INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:34 UTC

Konni APT Turns Victims Into Vectors: KakaoTalk Abuse Extends North Korean Espionage Reach

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0036
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	KakaoTalk (desktop, Windows), Windows OS (LNK/shortcut execution, scheduled tasks), Android (remote wipe via stolen Google credentials, referenced from prior November 2025 campaign)
Published	2026-03-17

Executive Summary

The North Korean Konni APT group is running a targeted espionage campaign that compromises Windows systems via spear-phishing, then abuses victims' active KakaoTalk desktop sessions to spread malware to their contact lists, enabling attackers to reach secondary victims through compromised trusted contacts. Affected organizations face risks of credential theft, persistent backdoor access, and secondary compromise of colleagues who receive malicious files from a known, trusted contact. The campaign's multi-RAT deployment and long-dwell design indicate intelligence collection objectives, with a related component enabling remote wipe of Android devices via stolen Google credentials.

Technical Analysis

Konni APT delivers spear-phishing emails (T1566.001) themed around North Korean human rights content. The initial payload is a Windows LNK/shortcut file (T1204.002) that executes to deploy EndRAT, a newly identified AutoIt-based remote access trojan (T1059.010). Persistence is established via scheduled tasks (T1053.005) and potentially security support provider abuse (T1547.005). Once the host is compromised, the actor abuses the victim's live KakaoTalk desktop session (T1534, Internal Spearphishing) to distribute malicious ZIP archives to the victim's contact list, bypassing sender-reputation controls. High-value targets receive layered RAT deployments: EndRAT, RftRAT, and Remcos, indicating a resilience-focused strategy designed for long dwell time. The actor collects local data (T1005), captures keystrokes and screenshots (T1056, T1113), archives exfiltration packages (T1560), and exfiltrates over standard application-layer protocols (T1071, T1041). A

related November 2025 component used stolen Google credentials (T1078) to enable remote wipe of Android devices via Google's Find My Device functionality. Relevant CWEs: CWE-693 (Protection Mechanism Failure, trust-based delivery bypasses reputation filters) and CWE-494 (Download of Code Without Integrity Check, AutoIt-based payload delivery). No CVE identifiers are associated with this campaign; exploitation relies on user execution and legitimate application abuse, not unpatched vulnerabilities. No vendor patch is applicable; remediation is detection and configuration-based.

Action Checklist

1. Step 1, Immediate: Block execution of LNK files delivered via email attachments at the mail gateway and endpoint; enforce rules preventing LNK/shortcut execution from user download directories and temp paths.
2. Step 2, Immediate: Alert users, particularly those with Korean-language contacts or North Korea-related work context, not to open unsolicited ZIP files received via KakaoTalk, even from known contacts, until the sender is verbally confirmed.
3. Step 3, Detection: Hunt endpoint telemetry for AutoIt interpreter (AutoIt3.exe) executing from non-standard paths, LNK files spawning cmd.exe or powershell.exe, and scheduled task creation by non-administrative users (Event ID 4698).
4. Step 4, Detection: Review KakaoTalk desktop process activity on endpoints; look for KakaoTalk spawning child processes, accessing the filesystem outside its normal profile directories, or making outbound connections to atypical destinations.
5. Step 5, Assessment: Inventory endpoints running KakaoTalk desktop (Windows) and identify users with Google accounts linked to Android devices; prioritize those users for credential review and session audit.
6. Step 6, Credential: Force re-authentication and review active sessions for Google accounts belonging to any user who has opened a suspicious attachment in the past 90 days; check Google account security activity for unauthorized Find My Device access.
7. Step 7, Communication: Notify security-aware users in affected populations (Korean-language communicators, human rights or policy researchers, Korea-region business contacts) with specific guidance on the KakaoTalk propagation vector.
8. Step 8, Long-term: Evaluate whether KakaoTalk desktop is a business-required application; if not, remove or restrict. If required, isolate to a controlled segment and enforce application allowlisting around its process tree.
9. Step 9, Long-term: Map your detection coverage against the full MITRE technique set for this campaign (T1566.001, T1204.002, T1059.010, T1053.005, T1534, T1071, T1041, T1078, T1547.005) and close gaps in your SIEM or EDR rule set.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO/incident response leadership and consider external IR engagement if more than 5 endpoints show evidence of AutoIt execution, KakaoTalk process abuse, or scheduled task creation by non-admin users; or if any user with high-value role (executive, researcher, policy advisor) reports opening a suspicious KakaoTalk attachment.

