INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 08:38 UTC

ScarCruft Deploys BirdCall Android Malware via Compromised Gaming Platform in Supply Chain Attack

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0274
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Android devices; users of compromised Korean-language gaming platform (specific platform name unconfirmed without direct source access)
Discovery Source	Gemini

Executive Summary

ScarCruft (APT37), a North Korean state-sponsored threat group, compromised a Korean-language gaming platform to distribute BirdCall, a surveillance-grade Android malware targeting ethnic Koreans in China, including North Korean defectors. The malware collects audio recordings, contacts, SMS messages, location data, and files from infected devices. While the immediate target population is specific, the supply chain delivery method and the actor's history of expanding operations warrant attention from any organization with Android device exposure or connections to Korean diaspora communities.

Technical Analysis

ScarCruft (also tracked as APT37, Reaper) executed a supply chain compromise against an unconfirmed Korean-language Android gaming platform, trojanizing game applications to deliver BirdCall malware to targeted Android devices. BirdCall capabilities reported across secondary sources include: audio recording, SMS and contact harvesting, GPS location tracking, and file exfiltration. The attack chain leverages compromised legitimate distribution infrastructure (T1195.002, Compromise Software Supply Chain) to bypass user trust barriers, with the trojanized APK serving as the initial access vehicle. Post-installation behaviors map to: T1636.002 (Contact List), T1636.003 (SMS Messages), T1430 (Location Tracking), T1533 (Data from Local System), T1437 (Application Layer Protocol for C2), T1418 (Software Discovery), and T1571 (Non-Standard Port). Relevant weaknesses include CWE-267 (Privilege Defined with Unsafe Actions), CWE-494 (Download of Code Without Integrity Check), and CWE-441 (Unintended Proxy/Intermediary). No CVE is assigned; no patch is applicable given the supply chain delivery model. Attribution to ScarCruft is assessed at high confidence based on TTP and tooling consistency with prior campaigns. Technical capability detail is medium confidence;

this assessment draws exclusively from secondary news reporting (Tier 3 outlets). No primary threat intelligence report, CISA advisory, or vendor ATR was consulted. Verify technical specifics and IOCs against primary threat intelligence sources before operationalizing detections.

Action Checklist

1. Containment: Identify and block network connections to known ScarCruft C2 infrastructure using current threat intelligence feeds; restrict sideloading and third-party APK installation on managed Android devices via MDM policy immediately.
2. Detection: Query MDM and UEM telemetry for Android devices that installed applications from unverified or newly registered sources; review endpoint telemetry for anomalous audio permission grants, bulk SMS reads, or high-frequency location polling on Android endpoints; check network logs for non-standard port outbound traffic (T1571) from mobile device segments.
3. Eradication: Remove any identified BirdCall-infected applications from enrolled devices; revoke device certificates and re-enroll clean devices where infection is confirmed; update mobile threat defense (MTD) signatures for BirdCall indicators when available from your MTD vendor.
4. Recovery: Validate managed Android fleet shows no residual C2 beacon activity post-remediation; confirm MDM policy enforcing app source restrictions is applied and reporting compliance; rotate credentials accessible via affected devices (contacts, email, any accounts reachable from the device).
5. Post-Incident: Review mobile device management policy gaps around third-party APK installation and app vetting; assess whether employees with access to sensitive data have adequate mobile endpoint controls; evaluate whether ScarCruft targeting criteria (Korean diaspora connections, defector support work, cross-border operations) intersects with your organization's personnel profile.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if any device forensic image confirms BirdCall exfiltration of audio recordings, SMS content, or location data belonging to employees who are North Korean defectors, support defector organizations, or have documented cross-border operations — this constitutes both a targeted nation-state surveillance incident against a protected population and a potential PII breach requiring regulatory notification assessment.
Recovery Notes	Post-containment, monitor all perimeter firewall and DNS resolver deny logs for ScarCruft IOCs for a minimum of 30 days, as BirdCall's supply chain delivery method means additional devices may have downloaded the trojanized APK before the compromise was detected and could activate beaconing after a delay. Verify that re-enrolled devices pass MDM compliance checks for 'Unknown sources: Disabled' and that no apps with RECORD_AUDIO, READ_CONTACTS, READ_SMS, or ACCESS_FINE_LOCATION permissions exist outside your approved application allowlist. Given ScarCruft's history of credential reuse and pivot to additional targets using harvested contact data, monitor for spearphishing activity targeting individuals whose contact information was present on any confirmed-infected device.

