INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-06 18:18 UTC

DPRK-Linked Kimsuky and ScarCruft Abuse GitHub and Dropbox as C2 in South Korea Campaigns

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0153
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows (LNK, PowerShell, Scheduled Tasks), Hangul Word Processor (HWP), GitHub (abused as C2 channel), Dropbox (abused as C2 channel)
Published	2026-04-06T12:24:00
Discovery Source	Rss

Executive Summary

North Korean threat actors Kimsuky and ScarCruft are actively targeting South Korean organizations through phishing campaigns that use legitimate cloud services, GitHub and Dropbox, as command-and-control channels, making malicious traffic difficult to distinguish from normal business activity. The campaigns rely on social engineering via Hangul Word Processor documents and Windows shortcut files rather than software vulnerabilities, meaning no patch exists to block initial access. Organizations with South Korean operations, government ties, or defense-adjacent work face elevated risk; existing signature-based and reputation-based security controls are likely insufficient against this approach.

Technical Analysis

Three overlapping attack chains attributed to Kimsuky and ScarCruft initiate via malicious LNK files delivered through spearphishing attachments (T1566.001, T1204.002). Lure documents use Hangul Word Processor (HWP) format, consistent with South Korea-targeted DPRK tradecraft. Post-execution, the chains rely on Windows-native tooling, PowerShell (T1059.001), VBScript (T1059.005), and scheduled tasks (T1053.005), to minimize forensic footprint (living-off-the-land). C2 traffic routes through GitHub repositories (T1102.002) and Dropbox (T1102), blending with legitimate platform traffic to bypass network-layer controls. Additional techniques include obfuscation (T1027), ingress tool transfer (T1105), data collection and archiving (T1560), masquerading (T1036), DLL hijacking (T1574.002), LOLBin abuse (T1218), hidden files (T1564.001), and

virtualization/sandbox evasion (T1497.001). No CVEs are associated with this activity. Relevant CWEs: CWE-601 (open redirect, abuse of legitimate services for C2), CWE-693 (protection mechanism failure against LotL), CWE-494 (download of code without integrity check). No patches apply; the attack surface is behavioral, not software-vulnerability-based. Technical detail confidence is moderate; validate against primary FortiGuard and Broadcom advisories before operationalizing.

Action Checklist

1. Step 1: Containment. Block outbound API calls and raw content requests to github.com and dropbox.com from endpoints and servers that have no documented business justification. Apply this at the proxy or firewall layer, scoped to unexpected or unapproved source systems. Do not apply a blanket block without first auditing legitimate GitHub/Dropbox use to avoid operational disruption.
2. Step 2: Detection. Search endpoint telemetry for LNK files executed from temp directories, email client process trees, or download folders (Event ID 4688, Sysmon Event ID 1). Hunt for PowerShell or WScript spawned by explorer.exe or Outlook with encoded command lines (Sysmon Event ID 1, Event ID 4104). Query proxy logs for outbound HTTPS to raw.githubusercontent.com or api.dropboxapi.com from non-developer workstations. Flag scheduled tasks created by PowerShell or WScript (Event ID 4698). Review HWP process execution chains for child processes.
3. Step 3: Eradication. Remove any scheduled tasks created outside change management processes on affected systems. Terminate and delete identified malicious LNK files, PowerShell scripts, and any dropped payloads. Revoke and rotate credentials for accounts active on systems showing C2 beaconing patterns. Remove attacker-controlled GitHub repositories or Dropbox resources used as staging if identified; report abuse to the platforms directly.
4. Step 4: Recovery. Validate that scheduled tasks are clean across affected hosts using 'schtasks /query' and endpoint telemetry. Confirm no residual beaconing to GitHub or Dropbox C2 endpoints by monitoring proxy logs for 72 hours post-remediation. Re-image endpoints where persistent access cannot be ruled out. Restore from known-good backups only after confirming backup integrity and confirming the backup predates initial compromise.
5. Step 5: Post-Incident. Audit detection coverage for LotL technique chains: PowerShell execution policy, script block logging (Event ID 4104), and process creation logging should be enabled and ingested by your SIEM. Evaluate whether your network controls distinguish sanctioned from unsanctioned cloud service usage; this campaign exploits the absence of that distinction. Review phishing simulation coverage for LNK-based lures and HWP files. Map control gaps to MITRE ATT&CK techniques T1102.002, T1059.001, T1053.005, and T1566.001 and document remediation actions in your risk register.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior IR leadership and legal/compliance immediately if proxy logs confirm successful data exfiltration (Dropbox upload API calls with non-trivial byte counts), if compromised accounts have access to sensitive research, government-contract, or personally identifiable data subject to breach notification obligations, or if the organization lacks the internal capability to perform memory forensics on hosts with confirmed C2 beaconing.

