INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-08 07:03 UTC

RedWing MaaS: Telegram-Distributed Android Banking Trojan Targets Financial Institutions With On-Device Fraud Capabilities

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0633
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Android devices; users of banking and cryptocurrency apps across 82 financial institutions; platforms mimicked include Google Play, Samsung Galaxy Store, Huawei AppGallery; emphasis on Russian financial sector targets
Published	2026-07-07T13:10:15
Discovery Source	Rss

Executive Summary

A Malware-as-a-Service platform called RedWing, distributed through Telegram, reportedly enables low-skill criminals to deploy Android banking trojans against users of 82 financial institutions, with reported emphasis on Russian banks and cryptocurrency services. The platform's subscription model lowers the barrier for fraud operators, making it resilient to individual takedowns through modular, rebrandable architecture. Organizations with a mobile banking presence or users in affected regions face elevated risk of customer account compromise and associated fraud losses. Note: core claims rest on a single T2 news source (The Hacker News, July 2026); independent corroboration from authoritative sources has not been identified.

Technical Analysis

RedWing is a reported Malware-as-a-Service (MaaS) platform advertised via Telegram that provides subscribers with an automated dropper builder, separable targeting configuration, and live device control. According to the primary source (The Hacker News, July 2026), technical capabilities include: overlay attacks to harvest banking credentials (CWE-927: Use of Implicit Intent for Sensitive Communication; CWE-693: Protection Mechanism Failure); accessibility service abuse for on-device interaction and data exfiltration (CWE-749: Exposed Dangerous Method or Function); and evasion techniques designed to bypass conventional mobile security tooling. MITRE ATT&CK for Mobile techniques reported include T1444 (Masquerade as

Legitimate Application), T1636.003 (Contact List Collection), T1406 (Obfuscated Files or Information), T1521 (Encrypted Channel), T1437 (Application Layer Protocol), T1412 (Capture SMS Messages), T1417 (Input Capture), T1660 (Phishing), T1582 (SMS Control), T1430 (Location Tracking), T1626 (Abuse Elevation Control Mechanism), and T1513 (Screen Capture). RedWing is reportedly linked to the Oblivion Android malware lineage per The Hacker News. Attribution to Russian-speaking actors carries moderate confidence based on targeting profile only. No CVE ID is associated. No patch or vendor advisory exists, this is a criminal platform, not a software vulnerability. No IOCs were provided in the source material. All technical claims are sourced from a single T2 article; treat as reported, not confirmed.

Action Checklist

1. Step 1: Containment, Audit your organization's mobile device management (MDM) policy to confirm enterprise-owned Android devices are restricted from sideloading applications outside approved stores. Block APK file downloads from Telegram and other non-official app store sources on managed endpoints where technically feasible, while preserving legitimate Telegram communication. Reference: NIST AC-20 (Use of External Systems), CIS 2.3 (Address Unauthorized Software).
2. Step 2: Detection, Monitor mobile threat defense (MTD) telemetry and endpoint detection tooling for indicators of accessibility service abuse (unusual accessibility service registrations), overlay activity, and anomalous outbound data from banking or cryptocurrency applications. Review AU-2 (Event Logging) requirements to confirm mobile device events are captured in your SIEM. Apply user account monitoring to flag unexpected account activity on devices enrolled in MDM.
3. Step 3: Eradication, There is no patch for this threat; RedWing is a criminal MaaS platform, not a software vulnerability. Eradication focus is removing unauthorized applications: audit installed app inventories on managed devices per CIS 2.1 (Establish and Maintain a Software Inventory), remove any unauthorized or sideloaded APKs, and revoke device trust for non-compliant endpoints. Reference NIST AC-2 (Account Management) to restrict application installation privileges.
4. Step 4: Recovery, Validate that MDM policies enforcing app allowlisting are active across all enrolled Android devices. Confirm accessibility service usage is logged and alerted. For any device suspected of compromise, perform a factory reset before re-enrollment. Post-remediation, monitor banking and crypto app sessions for anomalous behavior per AU-6 (Audit Record Review, Analysis, and Reporting). Apply credential rotation for any accounts accessed from a suspected device.
5. Step 5: Post-Incident, Review mobile application vetting procedures against CIS 2.1 and CIS 2.3 to ensure only authorized apps are permitted on managed devices. Assess whether your current mobile threat defense tooling detects accessibility service abuse and overlay attacks. Apply multi-factor authentication across all banking and financial application access paths to limit credential-only compromise impact. Reference NIST SI-4 (System Monitoring) to confirm mobile event sources are feeding your monitoring pipeline.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to CISO and legal counsel if forensic evidence confirms banking credentials or cryptocurrency private keys were exfiltrated from any device, as this triggers breach notification obligations under applicable financial sector regulations (e.g., GLBA, PSD2, or regional equivalents) and may require notification to affected financial institutions within defined regulatory windows.
Recovery Notes	After factory reset and re-enrollment of compromised devices, maintain elevated monitoring of banking and cryptocurrency account activity for a minimum of 30 days — RedWing's on-device fraud capability means fraudulent transactions may have been staged or pre-authorized before eradication, and some financial institutions may not surface unauthorized activity until settlement cycles complete. Verify with each affected financial institution that server-side session invalidation has been completed and that any pending transactions initiated from the compromised device have been reviewed and reversed where fraudulent. Confirm that re-enrolled devices pass MDM compliance checks for accessibility service restrictions and app allowlisting before returning to production use.
Forensic Artifacts	Android accessibility service registry dump ('adb shell settings get secure enabled_accessibility_services') — RedWing's primary persistence and interception mechanism; unauthorized entries here are the definitive indicator of active compromise on a device | APK files pulled from device storage via 'adb pull' for any package installed outside Google Play, Samsung Galaxy Store, or Huawei AppGallery — RedWing APKs mimic these stores' branding and are delivered via Telegram; SHA-256 hash each for IOC submission | Android full bug report ('adb bugreport') capturing volatile binder transaction logs, recent process activity, and SYSTEM_ALERT_WINDOW permission holder state — documents overlay attack infrastructure active at time of collection before factory reset destroys live state | Outbound network flow logs from device gateway or carrier covering the compromise window, filtered for HTTPS connections from banking and cryptocurrency app package names to non-CDN destinations — RedWing exfiltrates captured OTP codes and credentials over these channels to operator C2 infrastructure | Banking and cryptocurrency application local data directories (accessible under MDM managed profile) for session token caches, SQLite databases, and shared preferences files — RedWing's overlay and accessibility service components harvest and may locally stage captured credentials before transmission, leaving artifacts recoverable before factory reset

