INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-05 19:18 UTC

Asin Android Spyware Targets Arabic-Speaking Journalists and OSINT Researchers via Trojanized Conflict-Themed Apps

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0417
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Android devices (Xiaomi Redmi Note 13 Pro, Redmi Note 13 Pro+ 5G running Android 15); distributed via Facebook and Telegram
Published	2026-06-05T10:53:40
Discovery Source	Rss

Executive Summary

An unattributed threat actor is running a targeted Android spyware campaign, designated 'Asin,' against Arabic-speaking journalists and open-source intelligence researchers. The spyware is distributed through trojanized apps themed around government news, conflict mapping, and PDF tools, spread via Facebook and Telegram rather than app stores. Organizations employing journalists, OSINT analysts, or human rights researchers face direct risk of source exposure, surveillance of sensitive investigations, and compromise of internal communications.

Technical Analysis

ESET researchers identified the Asin Android spyware campaign in early 2025, targeting Arabic-speaking journalists and OSINT practitioners. Distribution uses socially engineered trojanized APKs delivered via Facebook and Telegram, bypassing app store vetting entirely. Confirmed affected devices include Xiaomi Redmi Note 13 Pro and Redmi Note 13 Pro+ 5G running Android 15, though the attack surface is not limited to these models. No CVE has been assigned. Applicable CWEs: CWE-276 (incorrect default permissions allowing excessive capability grants at install), CWE-668 (exposure of sensitive resources to unauthorized processes), CWE-923 (improper restriction of communication channels, enabling covert C2 contact). MITRE ATT&CK for Mobile techniques observed include T1406 (obfuscated files or information), T1582 (SMS control), T1476 (deliver malicious app via other means), T1418 (software discovery), T1432 (access contact list), T1444 (masquerade as legitimate application), T1636 (protected user data access), T1521 (encrypted channel), T1430

(location tracking), T1433 (access call log), and T1429 (capture audio). Operational objectives center on surveillance: contact harvesting, location tracking, audio capture, and call log access. CVSS scoring is not applicable to this campaign item. Severity is assessed qualitatively as high based on targeting scope, operational impact, and lack of available mitigations. No patch addresses this threat; the attack vector is social engineering and sideloading, not a vulnerability in Android itself. Threat actor remains unattributed as of reporting date. Detailed IOC information (hashes, C2 infrastructure) was not available in sources accessed during verification; behavioral indicators form the primary detection basis.