Forensic Artifacts	Android device forensic image of '/data/data//' directory: preserves SQLite databases containing staged SMS harvests, contact dumps, audio recording file references, and location logs collected by BirdCall prior to exfiltration — direct evidence of what data was taken and the exfiltration staging behavior (MITRE T1636, T1533). | Android Logcat buffer export ('adb logcat -d'): captures BirdCall runtime behavior including file system access events, permission invocations for RECORD_AUDIO and ACCESS_FINE_LOCATION, and outbound network call logs to C2 endpoints — critical for establishing the malware's collection timeline on each device. | MDM/UEM app installation telemetry: records the install timestamp, install source (sideload indicator: 'com.android.packageinstaller'), and package name of BirdCall on each enrolled device, establishing which users installed the trojanized gaming platform APK and when. | Perimeter firewall and DNS resolver logs for the mobile device network segment: documents outbound C2 beacon traffic on non-standard ports (MITRE T1571) and DNS queries to ScarCruft-associated domains, providing network-layer evidence of active infections and the exfiltration channel used by BirdCall. | Runtime permission grant history from Android bug reports ('adb bugreport'): contains a timestamped record of when BirdCall was granted RECORD_AUDIO, READ_SMS, ACCESS_FINE_LOCATION, and READ_CONTACTS permissions — establishes the moment surveillance capability became active on each device and supports timeline reconstruction for breach notification assessments.

Per-Action IR Details

Containment — Identify and block network connections to known ScarCruft C2 infrastructure using current threat intelligence feeds; restrict sideloading and third-party APK installation on managed Android devices via MDM policy immediately.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Pull current ScarCruft C2 IOCs from MISP, OpenCTI, or AlienVault OTX (search tag 'APT37' or 'ScarCruft'); push those IPs/domains as deny rules to your perimeter firewall or pfSense ACL immediately. For MDM-less environments: distribute a signed Android Enterprise Device Policy app config or use ADB in restricted mode — run 'adb shell settings put global install_non_market_apps 0' on each enrolled device, then confirm with 'adb shell settings get global install_non_market_apps'. Document the timestamp and device IDs touched.

Evidence: BEFORE blocking, capture full NetFlow or firewall session logs from the mobile device network segment (Wi-Fi SSID or MDM-reported IP range) for at least 30 days back, focusing on outbound connections over non-standard ports (per MITRE T1571) to IP ranges associated with ScarCruft infrastructure. Preserve MDM enrollment records and device check-in timestamps for all Android assets to establish which devices were online during the compromise window of the gaming platform distribution. If a mobile threat defense (MTD) agent is deployed, export raw event logs before any policy push to prevent log rotation.

Detection — Query MDM and UEM telemetry for Android devices that installed applications from unverified or newly registered sources; review endpoint telemetry for anomalous audio permission grants, bulk SMS reads, or high-frequency location polling on Android endpoints; check network logs for non-standard port outbound traffic (T1571) from mobile device segments.

NIST Phase: Detection Analysis

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

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

Compensating: Export MDM app inventory reports (Google Workspace endpoint management or Microsoft Intune free tier both expose installed app lists) and diff against your approved app allowlist — flag any APK with a package name not present in Google Play at the time of install or with an install source of 'com.android.packageinstaller' (sideload indicator). For network detection without SIEM: use Wireshark or Zeek on the mobile VLAN uplink and write a display filter for 'tcp.port != 80 && tcp.port != 443 && ip.src == [mobile_subnet]' to surface T1571 traffic. For permission abuse: pull Android bug reports via 'adb bugreport' and grep for 'RECORD_AUDIO', 'READ_SMS', and 'ACCESS_FINE_LOCATION' grant events correlated to the BirdCall package name once identified.