Recovery Notes	Re-image any endpoint where scheduled task persistence or secondary payloads cannot be conclusively ruled out — Kimsuky and ScarCruft are known to deploy multiple persistence mechanisms, and partial eradication of LNK or PowerShell stagers does not guarantee the absence of additional implants. Monitor proxy and DNS logs for outbound connections to GitHub and Dropbox from all internal endpoints for a minimum of 72 hours post-remediation, extending to 7 days if the dwell time prior to detection exceeded 48 hours. Restore affected systems from backups only after confirming via endpoint telemetry (Event ID 4688 timestamps and Prefetch file creation dates) that the backup image predates the earliest observed LNK execution or HWP child process spawn event.
Forensic Artifacts	Windows Prefetch files (%WINDIR%\Prefetch\) for LNK file execution and any spawned PowerShell or WScript processes — Kimsuky/ScarCruft LNK lures will leave execution traces here with timestamps that establish initial access timing | Scheduled task XML definitions in C:\Windows\System32\Tasks\ — ScarCruft and Kimsuky use schtasks for persistence; the XML will contain the encoded PowerShell command line used to beacon to GitHub or Dropbox C2 | PowerShell Script Block Logging events (Event ID 4104) in Microsoft-Windows-PowerShell/Operational — will contain decoded stager content including the raw.githubusercontent.com or api.dropboxapi.com URL and any downloaded payload code | Proxy or firewall logs showing outbound HTTPS connections to raw.githubusercontent.com and api.dropboxapi.com — HTTP method, URI path, user-agent string, and response byte size distinguish C2 tasking (GET of raw content) from legitimate developer traffic | HWP (Hangul Word Processor) process execution chain in Sysmon Event ID 1 logs — malicious HWP documents used in this campaign spawn child processes (powershell.exe, wscript.exe, cmd.exe) that are forensically captured as ParentImage=hwp.exe, which is not a normal parent process relationship in a clean environment

Per-Action IR Details

Step 1: Containment — Block outbound API calls and raw content requests to github.com and dropbox.com from endpoints and servers that have no documented business justification. Apply this at the proxy or firewall layer, scoped to unexpected or unapproved source systems. Do not apply a blanket block without first auditing legitimate GitHub/Dropbox use to avoid operational disruption.

NIST Phase: Containment

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

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

Compensating: On hosts without enterprise proxy visibility, deploy Sysmon with network connection logging (Event ID 3) and filter on DestinationHostname containing 'raw.githubusercontent.com' or 'api.dropboxapi.com'. Use Windows Firewall with Advanced Security via GPO or local policy to block outbound TCP 443 to specific IP ranges for these domains on non-approved endpoints. Generate the current block list with: `Resolve-DnsName raw.githubusercontent.com | Select-Object IPAddress` and `Resolve-DnsName api.dropboxapi.com | Select-Object IPAddress`, then add those IPs to a named firewall rule — noting DNS-resolved IPs may rotate and require periodic refresh.

Evidence: Before applying blocks, export proxy or firewall logs showing existing outbound connections to raw.githubusercontent.com and api.dropboxapi.com — capture source IP, user agent, URI path, HTTP method, and byte counts. Kimsuky/ScarCruft C2 via GitHub typically involves HTTP GET requests to raw content URLs containing encoded payloads or tasking instructions; Dropbox C2 uses the /2/files/download and /2/files/upload API endpoints. Preserve these logs to reconstruct staging and tasking timelines before blocking terminates the observable beacon pattern.