Action Checklist

1. Step 1: Containment. Identify all Android devices issued to journalists, OSINT analysts, and researchers in your organization. Temporarily restrict sideloading (installation from sources outside official app stores) via MDM policy enforcement. Block Facebook and Telegram as APK delivery vectors on managed devices where operationally feasible. Per NIST AC-19, enforce configuration requirements for mobile devices to prevent unauthorized app installation.
2. Step 2: Detection. Review MDM enrollment records and device logs for APKs installed from sources outside Google Play. Look for apps with names or icons referencing government news, conflict maps, or PDF utilities installed since early 2025. Check for anomalous outbound connections from mobile devices, particularly encrypted channels to unfamiliar endpoints (T1521). Review for permission grants covering contacts, call logs, microphone, and location on recently installed apps (T1432, T1433, T1429, T1430). Query MDM logs for devices where 'install from unknown sources' is enabled, per CIS 2.3; unauthorized software must be flagged and addressed. No specific IOC hashes or C2 infrastructure are confirmed in available sources; behavioral indicators are the primary detection path.
3. Step 3: Eradication. Remove any identified trojanized applications immediately. Factory reset compromised devices where feasible; if not, perform a full application audit and revoke all permissions granted to suspicious apps. Enforce MDM policies disabling 'install unknown apps' system-wide per NIST AC-19 and CIS 4.6. Re-issue devices to high-risk individuals (journalists, OSINT researchers) where compromise is suspected but cannot be ruled out.
4. Step 4: Recovery. After device remediation, rotate all credentials that were accessible on affected devices, including email, messaging apps, VPN, and any organizational accounts (D3-CRO). Verify MDM enrollment and configuration compliance across the mobile fleet. Monitor for re-infection attempts via continued social engineering on Telegram and Facebook. Confirm that 'install from unknown sources' remains disabled post-remediation per CIS 4.6.
5. Step 5: Post-Incident. Conduct targeted security awareness training for journalists and OSINT staff covering app installation risks and social engineering via Telegram and Facebook. Review mobile device management policies against NIST AC-19 and AC-20 to assess gaps in controlling app installation and external system usage. Implement a recurring review of app permissions on managed mobile devices per CIS 2.1 and CIS 2.3. Assess whether high-risk personnel (journalists, researchers) require hardened device configurations or dedicated isolated devices for sensitive work.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to legal, HR, and executive leadership if forensic evidence indicates Asin successfully exfiltrated journalist source identities, unpublished investigation details, or location data — this triggers potential source protection obligations, whistleblower protection legal exposure, and in jurisdictions with press freedom statutes, may constitute a notifiable incident; additionally escalate if any compromised device had access to organizational VPN or internal systems, as this extends the blast radius from mobile endpoints to the broader network.
Recovery Notes	After device remediation and credential rotation, monitor authentication logs for all rotated accounts for a minimum of 30 days for anomalous access attempts that would indicate adversary persistence established before remediation — Asin-class spyware targeting journalists typically seeks durable access to source communications, so credential reuse or session token theft from pre-wipe periods represents the highest residual risk. Verify weekly for the first month that 'install from unknown sources' remains disabled on all journalist and OSINT analyst devices and that no new apps matching the conflict-news or PDF-utility lure categories have been installed. Confirm with affected journalists whether they received and interacted with any Telegram or Facebook messages delivering the trojanized apps, and preserve those messages as evidence of the social engineering infrastructure used in the Asin campaign.
Forensic Artifacts	Full APK binary of the trojanized app extracted via 'adb pull' from /data/app// — provides SHA-256 hash for IOC sharing and enables static/dynamic analysis in MobSF to map Asin's data collection capabilities (contacts, call logs, microphone, GPS) against the declared and runtime-granted permissions on Xiaomi Redmi Note 13 Pro running Android 15 | Output of 'adb shell dumpsys package ' for each suspicious app — records exact install timestamp, installer source (expected to be com.facebook.katana or org.telegram.messenger rather than com.android.vending), and full list of granted dangerous permissions (READ_CONTACTS, READ_CALL_LOG, RECORD_AUDIO, ACCESS_FINE_LOCATION) that map to Asin's T1432, T1433, T1429, T1430 collection techniques | Network flow logs from corporate egress firewall or Wi-Fi controller for journalist/OSINT analyst device IPs — filtered for periodic outbound HTTPS connections to non-categorized or newly-registered domains, which would represent Asin's encrypted C2 exfiltration channel (MITRE T1521) and provide potential C2 infrastructure IOCs absent from current public reporting | Android logcat output captured via 'adb logcat -d -b all > _logcat.txt' before any wipe — preserves runtime evidence of Asin's background service execution, permission request dialogs accepted by the user, and any error messages revealing C2 communication attempts, which is particularly relevant given Xiaomi's MIUI/HyperOS layer on the Redmi Note 13 Pro may modify standard Android logging behavior | Telegram and Facebook message history from the delivery channel — request exports from affected journalists of the specific messages that delivered the trojanized APK links, preserving the social engineering lure text, sender account identifiers, and any associated media; this documents the Asin campaign's targeting methodology against Arabic-speaking journalists and provides intelligence for warning peer organizations

Per-Action IR Details

Step 1: Containment — Identify all Android devices issued to journalists, OSINT analysts, and researchers in your organization. Temporarily restrict sideloading (installation from sources outside official app stores) via MDM policy enforcement. Block Facebook and Telegram as APK delivery vectors on managed devices where operationally feasible. Per NIST AC-19, enforce configuration requirements for mobile devices to prevent unauthorized app installation.

