INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-02 06:12 UTC

NoVoice Rootkit Clones WhatsApp Sessions from 2.3 Million Infected Android Devices via Google Play

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0139
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Android devices with security patches prior to May 2021; Google Play ecosystem; WhatsApp (Android); Mali GPU driver (unspecified versions)
Published	2026-04-01T14:07:21
Discovery Source	Rss

Executive Summary

A large-scale Android malware campaign, designated 'NoVoice,' distributed rootkit-capable malware through more than 50 trojanized applications on Google Play, accumulating approximately 2.3 million installs before removal. The rootkit achieves kernel-level persistence and targets WhatsApp by extracting session keys, enabling attackers to clone messaging sessions on attacker-controlled infrastructure, giving adversaries full access to encrypted communications without requiring the device itself. Organizations whose employees use Android devices for business communications, including WhatsApp for operational or executive messaging, face a credible risk of session compromise and data exfiltration that cannot be remediated through standard app removal on older unpatched devices. NOTE: This campaign is sourced from secondary outlets with a source quality score of 0.56; CVE identifiers, full attribution, and the 2.3 million install figure require verification against primary sources before use in board-level reporting.

Technical Analysis

NoVoice is a kernel-level Android rootkit distributed via trojanized applications published to Google Play. The malware exploits previously patched Android kernel vulnerabilities and unspecified Mali GPU driver flaws to achieve ring-0 persistence, replacing system libraries to survive reboots and standard application removal. The primary payload targets WhatsApp by exfiltrating Signal Protocol session keys and encrypted message databases (T1409, T1533, T1521), enabling full session cloning on attacker infrastructure. Devices running Android security patch levels dated May 2021 or earlier are reported to have no clean software-based recovery

path. Relevant CWE mappings include CWE-269 (Improper Privilege Management), CWE-416 (Use After Free, consistent with Mali GPU driver exploitation patterns), CWE-494 (Download of Code Without Integrity Check), CWE-732 (Incorrect Permission Assignment), and CWE-311 (Missing Encryption of Sensitive Data). MITRE ATT&CK for Mobile techniques include T1628 (Hide Artifacts), T1577 (Compromise Application Executable), T1603 (Scheduled Task/Job), T1475 (Deliver Malicious App via Authorized App Store), T1629.003 (Impair Defenses: Disable or Modify Tools), T1407 (Download New Code at Runtime), and T1437 (Application Layer Protocol). Additional techniques (T1553, T1627, T1422, T1624, T1406, T1636, T1430, T1635, T1512) map to rootkit persistence, privilege escalation, obfuscation, and C2 communication patterns consistent with kernel-level malware families. Structural similarities to the Triada malware family have been noted; no formal attribution has been confirmed. No CVE identifiers were included in source data, specific CVE references require verification against Android Security Bulletins or NVD. Source quality score: 0.56; all technical specifics should be treated as unconfirmed until validated against Android Security Bulletins, CISA advisories, or MITRE ATT&CK confirmed campaign data.

Action Checklist

1. Step 1: Containment. Audit all managed Android devices for patch level. Flag and quarantine any device running an Android security patch dated May 2021 or earlier from corporate network access, VPN, email, and messaging systems immediately. For BYOD environments, issue an emergency policy notification requiring employees to verify their patch level via Settings > Security > Security patch level and report unpatched devices to IT.
2. Step 2: Detection. Query MDM/UEM platform (e.g., Intune, Jamf, VMware Workspace ONE) for enrolled Android devices with security patch level < 2021-06-01. For unmanaged devices, request self-attestation. Review app installation logs for any of the 50+ flagged applications; specific package names require validation from the BleepingComputer source URL or Google Play security advisory once confirmed. Monitor for anomalous WhatsApp session activity including simultaneous logins from unknown devices via WhatsApp's linked devices feature. Watch for unexpected outbound data transfers from Android devices to unrecognized IP ranges. NOTE: No confirmed IOC hashes or package names are available from current source data; organizations should monitor threat intelligence feeds (CISA, VirusTotal, internal threat intelligence platform) for package names and hashes as this campaign develops.
3. Step 3: Eradication. For devices on Android patch level May 2021 or earlier with confirmed or suspected infection, full factory reset is insufficient given reported kernel-level persistence; device replacement is the reported remediation path. For devices on current patch levels, remove any identified trojanized applications and apply all pending Android security updates immediately. Direct users to revoke all WhatsApp linked device sessions via WhatsApp > Linked Devices and re-register. Verify Google Play Protect is enabled and run a full scan.
4. Step 4: Recovery. Post-remediation, confirm Android security patch level is current (minimum: verify against current Android Security Bulletin at source.android.com/docs/security/bulletin). Re-enroll replaced devices through MDM before granting access to corporate resources. For accounts where WhatsApp session cloning may have occurred, treat the account as compromised: notify affected users, assess what business communications may have been exposed, and consider whether escalation to legal or compliance is warranted based on data sensitivity. Monitor MDM telemetry for re-infection indicators for 30 days post-remediation.
5. Step 5: Post-Incident. This campaign exposes three concrete control gaps: (1) absence of enforced minimum Android patch level policy in MDM - implement a compliance policy that blocks network access