Step 2: Detection — Search endpoint telemetry for LNK files executed from temp directories, email client process trees, or download folders (Event ID 4688, Sysmon Event ID 1). Hunt for PowerShell or WScript spawned by explorer.exe or Outlook with encoded command lines (Sysmon Event ID 1, Event ID 4104). Query proxy logs for outbound HTTPS to raw.githubusercontent.com or api.dropboxapi.com from non-developer workstations. Flag scheduled tasks created by PowerShell or WScript (Event ID 4698). Review HWP process execution chains for child processes.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run the following targeted queries manually on affected hosts. For LNK execution: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688} | Where-Object {$_.Message -like '*.lnk*'}`. For PowerShell with encoded commands: `Get-WinEvent -LogName 'Microsoft-Windows-PowerShell/Operational' | Where-Object {$_.Id -eq 4104} | Where-Object {$_.Message -like '*-enc*' -or $_.Message -like '*EncodedCommand*'}`. For scheduled task creation by PowerShell or WScript: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4698}`. For HWP child process chains, query Sysmon Event ID 1 filtering on ParentImage containing 'hwp.exe' or 'Hwp.exe'. Deploy the public Sigma rule 'proc_creation_win_lnk_execution_from_non_standard_location' against collected Sysmon logs using sigmac to convert to PowerShell or grep-compatible format.

Evidence: Collect the following before triage decisions: (1) Prefetch files for LNK execution under %WINDIR%\Prefetch — filenames will reference the LNK and any spawned interpreter; (2) Windows Security Event ID 4688 and Sysmon Event ID 1 logs showing process lineage — specifically hwp.exe, outlook.exe, or explorer.exe spawning powershell.exe or wscript.exe; (3) PowerShell Script Block Logging (Event ID 4104) entries in Microsoft-Windows-PowerShell/Operational containing Base64-encoded strings characteristic of Kimsuky stagers; (4) Scheduled task XML definitions from C:\Windows\System32\Tasks\ for any tasks created within the suspected compromise window; (5) Proxy or DNS logs showing queries to raw.githubusercontent.com or api.dropboxapi.com correlated by source hostname to the endpoint under investigation.

Step 3: Eradication — Remove any scheduled tasks created outside change management processes on affected systems. Terminate and delete identified malicious LNK files, PowerShell scripts, and any dropped payloads. Revoke and rotate credentials for accounts active on systems showing C2 beaconing patterns. Remove attacker-controlled GitHub repositories or Dropbox resources used as staging if identified — report abuse to the platforms directly.

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 AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Enumerate and export all scheduled tasks before removal for forensic preservation: `schtasks /query /fo CSV /v > C:\IR\schtasks_snapshot_$(Get-Date -Format yyyyMMdd).csv`. Remove confirmed malicious tasks: `schtasks /delete /tn "" /f`. For LNK and dropped payload removal, use `Get-FileHash` on identified files before deletion to document IOC hashes for threat intel sharing. Force credential rotation for affected accounts via Active Directory: `Set-ADAccountPassword -Identity -Reset -NewPassword (Read-Host -AsSecureString)` and immediately set `ChangePasswordAtLogon = $true`. Submit the attacker-controlled GitHub repository URL to GitHub's abuse reporting portal at github.com/contact/report-abuse and Dropbox at dropbox.com/abuse — include the specific repository path or shared link URL identified during investigation.

Evidence: Before eradication actions, preserve forensic copies of: (1) The scheduled task XML from C:\Windows\System32\Tasks\ for each malicious task — this will contain the command line, trigger timing, and the account context used by Kimsuky/ScarCruft to maintain persistence; (2) The full LNK file binary including the target path, working directory, and any embedded command arguments — Kimsuky LNK files often contain multi-stage PowerShell stagers hidden in the arguments field; (3) Any PowerShell script files dropped to %TEMP%,

%APPDATA%, or user profile subdirectories; (4) A memory dump of any active PowerShell or WScript processes prior to termination using ProcDump: `procdump.exe -ma C:\IR\powershell_.dmp`; (5) Windows Security Event ID 4648 (Explicit Credential Use) and Event ID 4624 (Logon) logs for the compromised account to establish lateral movement scope before credential rotation.

Step 4: Recovery — Validate that scheduled tasks are clean across affected hosts using 'schtasks /query' and endpoint telemetry. Confirm no residual beaconing to GitHub or Dropbox C2 endpoints by monitoring proxy logs for 72 hours post-remediation. Re-image endpoints where persistent access cannot be ruled out. Restore from known-good backups only after confirming backup integrity and confirming the backup predates initial compromise.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-9 (System Backup), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For scheduled task validation across multiple hosts without enterprise tooling, run `Invoke-Command -ComputerName (Get-Content hostlist.txt) -ScriptBlock {schtasks /query /fo CSV /v}` and diff the output against your pre-incident baseline or the forensic snapshot taken during eradication. For 72-hour beacon monitoring without a SIEM, configure Windows Firewall auditing (`auditpol /set /subcategory:"Filtering Platform Connection" /success:enable /failure:enable`) and collect Security Event ID 5156 (network connection allowed) filtered on remote addresses resolving to GitHub or Dropbox IP ranges. For backup integrity validation, compute SHA-256 hashes of backup archives before restore and compare against stored checksums: `Get-FileHash -Algorithm SHA256 `.

