SigmaHQ rule id: c51b284f-929b-4eb0-b34a-7e9cc18b0c3c) adapted for syslog from your perimeter firewall.

Evidence: Capture BEFORE analysis concludes: Android device ADB dump of 'dumpsys activity' and 'dumpsys package' output to document all installed APKs, declared permissions, and active services at time of detection — TrickMo variants persist via BIND_ACCESSIBILITY_SERVICE which survives app backgrounding; firewall proxy logs with full URI and connection metadata from Android device IP ranges for the 30 days prior to detection, since TrickMo's on-device fraud execution means fraudulent banking transactions will appear as legitimate HTTPS traffic from the device to bank endpoints; DNS resolver query logs filtered for .ton TLD queries and outbound DNS requests to non-corporate resolver IPs, which document the TrickMo C2 beacon pattern via TON blockchain lookups; any MDM compliance reports showing the device state (jailbreak/root detection status, unknown source installs enabled) at time of enrollment and at time of incident.

Step 3: Eradication — For confirmed infected devices: perform a factory reset; do not rely on antivirus removal alone given accessibility service persistence mechanisms. Revoke any active banking or financial application sessions associated with confirmed infected devices. Notify affected financial institutions of compromised devices to allow transaction review and session invalidation. Remove side-loaded APKs and enforce Google Play Protect or MDM application allowlisting.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AC-2 (Account Management), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Before factory reset, use ADB to pull the APK of the suspected TrickMo impersonator for forensic preservation: 'adb shell pm list packages -f | grep ' to get the APK path, then 'adb pull ./evidence/_.apk'. Submit the APK to VirusTotal or run it through MobSF (Mobile Security Framework, free and self-hostable) to confirm TrickMo classification and document the overlay target list (banking apps being impersonated). For session revocation without

enterprise IAM tooling, coordinate directly with the financial institution's fraud team using the device IMEI and account identifiers — most major banks in France, Italy, and Austria have fraud hotlines with session invalidation capability. Document the IMEI, Android device ID, and last-known IP before reset.

Evidence: Preserve BEFORE factory reset: full ADB backup of the device ('adb backup -apk -shared -all -f _backup.ab') or at minimum the APK file of the TrickMo impersonator application and its shared preferences/data directory if accessible — this documents which legitimate financial apps were being overlaid (TrickMo targets banking, crypto, and fintech apps in FR/IT/AT); extract and preserve the accessibility service configuration from 'adb shell settings get secure enabled_accessibility_services' to document persistence mechanism; capture transaction logs from affected banking applications for the 30 days prior to eradication to support financial institution fraud review — TrickMo executes on-device fraud so fraudulent transactions will appear in bank server logs as originating from the victim's authenticated session; document device IMEI, Android ID, and Google Account association for law enforcement referral if financial losses are confirmed.

Step 4: Recovery — Re-enroll wiped devices through MDM with a verified clean baseline before returning to production. Confirm banking application sessions have been re-established with fresh authentication. Monitor reinstated devices for 30 days for recurrence of SOCKS5 outbound traffic or anomalous accessibility service grants. Validate that fraud controls at financial institution partners have been notified and geolocation anomalies for affected accounts are under enhanced review.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: For MDM-less environments: enforce re-enrollment by requiring the device to pass a manual checklist before corporate resource access is restored — verify 'Unknown sources' / 'Install unknown apps' is disabled in Android settings, confirm Google Play Protect is enabled and has completed a fresh scan ('adb shell am start -a android.intent.action.VIEW -d market://launch?id=com.android.vending' then verify Play Protect status), and confirm no non-Play-Store APKs appear in 'adb shell pm list packages -f' against an approved whitelist. Set a 30-day monitoring cron job using a bash script that queries your firewall logs nightly for SOCKS5 outbound connections from the re-enrolled device's IP: 'grep -E "(1080|9050)" /var/log/firewall.log | grep ' and alerts via email if hits are found.

Evidence: Document DURING recovery phase: MDM re-enrollment timestamp and device attestation status (SafetyNet/Play Integrity API result) to establish a verified clean baseline — this is the recovery reference point if recurrence is detected in the 30-day watch period; screenshot or log export of Google Play Protect scan results post-wipe confirming no threats detected on the clean device; financial institution confirmation (email or ticket) that affected account sessions have been invalidated and fraud review has been initiated, including the transaction date range under review — this documents the blast radius for TrickMo's on-device fraud execution; fresh authentication tokens and session creation timestamps from banking applications re-established post-wipe to distinguish new legitimate sessions from any residual compromised sessions.

Step 5: Post-Incident — This campaign exposes three control gaps: absence of mobile threat defense on BYOD and corporate Android devices, lack of network-layer visibility into SOCKS5 traffic from mobile segments, and insufficient monitoring of Android accessibility service abuse. Implement MTD tooling with behavioral detection. Add TON DNS resolver blocking to DNS security policy. Evaluate whether BYOD devices accessing financial or corporate applications require enrolled MDM with application vetting as a prerequisite.