for devices below a defined patch threshold; (2) use of WhatsApp or other consumer messaging applications for business communications without session monitoring or MDM-enforced app vetting - evaluate whether consumer messaging should be permitted for business use or replaced with enterprise-grade alternatives; (3) reliance on Google Play vetting as a sufficient security control - consider supplementing with a managed app allowlist and mobile threat defense (MTD) solution that performs on-device behavioral analysis independent of Play Protect.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to legal, compliance, and executive leadership immediately if forensic evidence or user reporting confirms WhatsApp session cloning occurred on any device used for business communications, as cloned sessions provide attackers full read access to message history and attachments — triggering potential breach notification obligations under GDPR, HIPAA, or applicable state privacy laws depending on the sensitivity of communications exposed during the session clone window.
Recovery Notes	Post-containment, re-enrollment must be gated on verified current Android Security Bulletin patch level — not merely OS version — because the Mali GPU driver vulnerability exploited by NoVoice was patched in the May 2021 bulletin specifically; a device on Android 11 with a pre-May 2021 security patch remains vulnerable. Monitor MDM telemetry for all re-enrolled devices for a minimum of 30 days for indicators of re-infection, specifically new installations of applications not on the approved allowlist and new WhatsApp Linked Device session registrations from unrecognized device identifiers. Any re-infection indicator within the monitoring window should trigger immediate re-quarantine and escalation, as kernel-level rootkit persistence surviving a factory reset on older devices is a documented characteristic of this campaign.
Forensic Artifacts	ADB bug report archive (adb bugreport) from pre-replacement infected devices: contains dmesg kernel log showing Mali GPU driver exploitation artifacts, running process list at time of capture, and full installed package manifest with installer source — primary forensic record for this kernel-level rootkit campaign | MDM app installation logs showing package name, installation timestamp, and install source (com.android.vending) for any of the 50+ trojanized Play Store applications associated with the NoVoice campaign — installation timestamp establishes the earliest possible session compromise window | WhatsApp Linked Devices list exports or screenshots captured before session revocation — each unrecognized linked device entry represents a cloned session on attacker-controlled infrastructure and defines the scope of unauthorized message access | Network firewall or proxy logs for Android device IP ranges showing outbound TLS connections to non-Google/non-Meta ASNs during and after the trojanized app installation window — the NoVoice rootkit exfiltrates extracted WhatsApp session keys over C2 channels that would appear as anomalous outbound connections from the infected device | Google Play Protect scan history exported from MDM telemetry or device settings, showing any flagged, disabled, or removed applications — Play Protect removal of a NoVoice campaign application post-infection does not confirm eradication of the kernel-level rootkit component and should be treated as an infection confirmation indicator rather than a remediation record

Per-Action IR Details

Step 1: Containment — Audit all managed Android devices for patch level. Flag and quarantine any device running an Android security patch dated May 2021 or earlier from corporate network access, VPN, email, and

messaging systems immediately. For BYOD environments, issue an emergency policy notification requiring employees to verify their patch level via Settings > Security > Security patch level and report unpatched devices to IT.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy; CSF [RS] — Execute IR plan, categorize, contain, communicate, mitigate