Evidence: Capture Android device bug reports ('adb bugreport ') for any device that visited or downloaded from the compromised Korean-language gaming platform — these contain the runtime permission grant history, installed package list with install timestamps and sources, and battery/network usage stats per app that will show BirdCall's audio recording and location polling behavior. Extract MDM app installation logs filtered to the timeframe of the supply chain compromise window. Pull network proxy or DNS logs for queries to newly registered domains or domains using Korean-language TLDs (.kr) from mobile device IPs, which ScarCruft has historically used for C2 staging (MITRE ATT&CK T1583.001 — Acquire Infrastructure: Domains).

Eradication — Remove any identified BirdCall-infected applications from affected devices; revoke device certificates and re-enroll clean devices where infection is confirmed; update mobile threat defense (MTD) signatures for BirdCall indicators when available from your MTD vendor.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST IA-3 (Device Identification and Authentication), CIS 2.3 (Address Unauthorized Software), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without enterprise MTD: build a YARA rule targeting BirdCall's known characteristics — focus on strings associated with audio exfiltration routines, SMS harvesting classes, and APT37's reuse of obfuscation patterns documented in prior ScarCruft Android tools (RambleOn, Chinotto). Deploy via MobSF (open source) for static analysis of APKs on enrolled devices where you can extract the APK using 'adb shell pm path ' then 'adb pull '. Perform factory reset on confirmed-infected devices rather than attempting app-only removal — BirdCall-class surveillanceware has demonstrated persistence via accessibility service abuse (MITRE T1626) that survives simple uninstall on some Android versions. Revoke any MDM device certificates via your MDM admin console before re-enrollment.

Evidence: BEFORE wiping or removing the application, forensically image the device using UFED, Cellebrite UFED4PC, or the open-source Android Backup Extractor targeting '/data/data//' to preserve SQLite databases containing harvested SMS records, contact dumps, and audio file staging directories. Capture a full copy of the device's '/proc/net/tcp' and '/proc/net/tcp6' to document active C2 socket connections at time of eradication. Export the Android Logcat buffer ('adb logcat -d > device_logcat.txt') before any removal action to preserve runtime evidence of BirdCall's collection behavior including file access patterns and network calls.

Recovery — Validate managed Android fleet shows no residual C2 beacon activity post-remediation; confirm MDM policy enforcing app source restrictions is applied and reporting compliance; rotate credentials accessible via affected devices (contacts, email, any accounts reachable from the device).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST CM-6 (Configuration Settings), NIST AU-12 (Audit Record Generation), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Validate C2 silence by monitoring your perimeter firewall deny logs and DNS RPZ block logs for 14 days post-remediation, specifically watching for any queries or connection attempts to the ScarCruft IOC list you blocked during containment — any hit after eradication indicates reinfection or a missed device. For credential rotation without an enterprise PAM tool: generate a prioritized list from the recovered device's contact database backup (from forensic image) and email account linked to the device, then force password reset via your identity provider admin console (Google Workspace Admin or Microsoft Entra ID); enable login audit logging before rotation so you can detect

any in-progress account takeover using the stolen credentials. Confirm MDM compliance reporting shows 'Unknown sources: Disabled' for 100% of enrolled Android devices.

Evidence: Run a final MDM compliance report and export it as timestamped evidence that all previously non-compliant devices are now enrolled and policy-compliant; this serves as the recovery baseline. Query DNS resolver logs (Pi-hole, Cisco Umbrella free tier, or ISP logs) for 14 days post-remediation for any queries matching the ScarCruft C2 domain list — a hit indicates either a missed infected device or an attacker pivoting from stolen credentials. Document all accounts that had authenticated sessions on affected devices during the compromise window, as BirdCall's credential and contact harvesting capability (MITRE T1636 — Protected User Data: Contact List) means those third parties may also require notification.

Post-Incident — Review mobile device management policy gaps around third-party APK installation and app vetting; assess whether employees with access to sensitive data have adequate mobile endpoint controls; evaluate whether ScarCruft targeting criteria (Korean diaspora connections, defector support work, cross-border operations) intersects with your organization's personnel profile.