Recovery Notes	Post-containment: (1) Conduct password audits and session reviews for all flagged users, ensuring no persistent backdoors remain via compromised credentials or scheduled tasks; (2) implement detection rules for future KakaoTalk abuse and monitor for 60 days; (3) perform forensic analysis on affected endpoints to confirm malware removal and absence of secondary implants (e.g., AutoIt-compiled payloads, LNK shortcuts in startup folders); (4) brief leadership on user awareness effectiveness and adjust phishing training based on campaign success metrics.
Forensic Artifacts	Windows Event Log: Security (4688 process creation, 4624 logon, 4698 scheduled task), System (service installation), Application (KakaoTalk logs if present) | Sysmon logs: Event ID 1 (process creation), Event ID 3 (network connection), Event ID 11 (file creation), Event ID 12-13 (registry modification) | File system artifacts: %USERPROFILE%\Downloads (malicious ZIP/LNK files), %TEMP% (extracted AutoIt scripts), NTFS MFT and UsnJournal for timeline reconstruction | Registry hives: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run (persistence mechanisms), HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services (scheduled tasks), HKEY_CURRENT_USER\Software\Kakao (KakaoTalk configuration/injection points) | Network artifacts: DNS query logs (C2 domain resolution), firewall logs (KakaoTalk outbound connections to suspicious IPs), PCAP of KakaoTalk process traffic, Google Workspace audit logs (Find My Device access, session activity for linked accounts)

Per-Action IR Details

Step 1, Immediate: Block execution of LNK files delivered via email attachments at the mail gateway and endpoint; enforce rules preventing LNK/shortcut execution from user download directories and temp paths.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase — preventive controls)

Controls: NIST 800-53 CA-7 (continuous monitoring), NIST 800-53 SI-4 (information system monitoring), CIS Controls 6.2 (application allow listing)

Compensating: Use Windows AppLocker or Software Restriction Policy to block .lnk execution from %USERPROFILE%\Downloads and %TEMP%; alternatively, use Autoruns (Sysinternals) to audit and disable shell folder shortcuts. For mail gateways without native LNK filtering, configure Exchange transport rules to reject messages with .lnk attachments (PowerShell: Set-TransportRule -Identity 'Block LNK' -AttachmentHasExecutableContent $true).

Evidence: Before enforcement: capture baseline of legitimate .lnk usage via Event ID 4688 (process creation) filtered for lnk parent processes; document any business-critical LNK-based workflows. Preserve Windows Event ID 4688 and Sysmon Event ID 1 logs for 30 days post-deployment to validate no legitimate processes are blocked.

Step 2, Immediate: Alert users, particularly those with Korean-language contacts or North Korea-related work context, not to open unsolicited ZIP files received via KakaoTalk, even from known contacts, until the sender is verbally confirmed.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (user awareness and training)

Controls: NIST 800-53 AT-2 (security awareness training), NIST 800-53 AT-3 (security awareness training effectiveness), CIS Controls 17.7 (user awareness and training)

Compensating: Distribute phishing alert via email, Teams, or Slack with visual example of the KakaoTalk attack chain (spear-phish → ZIP → LNK → AutoIt). Include escalation path: suspicious files → CISO or security@[company]. No enterprise tool required; craft message in 15 minutes referencing the Konni campaign public advisories.

Evidence: Document the alert distribution date, list of recipients by department/role, and track user inquiries about suspicious KakaoTalk files via helpdesk tickets; correlate with subsequent Step 3 detection hits to measure user response effectiveness.