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access) — suspend remote access for unpatched devices, CIS 4.4 (Implement and Manage a Firewall on Servers) — block unpatched device network segments at perimeter, CIS 6.2 (Establish an Access Revoking Process) — revoke VPN and corporate resource access for non-compliant devices, CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without MDM: export the corporate VPN client's active session list and cross-reference device identifiers against a manually collected Android patch level spreadsheet via employee self-attestation form. Block non-compliant device MACs or certificate-based VPN identities at the firewall using a deny ACL. Use a free Google Sheet with enforced submission deadline and manager escalation for non-responders. For Wi-Fi segmentation without MDM: push a VLAN isolation rule on managed APs for any device not presenting a compliant MDM certificate.

Evidence: BEFORE quarantining, capture MDM enrollment records showing device patch level, last check-in timestamp, and enrolled app list. Export MDM compliance reports in PDF/CSV for chain of custody. Document the specific Android Security Patch Level string (e.g., '2021-04-05') from the device Settings > Security screen or MDM telemetry — this string is the primary indicator of Mali GPU driver vulnerability exposure. If accessible, pull device ADB bug report (`adb bugreport`) to preserve current process list and installed package manifest before network isolation alters device state.

Step 2: Detection — Query MDM/UEM platform (e.g., Intune, Jamf, VMware Workspace ONE) for enrolled Android devices with security patch level < 2021-06-01. For unmanaged devices, request self-attestation. Review app installation logs for any of the 50+ flagged applications — specific package names require validation from the BleepingComputer source URL or Google Play security advisory once confirmed. Monitor for anomalous WhatsApp session activity including simultaneous logins from unknown devices via WhatsApp's linked devices feature. Watch for unexpected outbound data transfers from Android devices to unrecognized IP ranges. NOTE: No confirmed IOC hashes or package names are available from current source data; operators should monitor threat intelligence feeds (CISA, VirusTotal, Threat Intelligence Platform of record) for package name and hash releases as this campaign is publicly reported.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis; CSF [DE] — Monitor, detect, analyze, correlate, triage adverse events

Controls: NIST SI-4 (System Monitoring) — monitor for anomalous WhatsApp session replication and outbound C2 traffic from Android endpoints, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review MDM app installation logs for trojanized Play Store packages, NIST IR-5 (Incident Monitoring) — track and document each identified vulnerable device as an incident record, NIST SI-5 (Security Alerts, Advisories, and Directives) — ingest CISA and Google Play Security advisories for NoVoice package name and hash releases, CIS 8.2 (Collect Audit Logs) — ensure MDM audit logs covering app installs and patch compliance are retained and searchable, CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without SIEM: query Microsoft Intune via Graph API using PowerShell — `Get-MgDeviceManagementManagedDevice | Where-Object {$_.operatingSystem -eq 'Android' -and $_.osVersion -lt '2021-06-01'}` — and export to CSV for manual triage. For WhatsApp session anomaly detection without EDR: instruct all users to navigate to WhatsApp > Linked Devices and screenshot the linked device list; flag any entry not recognized by the user as a known personal device. For outbound traffic monitoring on a budget: deploy a pfSense or OPNsense firewall with Suricata and load the Emerging Threats Mobile Malware ruleset (free); filter on Android device IP ranges for anomalous DNS lookups or TLS connections to non-whitelisted ASNs during off-hours.

Evidence: Query MDM for app installation history on all Android devices with patch level pre-June 2021, preserving the full package name list and installation timestamps. Capture WhatsApp Linked Devices screenshots or MDM app

usage logs showing WhatsApp session registration events — the NoVoice rootkit clones sessions by extracting WhatsApp session keys from the /data/data/com.whatsapp/ directory, so any secondary session registration on an unfamiliar device following the app install window is a primary indicator. Collect network flow logs (NetFlow or firewall logs) for Android device IP ranges, filtering on outbound connections established post-installation of any flagged app, particularly to non-Google, non-Meta ASNs. If available, export Google Play Protect scan history from device MDM telemetry noting any flagged or removed applications.