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 4.6 (Securely Manage Enterprise Assets and Software), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: For teams without MDM: use Android Debug Bridge (ADB) to audit sideload status on each device — run 'adb shell settings get global install_non_market_apps' and 'adb shell settings get secure install_non_market_apps'; a return value of '1' indicates sideloading is enabled and must be disabled immediately via 'adb shell settings put global install_non_market_apps 0'. Maintain a manual spreadsheet inventory of all journalist and OSINT analyst devices with IMEI, assigned user, and enrollment status. For Facebook/Telegram APK delivery blocking without enterprise MDM, configure the organization's DNS resolver (e.g., Pi-hole) to block APK download domains and enforce the rule via DHCP on the corporate Wi-Fi network.

Evidence: Before restricting sideloading, capture the current 'install_non_market_apps' setting and a full installed package list via 'adb shell pm list packages -f -i' — this preserves a timestamped baseline of all APKs present, their install paths under /data/app/, and installer source attribution. Export MDM enrollment records for all journalist and OSINT analyst devices, noting any devices that dropped off MDM management since early 2025, which may indicate a compromised or unmanaged device receiving Asin via Telegram or Facebook side-channels.

Step 2: Detection — Review MDM enrollment records and device logs for APKs installed from sources outside Google Play. Look for apps with names or icons referencing government news, conflict maps, or PDF utilities installed since early 2025. Check for anomalous outbound connections from mobile devices, particularly encrypted channels to unfamiliar endpoints (T1521). Review for permission grants covering contacts, call logs, microphone, and location on recently installed apps (T1432, T1433, T1429, T1430). Query MDM logs for devices where 'install from unknown sources' is enabled — per CIS 2.3, unauthorized software must be flagged and addressed. No specific IOC hashes or C2 infrastructure are confirmed in available sources; behavioral indicators are the primary detection path.

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), NIST AC-19 (Access Control for Mobile Devices), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software)

Compensating: Without SIEM/EDR, run 'adb shell pm list packages -f -i --user 0' on each enrolled device and pipe the output through grep for installer sources other than 'com.android.vending' (Google Play) — any APK installed via 'com.facebook.katana', 'org.telegram.messenger', or 'null' installer is a priority triage target. For permission auditing, run 'adb shell dumpsys package | grep -E "CONTACTS|READ_CALL_LOG|RECORD_AUDIO|ACCESS_FINE_LOCATION"' against each suspicious package. For outbound C2 detection on a budget, deploy Wireshark or tcpdump on the network egress point and filter for mobile device IPs making repeated HTTPS connections to IPs with no PTR record or domains registered after January 2025 — Asin is expected to use encrypted exfiltration channels consistent with MITRE T1521.

Evidence: Capture the full output of 'adb shell dumpsys package' for every APK not installed via Google Play before any remediation — this records declared permissions, granted runtime permissions, install timestamp, and installer package name. Preserve network flow logs from the corporate Wi-Fi controller or firewall for all journalist and OSINT analyst device IPs, filtering for outbound connections on ports 443 and 8443 to IPs not associated with established services — Asin spyware consistent with T1432, T1433, T1429, T1430 would show periodic beacon-like connections to C2 infrastructure for exfiltrating contacts, call logs, audio recordings, and GPS coordinates. Document exact app names and icon descriptions referencing government news aggregation, conflict mapping (e.g., Gaza or Ukraine conflict themed), or PDF conversion utilities, as these are the confirmed Asin lure categories.

Step 3: Eradication — Remove any identified trojanized applications immediately. Factory reset compromised devices where feasible; if not, perform a full application audit and revoke all permissions granted to suspicious apps. Enforce MDM policies disabling 'install unknown apps' system-wide per NIST AC-19 and CIS 4.6. Re-issue devices to high-risk individuals (journalists, OSINT researchers) where compromise is suspected but cannot be ruled out.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-19 (Access Control for Mobile Devices), NIST SI-2 (Flaw Remediation), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 2.3 (Address Unauthorized Software)