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 PM-12 (Insider Threat Program), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Conduct a personnel profile review using only HR-approved data: identify employees with Korean-language proficiency, ties to North Korean defector support organizations, or roles involving cross-border operations into China — this mirrors ScarCruft's documented targeting of ethnic Koreans abroad and North Korean defector communities, and should inform tiered mobile security controls for those individuals. For policy gap assessment without a GRC tool: create a simple spreadsheet comparing your current MDM policy settings against the CIS Benchmark for Android (available free at cisecurity.org) and score each gap by data sensitivity of the employees affected. Submit findings as a formal lessons-learned memo referencing this incident, per NIST 800-61r3 §4 requirements, and include recommended timeline for MDM policy hardening.

Evidence: Compile the full incident timeline from MDM enrollment logs, network firewall logs, and device forensic images collected during earlier phases into a single chronological record — this is the primary artifact for lessons-learned and any regulatory reporting. Document whether any BirdCall-exfiltrated data (audio recordings, SMS content, contact lists, location history) meets PII or sensitive personal data thresholds under applicable privacy regulations (GDPR, South Korea PIPA, or U.S. state laws) that would trigger breach notification obligations; this determination requires legal review. Retain all forensic images and log exports for a minimum consistent with your incident record retention policy (NIST AU-11) and applicable breach notification statutes.

Detection Guidance

Primary detection surfaces are MDM/UEM platforms and mobile threat defense solutions. Look for: (1) Android applications installed outside approved app store channels, particularly Korean-language gaming apps with elevated permission requests (microphone, contacts, SMS, location, storage); (2) Outbound network traffic from mobile device segments on non-standard ports, consistent with T1571; (3) Processes on Android devices with concurrent microphone, contacts, and SMS permissions active outside normal usage hours; (4) Bulk SMS read events or rapid contact enumeration on Android endpoints, indicative of T1636.002 and T1636.003; (5) High-frequency GPS polling inconsistent with foreground app usage, T1430. IOCs: No hashes, domains, or IP addresses are provided from secondary reporting at this time. Pull current BirdCall and ScarCruft IOC sets from primary threat intelligence platforms (CISA, your vendor ATR subscription, or ISAC feeds) and cross-reference against mobile telemetry. MITRE ATT&CK for Mobile provides detection logic scaffolding for the mapped techniques.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`[not available — no confirmed IOCs extractable from secondary sources at this time]`	BirdCall C2 infrastructure — pull current indicators from threat intelligence platform or ISAC feeds; do not operationalize unverified values	LOW

Framework Mappings

MITRE-ATTACK

- **T1636.002** — Call Log
- **T1437** — Application Layer Protocol
- **T1418** — Software Discovery
- **T1195.002** — Compromise Software Supply Chain
- **T1533** — Data from Local System
- **T1636.003** — Contact List
- **T1430** — Location Tracking
- **T1571** — Non-Standard Port

NIST-800-53R5

- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **15.1** — Establish and Maintain an Inventory of Service Providers

NIST-CSF-2

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

ISO-27001-2022

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

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1636.002	Call Log	Collection
T1437	Application Layer Protocol	Command-And-Control
T1418	Software Discovery	Discovery
T1195.002	Compromise Software Supply Chain	Initial-Access
T1533	Data from Local System	Collection
T1636.003	Contact List	Collection
T1430	Location Tracking	Collection
T1571	Non-Standard Port	Command-And-Control

Sources

Source	URL	Tier
ScarCruft Hacks Gaming Platform to Deploy BirdCall Malware on ...	https://thehackernews.com/2026/05/scarcruft-hacks-gaming-platform-t...	T3
North Koreans Spy on Defectors Via Android Game Apps	https://www.bankinfosecurity.com/north-koreans-spy-on-defectors-via...	T3
ScarCruft hackers push BirdCall Android malware via game platform	https://www.bleepingcomputer.com/news/security/scarcruft-hackers-pu...	T3
ScarCruft Hacks Gaming Platform to Deploy BirdCall Malware on ...	https://x.com/TheHackersNews/status/2051589864467075341	T3
ScarCruft Compromises Gaming Platform in Supply Chain Attack to ...	https://www.instagram.com/p/DX8950UFpWN/	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-06 08:38 UTC by TJS Security Command Center