Step 3: Eradication — For devices on Android patch level May 2021 or earlier with confirmed or suspected infection, full factory reset is insufficient given reported kernel-level persistence; device replacement is the reported remediation path. For devices on current patch levels, remove any identified trojanized applications and apply all pending Android security updates immediately. Direct users to revoke all WhatsApp linked device sessions via WhatsApp > Linked Devices and re-register. Verify Google Play Protect is enabled and run a full scan.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication; CSF [RS] — Remove threat from environment, verify eradication

Controls: NIST SI-2 (Flaw Remediation) — apply current Android Security Bulletin patches; replace devices where Mali GPU driver patching is unachievable, NIST SI-3 (Malicious Code Protection) — verify Google Play Protect is active and has completed a full on-device scan post-app removal, NIST SI-7 (Software, Firmware, and Information Integrity) — verify OS integrity on replacement devices before re-enrollment, NIST IR-4 (Incident Handling) — execute eradication actions per documented incident handling procedures, CIS 2.3 (Address Unauthorized Software) — remove all identified trojanized applications; document package names and removal timestamps, CIS 7.3 (Perform Automated Operating System Patch Management) — enforce Android security update application immediately upon device re-enrollment, CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams without mobile forensics tooling: use ADB to enumerate installed packages on non-replaced devices before wiping — `adb shell pm list packages -f -i > installed_packages_$(date +%F).txt` — preserving installer source (com.android.vending = Play Store install). For WhatsApp session revocation verification without centralized monitoring: have users perform the linked devices revocation while on a screen-share call with IT, capturing confirmation screenshots for the incident record. For kernel-level persistence verification on devices being evaluated for replacement vs. reset: use `adb shell dmesg | grep -i 'mali\|gpu\|rootkit\|suspicious'` and capture output; any anomalous kernel module entries referencing the Mali GPU driver confirm replacement is required over reset.

Evidence: BEFORE device replacement or wipe, capture a full ADB bug report (`adb bugreport device_serial_YYYYMMDD.zip`) containing kernel logs (dmesg), running process list, and installed package manifest — this is the primary forensic record for the kernel-level Mali GPU driver exploitation. Preserve the /data/data/com.whatsapp/ directory structure reference (document inaccessible paths that would require root forensics) to support later determination of session key extraction scope. Screenshot or export WhatsApp Linked Devices list showing any attacker-controlled session registrations before revocation. Document the device IMEI, serial number, and last MDM check-in timestamp for chain-of-custody records.

Step 4: Recovery — Post-remediation, confirm Android security patch level is current (minimum: verify against current Android Security Bulletin at source.android.com/docs/security/bulletin). Re-enroll replaced devices through MDM before granting access to corporate resources. For accounts where WhatsApp session cloning may have occurred, treat the account as compromised: notify affected users, assess what business communications may have been exposed, and consider whether escalation to legal or compliance is warranted based on data sensitivity. Monitor MDM telemetry for re-infection indicators for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery; CSF [RC] — Execute recovery plan, restore systems, verify integrity, communicate

Controls: NIST IR-4 (Incident Handling) — verify recovery actions align with the documented incident response plan, NIST IR-6 (Incident Reporting) — notify affected users and escalate to legal/compliance if WhatsApp session cloning exposed regulated data (PII, PHI, financial communications), NIST SI-2 (Flaw Remediation) — verify current Android

Security Bulletin patch level on all re-enrolled devices before restoring access, NIST AU-11 (Audit Record Retention) — retain all MDM compliance logs, WhatsApp session records, and incident documentation per policy for post-incident review, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — update asset inventory with replacement device records and disposal of compromised hardware, CIS 6.1 (Establish an Access Granting Process) — re-grant corporate access only after MDM compliance policy confirms patch level and app inventory are clean, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA re-enrollment on corporate apps accessed from replacement devices

Compensating: For teams without automated MDM compliance gating: create a manual re-enrollment checklist requiring IT sign-off confirming: (1) Android Security Patch Level verified against current bulletin at source.android.com, (2) no flagged package names present in `adb shell pm list packages` output, (3) WhatsApp Linked Devices list shows only user-recognized sessions, and (4) Google Play Protect scan completed clean. Use a ticketing system entry per device as the access re-authorization record. For the 30-day monitoring period without SIEM: schedule weekly MDM compliance report exports and diff against baseline using a simple PowerShell or bash script comparing enrolled package lists.