Compensating: Before factory reset, perform a forensic-quality backup using 'adb backup -apk -shared -all -f _pre-wipe.ab' to preserve the APK and data for post-incident analysis — label the backup file with device owner and date. For devices where factory reset is not operationally feasible (journalists with active sources in messaging apps), use 'adb shell pm uninstall --user 0 ' to remove the trojanized app, then immediately revoke all dangerous permissions via 'adb shell pm revoke android.permission.READ_CONTACTS' (repeat for RECORD_AUDIO, ACCESS_FINE_LOCATION, READ_CALL_LOG). Verify removal with 'adb shell pm list packages' and confirm the package no longer appears. For re-issued devices, apply a hardened Android baseline before provisioning — disable developer options, enforce Google Play Protect, and enroll in MDM before handing to the journalist.

Evidence: Prior to wiping or uninstalling, extract the APK binary from the device using 'adb shell pm path ' to get the install path, then 'adb pull .apk' — submit this APK to VirusTotal or an internal sandbox (e.g., Cuckoo or MobSF) to generate a behavioral report and SHA-256 hash for IOC sharing with peer organizations covering journalists and OSINT researchers. Capture a full 'adb bugreport' before reset — this includes logcat, system logs, running process list, and network state at time of capture, preserving evidence of Asin's runtime behavior on Xiaomi Redmi Note 13 Pro hardware running Android 15.

Step 4: Recovery — After device remediation, rotate all credentials that were accessible on affected devices, including email, messaging apps, VPN, and any organizational accounts (D3-CRO). Verify MDM enrollment and configuration compliance across the mobile fleet. Monitor for re-infection attempts via continued social engineering on Telegram and Facebook. Confirm that 'install from unknown sources' remains disabled post-remediation per CIS 4.6.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-19 (Access Control for Mobile Devices), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For credential rotation without enterprise IAM tooling: generate a prioritized list of all accounts the affected journalist or OSINT analyst authenticated to from the compromised device — cross-reference browser saved credentials ('adb shell run-as cat /data/data//databases/logins.json' where accessible), email client configuration, and VPN profiles. Force password reset and revoke active sessions for each account via the respective provider's admin console. For ongoing re-infection monitoring without SIEM, configure the organization's email gateway (e.g., Google Workspace or Microsoft 365 admin alert rules) to flag inbound messages containing APK attachments or links to APK hosting domains sent to journalist accounts. Set up a weekly manual check on enrolled devices using 'adb shell settings get global install_non_market_apps' to verify sideloading remains disabled.

Evidence: Before rotating credentials, query authentication logs for each rotated account (Google Workspace Admin audit log, Microsoft Entra sign-in logs, VPN authentication logs) for the period since the estimated Asin installation date — look for login events from IP addresses or device fingerprints inconsistent with the journalist's normal work pattern, which would indicate Asin had already exfiltrated credentials and an adversary may have established persistent access to organizational accounts independent of the device. Preserve these logs under AU-11 retention requirements before rotation invalidates their investigative relevance.

Step 5: Post-Incident — Conduct targeted security awareness training for journalists and OSINT staff covering app installation risks and social engineering via Telegram and Facebook. Review mobile device management policies against NIST AC-19 and AC-20 to assess gaps in controlling app installation and external system usage. Implement a recurring review of app permissions on managed mobile devices per CIS 2.1 and CIS 2.3. Assess whether high-risk personnel (journalists, researchers) require hardened device configurations or dedicated isolated devices for sensitive work.

NIST Phase: Post Incident

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

Controls: NIST AC-19 (Access Control for Mobile Devices), NIST AC-20 (Use of External Systems), NIST AU-6 (Audit Record Review, Analysis, and Reporting), 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), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For a 2-person team, automate the recurring app permission review using a monthly cron job that runs 'adb shell dumpsys package' across all enrolled devices (via an ADB-over-network script), filters for dangerous permission grants on non-Play-installed packages, and emails the output to the security team. For hardened device configurations for journalists and OSINT researchers specifically, evaluate the free GrapheneOS hardened Android build (grapheneos.org) for Pixel devices as an alternative to stock Xiaomi Android 15 — GrapheneOS provides verified boot, per-app permission sandboxing, and network permission controls that would significantly limit Asin-class spyware's ability to exfiltrate contacts, audio, and location. Document lessons learned specifically around the Asin delivery vector (conflict-themed lures on Telegram and Facebook) and distribute a one-page advisory to all journalist and OSINT staff with screenshots of the lure app categories identified in this campaign.