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 SI-4 (System Monitoring), NIST SI-3 (Malicious Code Protection), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 8.2 (Collect Audit Logs)

Compensating: For teams without MTD budget: deploy a free YARA rule targeting TrickMo APK characteristics (overlay activity declarations, BIND_ACCESSIBILITY_SERVICE combined with SYSTEM_ALERT_WINDOW and RECEIVE_SMS permissions in AndroidManifest.xml) and run it against any APKs extracted from employee devices during MDM check-ins using 'yara trickmo_rules.yar '. Add TON resolver IPs and the .ton TLD to Pi-hole or your existing DNS filtering solution as a permanent block category. Write a Sigma detection rule for your firewall log pipeline that fires on outbound SOCKS5 connection attempts (TCP SYN to port 1080/9050) originating from the mobile device VLAN segment. Document all three control gaps in a formal lessons-learned memo referencing this TrickMo campaign for the next risk assessment cycle per NIST IR-8.

Evidence: Compile for lessons-learned and risk register: complete timeline of TrickMo activity on the network reconstructed from DNS logs, firewall session logs, and MDM compliance events — this documents the dwell time between initial device compromise and detection, which informs detection gap prioritization; inventory of all corporate and BYOD Android devices that had access to financial or corporate applications during the incident window, cross-referenced against MDM enrollment status, to quantify the unmonitored attack surface that enabled this campaign; documentation of which financial institutions and account types were exposed to TrickMo's overlay and on-device fraud capability, to support breach notification evaluation under GDPR (France, Italy, Austria are all EU jurisdictions with 72-hour notification requirements if personal financial data was exfiltrated).

Detection Guidance

Primary behavioral indicators: (1) Android devices granting accessibility service permissions to applications not on an approved list, query MDM or MTD consoles for BIND_ACCESSIBILITY_SERVICE grants. (2) Outbound SOCKS5 proxy traffic (port 1080 or custom ports) from mobile device network segments, filter firewall logs for TCP connections to external IPs on port 1080 from Android device IP ranges. (3) DNS queries to TON-associated resolvers (TON DNS operates via custom resolvers; flag queries to non-standard DNS IPs from mobile segments). (4) Overlay activity: look for SYSTEM_ALERT_WINDOW permission usage by non-system applications in device logs. (5) Anomalous banking application session activity originating from the same device IP as other malicious indicators. No public IOC hash list was available in reviewed sources at time of writing, consult Cleafy (cleafy.com/cleafy-labs), ThreatFabric (threatfabric.com/blogs), and Zimperium for updated IOC feeds specific to TrickMo.C. Source quality score for this item is 0.64, treat IOC-level details as requiring verification against vendor-direct publications before operationalizing.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`.ton (TON blockchain DNS namespace)`	TrickMo variant uses TON blockchain DNS for C2 communications; block resolution of .ton domains and queries to non-standard TON DNS resolvers at the network perimeter	MEDIUM
URL	`SOCKS5 proxy endpoints — specific IPs not publicly disclosed in reviewed sources`	Infected devices act as SOCKS5 proxy exit nodes; monitor outbound TCP port 1080 from Android device segments for anomalous external connections	LOW

Framework Mappings

MITRE-ATTACK

- **T1583.006** — Web Services
- **T1055** — Process Injection
- **T1417** — Input Capture
- **T1418** — Software Discovery
- **T1625** — Hijack Execution Flow
- **T1090.003** — Multi-hop Proxy
- **T1521** — Encrypted Channel
- **T1437** — Application Layer Protocol

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

SOC2-TSC

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1583.006	Web Services	Resource-Development

Technique ID	Technique Name	Tactic
T1055	Process Injection	Defense-Evasion
T1417	Input Capture	Collection
T1418	Software Discovery	Discovery
T1625	Hijack Execution Flow	Persistence
T1090.003	Multi-hop Proxy	Command-And-Control
T1521	Encrypted Channel	Command-And-Control
T1437	Application Layer Protocol	Command-And-Control

Sources

Source	URL	Tier
A new TrickMo saga: from Banking Trojan to Victim's Data Leak	https://www.cleafy.com/cleafy-labs/a-new-trickmo-saga-from-banking-...	T3
TrickMo Android Trojan Exploits Accessibility Services for On-Device ...	https://thehackernews.com/2024/09/trickmo-android-trojan-exploits.html	T3
Banking Trojans | Mobile Security Glossary - Zimperium	https://zimperium.com/glossary/banking-trojans	T3
New TrickMo Variant: Device Take Over malware targeting Banking ...	https://www.threatfabric.com/blogs/new-trickmo-variant-device-take-...	T3
Android / Mobile (TrickMo.C Banking Trojan Campaign)	https://techjacksolutions.com/scc-vendor-rollup/android-mobile-tric...	T3

Generated 2026-05-12 19:06 UTC by TJS Security Command Center