Step 3, Detection: Hunt endpoint telemetry for AutoIt interpreter (AutoIt3.exe) executing from non-standard paths, LNK files spawning cmd.exe or powershell.exe, and scheduled task creation by non-administrative users (Event ID 4698).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (detection and analysis — indicators of compromise)

Controls: NIST 800-53 SI-4 (information system monitoring), NIST 800-53 AU-12 (audit generation), CIS Controls 6.4 (advanced system hardening)

Compensating: Without EDR: enable Sysmon (Event ID 1 for process creation, Event ID 11 for file operations) and Windows Event Log 4688. Query manually using wevtutil or PowerShell Get-WinEvent for: (ProcessName='AutoIt3.exe' AND NOT Path LIKE 'C:\Program Files%') OR (ParentImage LIKE '%lnk%' AND (CommandLine LIKE '%cmd.exe%' OR CommandLine LIKE '%powershell.exe%')) OR (Event ID 4698 AND NOT User LIKE '%SYSTEM%' AND NOT User LIKE '%ADMIN%'). Export to CSV for manual review.

Evidence: Preserve: Windows Event Log System (4698 scheduled task creation), Security (4688 process creation if enabled), Application logs; Sysmon logs (if deployed); the actual .lnk files and any extracted AutoIt scripts found in %TEMP% or %USERPROFILE%\Downloads; memory dumps of AutoIt3.exe if running; process tree screenshots or autoruns output showing parent-child relationships.

Step 4, Detection: Review KakaoTalk desktop process activity on endpoints; look for KakaoTalk spawning child processes, accessing the filesystem outside its normal profile directories, or making outbound connections to atypical destinations.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (anomaly detection and baselining)

Controls: NIST 800-53 SI-4 (system monitoring), NIST 800-53 CA-7 (continuous monitoring), CIS Controls 13.5 (network segmentation)

Compensating: Without EDR: enable Sysmon Event ID 1 (process creation), Event ID 3 (network connection), and Event ID 11 (file creation). Query for parent process 'KakaoTalk.exe' spawning child processes (excluding normal child processes like updates); use netstat -anbo or Get-NetTCPConnection -OwningProcess (KakaoTalk PID) to capture outbound connections, then cross-reference IPs against threat intelligence feeds (AbuseIPDB, VirusTotal IP reputation). KakaoTalk normal profile directories: %APPDATA%\Kakao\KakaoTalk; alert on writes outside this path.

Evidence: Preserve: Sysmon logs (all events for KakaoTalk process ID for 7 days prior); full network packet captures (PCAP) of KakaoTalk outbound traffic via tcpdump or Wireshark; registry hives (HKEY_CURRENT_USER\Software\Kakao) for any injected keys; file system timeline (MFT, UsnJournal) showing file creation/modification outside normal KakaoTalk directories; parent process tree and command line arguments for any child processes.

Step 5, Assessment: Inventory endpoints running KakaoTalk desktop (Windows) and identify users with Google accounts linked to Android devices; prioritize those users for credential review and session audit.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (prioritization of incidents based on impact assessment)

Controls: NIST 800-53 IA-4 (identifier management), NIST 800-53 AC-2 (account management), CIS Controls 5.2 (account inventory)

Compensating: Without enterprise asset management: use WMI queries via PowerShell (Get-WmiObject Win32_Process | Where {$_.Name -eq 'KakaoTalk.exe'}) or Sysmon event logs to list endpoints with KakaoTalk; query Active Directory for user UPN and cross-reference against mobile device inventory (MDM, if present) or ask users directly via survey. Create a spreadsheet of (User, Endpoint, KakaoTalk version, Google Account linked to Android). Use this list to manually schedule credential audits.

Evidence: Preserve: baseline inventory of KakaoTalk installations (hostname, user, installation date, version); list of users with linked Google accounts (from directory or user survey); screenshots or exports of users' Android device enrollment records if MDM is present.

Step 6, Credential: Force re-authentication and review active sessions for Google accounts belonging to any user who has opened a suspicious attachment in the past 90 days; check Google account security activity for unauthorized Find My Device access.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (containment — stopping the attack). Also: NIST 800-63B (authentication and lifecycle management).

Controls: NIST 800-53 IA-2 (authentication), NIST 800-53 IA-4 (identifier management), NIST 800-53 AC-11 (session lock), CIS Controls 5.6 (access control review)

Compensating: Without Azure AD or SSO: force password reset via Active Directory (ldp.exe or PowerShell Set-ADAccountPassword) for flagged users. For Google account review: access Google Admin Console (if organization uses Google Workspace) and check Security > Your devices > Find My Device logs for suspicious device location requests. For personal Google accounts: send users a link to myaccount.google.com/security-checkup and ask them to review active sessions (Security > Your devices) and disable Find My Device access if unauthorized. Instruct users to sign out all sessions on Google Account and re-authenticate only on known devices.