Evidence: Compile the final incident timeline documenting: the estimated Asin installation date per device (from 'adb shell dumpsys package' install timestamps), the permissions granted and data categories potentially exfiltrated (contacts via T1432, call logs via T1433, audio via T1429, location via T1430), any organizational accounts with evidence of post-compromise access, and the social engineering vector (Facebook or Telegram message that delivered the trojanized APK). This timeline serves as both the post-incident report and the training case study for journalist security awareness sessions, and should be shared (with PII removed) with peer organizations in the press freedom and human rights research community to enable detection of the same Asin campaign targeting other Arabic-speaking journalist populations.

Detection Guidance

Primary detection relies on behavioral and permission-based indicators rather than signature IOCs, as no confirmed hashes or C2 addresses are available in current sources. Key indicators: (1) Android apps installed outside Google Play since early 2025 on devices belonging to journalists or OSINT staff, particularly apps themed around government news, conflict mapping, or PDF utilities; (2) permission grants at install covering microphone access (T1429), contacts (T1432), call logs (T1433), and location (T1430) on recently sideloaded apps; (3) outbound encrypted traffic from mobile devices to unfamiliar endpoints, especially persistent low-volume connections consistent with C2 beaconing (T1521); (4) SMS send/receive activity by non-messaging apps (T1582); (5) MDM alerts on devices where 'install from unknown sources' is enabled. Query MDM platform for devices with elevated permission profiles. If mobile EDR is deployed, alert on apps using obfuscated code structures (T1406) or masquerading as legitimate utilities (T1444). Baseline: compare installed app lists against the authorized software inventory required by CIS 2.1. Until ESET or partner organizations release confirmed IOC hashes or C2 infrastructure, rely on the behavioral and permission-based indicators listed above. These are sufficient for detection if devices are monitored via MDM or mobile EDR. Do not delay defense based on pending IOC release. Treat any specific values circulating in feeds as unverified until ESET publishes full IOC disclosure.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs available in reviewed sources`	ESET research referenced by T3 sources; full IOC disclosure not yet confirmed in available materials. Monitor ESET threat intelligence publications for hash, domain, and C2 releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T1406** — Obfuscated Files or Information
- **T1582** — SMS Control
- **T1476**
- **T1418** — Software Discovery
- **T1432**
- **T1444**
- **T1636** — Protected User Data
- **T1521** — Encrypted Channel
- **T1430** — Location Tracking
- **T1433**
- **T1429** — Audio Capture

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1406	Obfuscated Files or Information	Defense-Evasion
T1582	SMS Control	Impact
T1476		
T1418	Software Discovery	Discovery
T1432		
T1444		
T1636	Protected User Data	Collection
T1521	Encrypted Channel	Command-And-Control

Technique ID	Technique Name	Tactic
T1430	Location Tracking	Collection
T1433		
T1429	Audio Capture	Collection

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/android-spyware-asin-targets-arab...	T3
Redmi 13 Security Patch update has arrived. Has anyone done it	https://www.facebook.com/groups/2605632532990184/posts/409552950400...	T3
Xiaomi Redmi Note 13 Pro Plus Phone Platform Intelligence - Genians	https://journey.genians.com/platform/Xiaomi_Redmi_Note_13_Pro_Plus_...	T3
Has the redmi note 13 pro plus received any Android version updates?	https://www.reddit.com/r/XiaomiGlobal/comments/1lxt62q/has_the_redm...	T3
Redmi Note 13 Pro + Frp Bypass Android 15 | With Out Pc - YouTube	https://www.youtube.com/watch?v=CIuBBvsvjQI	T3

Generated 2026-06-05 19:18 UTC by TJS Security Command Center