Evidence: Preserve all MDM re-enrollment timestamps and compliance policy pass/fail records for each replacement device as evidence of recovery completion. Collect and retain WhatsApp Linked Devices screenshots post-revocation from all affected users, confirming no residual attacker-controlled sessions remain. For any user whose WhatsApp session may have been cloned, preserve a log of approximate session clone window (estimated from app installation timestamp to session revocation timestamp) to scope the potential data exposure period for legal and compliance review. Document Android Security Bulletin patch level confirmation for each re-enrolled device against the current bulletin reference.

Step 5: Post-Incident — This campaign exposes three concrete control gaps: (1) absence of enforced minimum Android patch level policy in MDM — implement a compliance policy that blocks network access for devices below a defined patch threshold; (2) use of WhatsApp or other consumer messaging applications for business communications without session monitoring or MDM-enforced app vetting — evaluate whether consumer messaging should be permitted for business use or replaced with enterprise-grade alternatives; (3) reliance on Google Play vetting as a sufficient security control — consider supplementing with a managed app allowlist and mobile threat defense (MTD) solution that performs on-device behavioral analysis independent of Play Protect.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity; CSF [GV, ID] — Lessons learned, update policies, improve detection, share intelligence

Controls: NIST IR-4 (Incident Handling) — conduct formal lessons-learned review and update incident handling procedures to address MDM patch enforcement gaps, NIST IR-8 (Incident Response Plan) — update the IR plan to include Android rootkit scenarios with kernel-level persistence requiring device replacement rather than reset, NIST SI-2 (Flaw Remediation) — codify mandatory Android patch level enforcement as a tracked compliance metric with defined remediation SLAs, NIST SI-4 (System Monitoring) — implement MDM-based behavioral alerting for anomalous WhatsApp session registrations and sideloaded or newly installed applications on managed Android devices, NIST CM-7 (Least Functionality) — enforce managed app allowlist via MDM to prevent installation of non-vetted applications on corporate or BYOD devices accessing corporate resources, CIS 2.1 (Establish and Maintain a Software Inventory) — maintain and enforce a vetted mobile app allowlist in MDM covering all devices with access to corporate data or messaging, CIS 2.2 (Ensure Authorized Software is Currently Supported) — remove authorization for any application not receiving active security updates from its developer, CIS 7.2 (Establish and Maintain a Remediation Process) — establish a documented mobile patch SLA: critical Android security bulletins patched within 30 days; devices unable to receive patches flagged for replacement, CIS 6.3 (Require MFA for Externally-Exposed Applications) — require MFA on all enterprise applications accessible from mobile devices, independent of the messaging platform used

Compensating: For teams without budget for a commercial MTD solution: deploy a free Mobile Threat Defense alternative using Google Play Protect's Advanced Protection Program (free for consumer accounts, Google Workspace for Enterprise includes enhanced Play Protect scanning) combined with an MDM compliance policy in Intune or Jamf that enforces minimum patch level and denies enrollment to rooted devices. For app allowlisting without commercial MTD: configure MDM-required apps and blocked apps lists natively in Intune (Android Enterprise) or Jamf — this is a

built-in feature requiring no additional license. To monitor for future WhatsApp session cloning campaigns without SIEM: write a Sigma rule targeting MDM event logs for new WhatsApp Linked Device registration events originating from non-enrolled device identifiers and feed it to any free log aggregator (ELK/OpenSearch).

Evidence: Aggregate and archive all incident documentation for lessons-learned input: MDM compliance query results, device quarantine records, app installation logs for flagged trojanized applications, WhatsApp linked device revocation screenshots, and the device replacement/disposal records. This documentation package should directly inform the three control gap remediations identified — use the MDM query results to quantify how many devices were non-compliant (gap 1 evidence), the WhatsApp session clone scope assessment to justify the consumer messaging policy review (gap 2 evidence), and the trojanized app installation records to support the Google Play vetting supplementation decision (gap 3 evidence). Retain for a minimum period consistent with your data retention policy and any applicable breach notification regulatory requirements.