Evidence: Preserve: before password resets, export Active Directory login history (Event ID 4624) for past 90 days; screenshots or logs of Google Admin Console Find My Device activity; list of suspended/reset accounts with timestamps; Google Workspace audit logs showing account activity and sessions (download via Admin Console > Reports > Audit and investigation > Google Account, filter by date range).

Step 7, Communication: Notify security-aware users in affected populations (Korean-language communicators, human rights or policy researchers, Korea-region business contacts) with specific guidance on the KakaoTalk propagation vector.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 and §4.4 (communication and disclosure)

Controls: NIST 800-53 AT-1 (security awareness policy), NIST 800-53 IR-4 (incident handling), CIS Controls 17.7 (user awareness)

Compensating: Send targeted email or in-person briefing to identified high-risk user populations. Include: (1) threat description (Konni APT, KakaoTalk abuse, contact propagation), (2) technical indicators (LNK files in ZIP, AutoIt execution), (3) user actions (do not open unsolicited ZIP from KakaoTalk; verify sender via phone call; report to security@[company]), (4) response steps if they believe they were targeted (change password, audit Google account, run malware scan, contact IR team). Provide helpdesk contact and 24-hour escalation number for immediate concerns.

Evidence: Document: date of notification, recipient list by role/department, communication method (email/in-person), content delivered, any user inquiries or reported suspicious activity within 7 days post-notification. Track helpdesk ticket volume for 'suspicious KakaoTalk attachment' queries as a metric of campaign reach.

Step 8, Long-term: Evaluate whether KakaoTalk desktop is a business-required application; if not, remove or restrict. If required, isolate to a controlled segment and enforce application allow listing around its process tree.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 (eradication); also 800-53 CM-2 (baseline configuration management).

Controls: NIST 800-53 CM-2 (baseline configuration management), NIST 800-53 CM-7 (least functionality), CIS Controls 6.2 (application allow listing), CIS Controls 13.1 (network segmentation — isolation of high-risk systems)

Compensating: Survey business units on KakaoTalk usage; if not critical, uninstall via Group Policy (Computer Configuration > Software Installation or SCCM). If required: (1) Create an isolated network segment (VLAN) for KakaoTalk users only; (2) apply AppLocker rules to allow only signed KakaoTalk binaries and approved child processes (e.g., exclude cmd.exe, powershell.exe, wscript.exe spawning from KakaoTalk); (3) disable KakaoTalk auto-update to enforce manual updates only; (4) run KakaoTalk in a non-admin context by default (enforced via Group Policy Restricted Groups or scheduled task execution context).

Evidence: Preserve: baseline configuration of KakaoTalk (version, installation location, allowed parent/child processes, network destinations) before and after policy deployment; audit logs showing policy application to

endpoints; post-deployment scan results confirming non-compliant installations removed; list of approved child processes with justification.

Step 9, Long-term: Map your detection coverage against the full MITRE technique set for this campaign (T1566.001, T1204.002, T1059.010, T1053.005, T1534, T1071, T1041, T1078, T1547.005) and close gaps in your SIEM or EDR rule set.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 (post-incident activities — lessons learned and detection engineering).

Controls: NIST 800-53 IR-4 (incident handling), NIST 800-53 CA-7 (continuous monitoring), NIST 800-53 SI-4 (information system monitoring), CIS Controls 8.9 (security event logging)

Compensating: Without EDR: manually create SIEM correlation rules using Sysmon/Windows Event Logs. Map to MITRE techniques: T1566.001 (spear-phishing attachment) → log email gateway rejections + Event ID 4688 .lnk execution attempts; T1204.002 (user execution of malicious file) → Event ID 4688 .lnk or AutoIt3.exe spawning; T1059.010 (PowerShell command-line execution) → Event ID 4688 or PowerShell ScriptBlockLogging (Event ID 4104); T1053.005 (scheduled task creation) → Event ID 4698; T1534 (internal spear-phishing via compromised account) → mail gateway logs for emails sent by internal users to external recipients (anomaly detection); T1071 (application layer protocol) → netstat logs of KakaoTalk.exe outbound connections; T1041 (exfiltration over C2) → DNS query logs or PCAP analysis for unknown domains; T1078 (valid accounts) → Event ID 4624 logons from unusual locations/times; T1547.005 (boot or logon autostart execution) → registry/Run keys and Task Scheduler entries. Document coverage gaps and create rules to fill them.