Per-Action IR Details

Step 1: Containment — Audit your organization's mobile device management (MDM) policy to confirm enterprise-owned Android devices are restricted from sideloading applications outside approved stores. Block Telegram-sourced APK delivery on managed endpoints where technically feasible. Reference: NIST AC-20 (Use of External Systems), CIS 2.3 (Address Unauthorized Software).

NIST Phase: Containment

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

Controls: NIST AC-20 (Use Of External Systems), CIS 2.3 (Address Unauthorized Software)

Compensating: For teams without enterprise MDM: use Android Debug Bridge (adb shell pm list packages -f) to enumerate installed APKs on enrolled devices and cross-reference against an approved allowlist maintained in a spreadsheet or CSV. Block Telegram's known APK delivery domains at the perimeter firewall or DNS layer using pi-hole or a manually maintained block list; confirm with Wireshark packet capture that APK download traffic to t.me or telegram.org is dropped before device reach.

Evidence: Before enforcing any new MDM restriction or revoking device trust, capture: (1) a full installed package list from each managed Android device via 'adb shell pm list packages -f' — RedWing APKs frequently masquerade as Google Play, Samsung Galaxy Store, or Huawei AppGallery installer packages, so preserve this snapshot before removal; (2) Android logcat output ('adb logcat -d') to preserve any accessibility service registration events already

recorded in volatile system logs; (3) active network connections from the device ('adb shell netstat -an') to identify any live C2 connections prior to policy enforcement, as RedWing maintains outbound beacon channels that will disappear once MDM restrictions terminate network access.

Step 2: Detection — Monitor mobile threat defense (MTD) telemetry and endpoint detection tooling for indicators of accessibility service abuse (unusual accessibility service registrations), overlay activity, and anomalous outbound data from banking or cryptocurrency applications. Review AU-2 (Event Logging) requirements to confirm mobile device events are captured in your SIEM. Apply D3-LAM (Local Account Monitoring) to flag unexpected account activity on devices enrolled in MDM.

NIST Phase: Detection Analysis

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

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

Compensating: Without commercial MTD: deploy an Android accessibility service audit script via adb — 'adb shell settings get secure enabled_accessibility_services' — on a scheduled basis (cron or Task Scheduler wrapper) and alert on any service registration that does not match an approved list of accessibility tools. For overlay detection, query 'adb shell dumpsys window windows' and parse for SYSTEM_ALERT_WINDOW permission holders outside of known legitimate apps. Forward adb logcat output for banking and cryptocurrency app package names to a local syslog instance and use a Sigma rule filtering on 'INJECT_EVENTS' or 'BIND_ACCESSIBILITY_SERVICE' permission grants.