Detection Guidance

Primary detection vector is MDM/UEM patch-level inventory query: filter enrolled Android devices with security patch date <= 2021-05-01. Secondary detection: review app installation history for sideloaded or Play-sourced applications installed in the campaign's active window; specific package names and hashes are not confirmed in current source data and must be sourced from a validated threat intelligence feed or vendor advisory when available. Behavioral indicators include: (1) unexpected WhatsApp linked device sessions appearing for user accounts, detectable via user notification and IT-assisted review of Linked Devices list; (2) anomalous outbound traffic volumes from Android devices to non-whitelisted IPs, particularly on ports associated with encrypted C2 (T1437); (3) MDM reporting device integrity failures, rooted device flags, or system library modification alerts (T1628, T1577). For organizations with a Mobile Threat Defense solution, enable alerts for privilege escalation events, kernel exploit indicators, and unauthorized system library modifications. No confirmed IOC hashes, domains, or IP addresses are available from current source data at this time; treat any IOCs published by secondary outlets as unverified until cross-referenced with Google Threat Intelligence, CISA, or a primary research report.

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No confirmed IOCs available`	Source data contains no verified hashes, domains, IP addresses, or package names. Source quality score is 0.56. IOCs from secondary outlets (BleepingComputer, Malwarebytes blog) should be treated as unverified until cross-referenced with Android Security Bulletins, Google Threat Intelligence, or CISA advisories. Update this field when primary-source IOC data is confirmed.	LOW

Framework Mappings

MITRE-ATTACK

- **T1628** — Hide Artifacts

- **T1533** — Data from Local System
- **T1521** — Encrypted Channel
- **T1553** — Subvert Trust Controls
- **T1627** — Execution Guardrails
- **T1577** — Compromise Application Executable
- **T1603** — Scheduled Task/Job
- **T1475**
- **T1422** — System Network Configuration Discovery
- **T1624** — Event Triggered Execution
- **T1406** — Obfuscated Files or Information
- **T1437** — Application Layer Protocol
- **T1636** — Protected User Data
- **T1430** — Location Tracking
- **T1409** — Stored Application Data
- **T1635** — Steal Application Access Token
- **T1512** — Video Capture
- **T1629.003** — Disable or Modify Tools
- **T1407** — Download New Code at Runtime

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A08:2021** — Software and Data Integrity Failures

NIST-800-53R5

- **AC-6** — Least Privilege
- **SI-16** — Memory Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **AC-3** — Access Enforcement
- **SC-13** — Cryptographic Protection
- **SI-4** — System Monitoring

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **3.3** — Configure Data Access Control Lists
- **7.3** — Perform Automated Operating System Patch Management

- **7.4** — Perform Automated Application Patch Management
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography
- **A.5.23** — Information security for use of cloud services

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1628	Hide Artifacts	Defense-Evasion
T1533	Data from Local System	Collection
T1521	Encrypted Channel	Command-And-Control
T1553	Subvert Trust Controls	Defense-Evasion
T1627	Execution Guardrails	Defense-Evasion
T1577	Compromise Application Executable	Persistence
T1603	Scheduled Task/Job	Execution
T1475		
T1422	System Network Configuration Discovery	Discovery
T1624	Event Triggered Execution	Persistence
T1406	Obfuscated Files or Information	Defense-Evasion
T1437	Application Layer Protocol	Command-And-Control
T1636	Protected User Data	Collection
T1430	Location Tracking	Collection
T1409	Stored Application Data	Collection
T1635	Steal Application Access Token	Credential-Access

Technique ID	Technique Name	Tactic
T1512	Video Capture	Collection
T1629.003	Disable or Modify Tools	Defense-Evasion
T1407	Download New Code at Runtime	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/novoice-android-malw...	T3
Google patches 107 Android flaws, including two being actively ...	https://www.malwarebytes.com/blog/news/2025/12/google-patches-107-a...	T3
WhatsApp Confirms Update After Google Issues 'Attack Surface ...	https://www.forbes.com/sites/zakdoffman/2026/01/26/google-issues-wh...	T3
Look What You Made Us Patch: 2025 Zero-Days in Review	https://cloud.google.com/blog/topics/threat-intelligence/2025-zero-...	T3
Android's Latest Security Update Patches Spyware-Exploited Mali ...	https://www.bitdefender.com/en-us/blog/hotforsecurity/androids-late...	T3

Generated 2026-04-02 06:12 UTC by TJS Security Command Center