Evidence: Preserve: current SIEM/EDR rule set (export rules, queries, correlations); MITRE technique mapping document (technique ID → detection rule); incident timeline showing which attacks succeeded due to detection gaps; post-remediation rule testing results (false positives, true positives) over 30-day validation period.

Detection Guidance

Primary behavioral indicators: (1) LNK file execution spawning cmd.exe, wscript.exe, or powershell.exe from user profile or temp directories, look for process creation events where parent is explorer.exe and grandchild is a shell interpreter launching from %TEMP%, %APPDATA%, or %USERPROFILE%\Downloads. (2) AutoIt3.exe executing from non-standard paths or with obfuscated script arguments (T1027). (3) Scheduled task creation (Windows Event ID 4698) by non-admin users, particularly tasks with randomized names or system-path executables. (4) KakaoTalk desktop process (KakaoTalk.exe) spawning child processes or accessing file paths outside its normal AppData directory. (5) Outbound C2 traffic: look for AutoIt-based processes or Remcos-associated processes making HTTP/S connections to low-reputation or newly registered domains. (6) Data staging: archive creation (ZIP) in user temp directories, followed by outbound file transfer activity (T1560, T1041). For Google credential abuse: review Google Workspace or personal account audit logs for Find My Device activations or remote wipe commands issued from unfamiliar IP addresses or outside normal user geography. SIEM query focus areas: process lineage from LNK execution, scheduled task creation by standard users, KakaoTalk child process anomalies, and AutoIt interpreter invocations. EDR behavioral rules should flag LNK-to-shell-interpreter chains and AutoIt execution from download paths. Important: Specific IOC hashes, domains, and IPs are not available from the current T3 sources. Before implementing hash or IP-based blocking rules, enrich this intelligence with a primary threat intelligence feed (CISA, vendor APT report, or commercial threat feed). Behavioral detection rules (process lineage, scheduled task anomalies, KakaoTalk child process spawning) are actionable immediately without IOC confirmation.

Indicators of Compromise

Type	Value	Context	Confidence
FILE-TYPE	`LNK/Windows Shortcut`	Initial access payload delivered via spear-phishing email; executes to deploy EndRAT	HIGH
FILE-TYPE	`ZIP archive`	Malicious ZIP files distributed via compromised victim's KakaoTalk desktop session to contact list	HIGH
PROCESS	`AutoIt3.exe`	EndRAT is AutoIt-based; execution of AutoIt interpreter from non-standard or user-writable paths is a behavioral indicator	HIGH
PROCESS	`KakaoTalk.exe spawning child processes`	Anomalous KakaoTalk child process activity indicates active session abuse for internal propagation (T1534)	MEDIUM
MALWARE-FAMILY	`EndRAT`	Newly identified AutoIt-based RAT; primary payload in this campaign	HIGH
MALWARE-FAMILY	`RftRAT`	Secondary RAT deployed on high-value hosts for resilience	HIGH
MALWARE-FAMILY	`Remcos`	Commercial RAT deployed on high-value hosts alongside EndRAT and RftRAT	HIGH
TECHNIQUE	`Google Find My Device remote wipe via stolen credentials`	Related November 2025 campaign component; stolen Google credentials used to enable Android remote wipe	MEDIUM
NOTE	`No confirmed IOCs extracted`	The source data provided does not include specific file hashes, C2 IP addresses, or domains attributed to this campaign. The source quality score is 0.712 and all URLs are Tier 3. IOCs should be sourced directly from a primary threat intelligence report or vendor analysis of this campaign before operationalizing. Do not treat absence of IOCs here as confirmation that none exist.	LOW
DOMAIN	`Not available in current source data`	C2 infrastructure for EndRAT, RftRAT, and Remcos not published in T3 sources at time of configuration. Monitor Genians and threat intel feeds for updates.	LOW