Evidence: This step is analytical and does not alter live state, so volatile capture is advisory rather than blocking. Collect and preserve before analysis concludes: (1) Android Settings > Accessibility > Downloaded Services registry snapshot, which records all registered accessibility services — RedWing's core mechanism for intercepting banking app sessions; (2) 'adb shell dumpsys package' output filtered for apps holding SYSTEM_ALERT_WINDOW permission, the prerequisite for overlay attacks against banking UIs; (3) network flow logs from the device's carrier or Wi-Fi gateway showing outbound HTTPS connections from banking or cryptocurrency app package names to non-CDN IP ranges, which RedWing uses to exfiltrate captured credentials and OTP codes; (4) Android Security Event logs if device is enrolled in a managed profile, filtering for package installation events sourced outside Google Play (installer origin = 'com.telegram.messenger' or null).

Step 3: Eradication — There is no patch for this threat; RedWing is a criminal MaaS platform, not a software vulnerability. Eradication focus is removing unauthorized applications: audit installed app inventories on managed devices per CIS 2.1 (Establish and Maintain a Software Inventory), remove any unauthorized or sideloaded APKs, and revoke device trust for non-compliant endpoints. Reference D3-UAP (User Account Permissions) to restrict application installation privileges.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), NIST AC-6 (Least Privilege)

Compensating: For teams without MDM remote wipe capability: use 'adb shell pm uninstall --user 0 ' to remove identified RedWing APKs by package name from individual devices. Hash each suspicious APK before removal using 'adb shell pm path ' followed by 'sha256sum' of the pulled APK file — this preserves forensic evidence of the specific RedWing variant (MaaS builds are rebrandable, so hashes enable downstream threat intelligence sharing). Revoke device trust manually by removing the device certificate from your internal CA or disabling its MDM enrollment profile.

Evidence: Before uninstalling any APK or performing factory reset, acquire: (1) a forensic copy of the suspicious APK file via 'adb pull ' — RedWing's modular, rebrandable architecture means the APK itself is the primary artifact for variant identification and IOC extraction; (2) SHA-256 hash of the APK for submission to VirusTotal or internal threat intel platforms; (3) 'adb shell dumpsys accessibility' full output to document which accessibility service the RedWing component registered, including service label, package name, and permission flags; (4) a full Android bug report ('adb bugreport') from any device confirmed or suspected of compromise — this captures volatile process state, binder transaction logs, and recent application activity that a factory reset will permanently destroy; (5) banking and cryptocurrency app local data directories (where accessible under managed profile) for evidence of overlay injection

artifacts or stolen session token caches.

Step 4: Recovery — Validate that MDM policies enforcing app allowlisting are active across all enrolled Android devices. Confirm accessibility service usage is logged and alerted. For any device suspected of compromise, perform a factory reset before re-enrollment. Post-remediation, monitor banking and crypto app sessions for anomalous behavior per AU-6 (Audit Record Review, Analysis, and Reporting). Apply D3-CRO (Credential Rotation) for any accounts accessed from a suspected device.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AC-2 (Account Management), CIS 6.2 (Establish an Access Revoking Process), CIS 5.2 (Use Unique Passwords)

Compensating: For teams without automated credential rotation: generate a prioritized list of banking and cryptocurrency accounts accessed from suspected devices within the compromise window (pull from browser history or app session logs before factory reset), then manually force password resets for each account via institution support channels. Where banking apps support it, instruct affected users to invalidate all active sessions from the account security portal. For cryptocurrency accounts specifically, assess whether private keys or seed phrases were stored or typed on the compromised device — if so, treat key material as fully compromised and initiate wallet migration to a clean device.

Evidence: Before factory-resetting any suspected device, complete all volatile captures listed in Step 3. Before rotating credentials for banking and cryptocurrency accounts, document: (1) the full list of financial institutions and cryptocurrency services the user accessed from the compromised device — RedWing targets 82 named institutions, so scope the credential rotation to confirmed installed banking apps by reviewing 'adb shell pm list packages' output against the RedWing target list; (2) session token artifacts from banking app data directories if accessible under MDM managed profile, to determine whether active authenticated sessions exist that require server-side invalidation in addition to password rotation; (3) outbound DNS and HTTPS connection logs from the device covering the suspected compromise window, to identify which RedWing C2 infrastructure received exfiltrated data and to scope what credentials may have been transmitted.