Type	Value	Context	Confidence
HASH	`Not available in current source data`	File hashes for EndRAT, RftRAT, and Remcos samples not extracted from available sources. Check Genians blog (genians.co.kr/en/blog/threat_intelligence /kakaotalk) for sample hashes.	LOW
URL	`Not available in current source data`	Payload delivery URLs not published in available T3 sources. Pending full technical report release.	LOW

Framework Mappings

MITRE-ATTACK

- **T1005** — Data from Local System
- **T1056** — Input Capture
- **T1027** — Obfuscated Files or Information
- **T1053.005** — Scheduled Task
- **T1041** — Exfiltration Over C2 Channel
- **T1560** — Archive Collected Data
- **T1059.010** — AutoHotKey & AutoIT
- **T1071** — Application Layer Protocol
- **T1078** — Valid Accounts
- **T1204.002** — Malicious File
- **T1105** — Ingress Tool Transfer
- **T1091** — Replication Through Removable Media
- **T1021** — Remote Services
- **T1547.005** — Security Support Provider
- **T1534** — Internal Spearphishing
- **T1113** — Screen Capture
- **T1566.001** — Spearphishing Attachment

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

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

CIS-V8

- **2.5**
- **2.6**
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

SOC2-TSC

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1005	Data from Local System	Collection
T1056	Input Capture	Collection
T1027	Obfuscated Files or Information	Defense-Evasion
T1053.005	Scheduled Task	Execution
T1041	Exfiltration Over C2 Channel	Exfiltration
T1560	Archive Collected Data	Collection
T1059.010	AutoHotKey & AutoIT	Execution
T1071	Application Layer Protocol	Command-And-Control

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1204.002	Malicious File	Execution
T1105	Ingress Tool Transfer	Command-And-Control
T1091	Replication Through Removable Media	Lateral-Movement
T1021	Remote Services	Lateral-Movement
T1547.005	Security Support Provider	Persistence
T1534	Internal Spearphishing	Lateral-Movement
T1113	Screen Capture	Collection
T1566.001	Spearphishing Attachment	Initial-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/konni-deploys-endrat-through-spea...	T3
North Korea–linked hackers spread KakaoTalk malware ...	https://biz.chosun.com/en/en-it/2026/03/16/BT35MRSJKNFOXESEWOH3RTEBBM/	T3
NK hackers hijack Google, KakaoTalk accounts to control ...	https://www.koreaherald.com/article/10612803	T3
North Korean hackers exploit Google's safety tools for remote ...	https://www.csoonline.com/article/4088037/north-korean-hackers-expl...	T3
Konni APT Hijacks KakaoTalk Accounts to Spread Malware ...	https://cybersecuritynews.com/konni-apt-hijacks-kakaotalk-accounts/	T3
Konni APT Hijacks KakaoTalk Accounts to Spread Malware in Multi ...	https://cybersecuritynews.com/konni-apt-hijacks-kakaotalk-accounts/...	T3
KaKaoTalkPC Messenger Remote Code Execution Vulnerability	https://fortiguard.fortinet.com/encyclopedia/endpoint-vuln/2019	T3

Source	URL	Tier
Remote code execution vulnerability exists in KaKaoTalk... - GitHub	https://github.com/advisories/GHSA-cvfh-r7mx-qwxc	T3
LNK remote code execution vulnerability: June 13, 2017	https://support.microsoft.com/en-au/topic/lnk-remote-code-execution...	T1
Analysis of the Spear-Phishing and KakaoTalk-Linked Threat ...	https://www.genians.co.kr/en/blog/threat_intelligence/kakaotalk	T3
State-Sponsored Remote Wipe Tactics Targeting Android Devices	https://www.genians.co.kr/en/blog/threat_intelligence/android	T3
KakaoTalk: A critical vulnerability for remote threat actors - LinkedIn	https://www.linkedin.com/posts/cybersecurity-news_1-click-exploit-i...	T3

Generated 2026-03-29 18:34 UTC by TJS Security Command Center