Step 5: Post-Incident — Review mobile application vetting procedures against CIS 2.1 and CIS 2.3 to ensure only authorized apps are permitted on managed devices. Assess whether your current mobile threat defense tooling detects accessibility service abuse and overlay attacks. Apply D3-MFA (Multi-factor Authentication) across all banking and financial application access paths to limit credential-only compromise impact. Reference NIST SI-4 (System Monitoring) to confirm mobile event sources are feeding your monitoring pipeline.

NIST Phase: Post Incident

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

Controls: CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), NIST AU-2 (Event Logging)

Compensating: For teams without commercial MTD: write a standing YARA rule targeting RedWing APK structural patterns (DEX file strings referencing accessibility service binding, overlay permission declarations, and Telegram-sourced installer metadata) and apply it via YARA on any APK submitted to an internal review queue before device sideload approval is granted. Document the rule and scanning procedure in your mobile app vetting SOP. For MFA on banking applications where the institution supports TOTP: configure authenticator app enrollment on a separate, organization-controlled device rather than the same handset accessing the banking app, eliminating single-device OTP interception — the primary mechanism RedWing uses to bypass SMS-based 2FA.

Evidence: This phase is retrospective and does not alter live system state; volatile capture obligations are satisfied in prior steps. Post-incident evidence to preserve for lessons-learned and threat intelligence: (1) the full timeline of accessibility service registration events across all affected devices, reconstructed from logcat archives and MDM telemetry, to establish RedWing's dwell time and identify the initial infection vector (Telegram APK delivery timestamp vs. first malicious accessibility service registration); (2) a catalog of all banking and cryptocurrency app package names

installed on compromised devices cross-referenced against RedWing's known 82-institution target list, to inform peer organization threat sharing; (3) any Telegram channel metadata or APK delivery URLs captured during network forensics, for submission to threat intelligence platforms and law enforcement referral given the MaaS criminal infrastructure context.

Detection Guidance

Detection should focus on behavioral indicators rather than static IOCs, as no IOCs were provided in the source material. Key signals to monitor: (1) Accessibility service registrations, alert on Android devices where a newly installed or unknown application registers an accessibility service; most legitimate banking apps do not require this. (2) Overlay activity, monitor for applications rendering over banking or cryptocurrency app windows, particularly from packages not in your approved software inventory (CIS 2.1). (3) Anomalous SMS and screen capture activity, MITRE techniques T1412 and T1513 indicate SMS interception and screen capture; mobile threat defense platforms with behavioral analysis should be tuned for these patterns. (4) Unusual outbound encrypted channels, T1521 and T1437 suggest command-and-control over encrypted application-layer protocols; baseline normal mobile application traffic and alert on deviations. (5) Application impersonation, T1444 indicates masquerading as Google Play, Samsung Galaxy Store, or Huawei AppGallery; validate APK signing certificates against known-good store signatures. No specific log queries, event IDs, or IOC values can be provided from the available source material. All detection recommendations are derived from reported MITRE technique mappings.

Framework Mappings

MITRE-ATTACK

- **T1444**
- **T1636.003** — Contact List
- **T1406** — Obfuscated Files or Information
- **T1521** — Encrypted Channel
- **T1437** — Application Layer Protocol
- **T1412**
- **T1417** — Input Capture
- **T1660** — Phishing
- **T1582** — SMS Control
- **T1430** — Location Tracking
- **T1626** — Abuse Elevation Control Mechanism
- **T1513** — Screen Capture

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

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

SOC2-TSC

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

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1444		
T1636.003	Contact List	Collection
T1406	Obfuscated Files or Information	Defense-Evasion
T1521	Encrypted Channel	Command-And-Control
T1437	Application Layer Protocol	Command-And-Control
T1412		
T1417	Input Capture	Collection
T1660	Phishing	Initial-Access
T1582	SMS Control	Impact
T1430	Location Tracking	Collection
T1626	Abuse Elevation Control Mechanism	Privilege-Escalation
T1513	Screen Capture	Collection

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/redwing-maas-packages-android-ban.. .	T2
Google just revealed its Android security team detected and ...	https://qz.com/514720/google-just-revealed-its-android-security-tea...	T3
Hundreds of Android banking and crypto apps hit by ...	https://www.techradar.com/pro/security/hundreds-of-android-banking-...	T3

Source	URL	Tier
Security vulnerabilities are common in bank mobile apps	https://www.prosightfa.org/insights/security-vulnerabilities-are-co...	T3
Banking Trojans continue to surface on Google Play	https://www.welivesecurity.com/2018/10/24/banking-trojans-continue-...	T1

Generated 2026-07-08 07:03 UTC by TJS Security Command Center