Evidence: Before declaring recovery complete, document: (1) A clean schtasks export from each remediated host timestamped post-eradication, compared against the malicious task snapshot, confirming removal; (2) 72 hours of proxy or firewall logs showing zero outbound connections from remediated endpoints to raw.githubusercontent.com or api.dropboxapi.com — this rules out secondary persistence mechanisms not identified during eradication; (3) File system integrity verification of %WINDIR%\System32\Tasks\ using `Get-ChildItem` with creation timestamps to confirm no new tasks were added post-remediation; (4) Confirmation of the backup creation date against the earliest suspected compromise date derived from the LNK execution or HWP child process timestamps identified during detection.

Step 5: Post-Incident — Audit detection coverage for LotL technique chains: PowerShell execution policy, script block logging (Event ID 4104), and process creation logging should be enabled and ingested by your SIEM. Evaluate whether your network controls distinguish sanctioned from unsanctioned cloud service usage — this campaign exploits the absence of that distinction. Review phishing simulation coverage for LNK-based lures and HWP files. Map control gaps to MITRE ATT&CK techniques T1102.002, T1059.001, T1053.005, and T1566.001 and document remediation actions in your risk register.

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 AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), NIST SI-4 (System Monitoring), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: Verify PowerShell Script Block Logging is enabled via GPO or registry: `Set-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging' -Name 'EnableScriptBlockLogging' -Value 1`. Validate process creation auditing is active: `auditpol /get /subcategory:"Process Creation"` — should show Success enabled. For LNK-based phishing simulation coverage, use the GoPhish open-source framework with LNK attachment payloads to test user detection rates. Convert the MITRE ATT&CK technique mappings (T1102.002 — Web Service: Bidirectional Communication, T1059.001 — PowerShell, T1053.005 — Scheduled Task, T1566.001 — Spearphishing Attachment) to Sigma detection rules using the public SigmaHQ repository and deploy them against Sysmon and Windows Event Log sources. For HWP file handling, evaluate whether your organization requires the Hangul Word Processor and consider restricting it via AppLocker if not operationally required.

Evidence: Post-incident, compile the following for the lessons-learned record and risk register: (1) A gap analysis of which Sysmon Event IDs (1, 3, 11) and Windows Event IDs (4688, 4104, 4698) were logging and forwarding at time of compromise versus which were missing — this directly maps to the detection latency for this Kimsuky/ScarCruft campaign; (2) Proxy log evidence showing the duration of C2 beaconing to GitHub/Dropbox before detection, establishing dwell time specific to this incident; (3) A list of all endpoints that executed HWP files or LNK files during the compromise window, drawn from Prefetch and Event ID 4688 logs, to assess potential scope beyond confirmed victims; (4) Documentation of whether the attacker-controlled GitHub repository or Dropbox account was public or required authentication — this affects the fidelity of proxy-based detection going forward.

Detection Guidance

Primary behavioral indicators: LNK files executed from user-writable directories (Downloads, Temp, AppData) spawning PowerShell or WScript (Sysmon Event ID 1, parent-child process chain). PowerShell with Base64-encoded or heavily obfuscated command lines (Event ID 4104, Script Block Logging required). Scheduled task creation via PowerShell or WScript outside business hours or change windows (Event ID 4698/4702). Outbound HTTPS connections from non-developer endpoints to raw.githubusercontent.com, api.github.com, or api.dropboxapi.com, particularly with regular interval beaconing patterns consistent with C2 polling. HWP (Hangul Word Processor) files spawning child processes other than the HWP application itself. DLL side-loading indicators: unsigned DLLs loaded by legitimate Windows binaries from user-writable paths (Sysmon Event ID 7, ImageLoaded not signed by Microsoft). Sandbox/VM evasion activity: system enumeration commands (systeminfo, wmic) executed immediately after LNK execution before any payload action. Note: no confirmed IOC hashes or specific C2 repository URLs are available in the current source set. Validate against FortiGuard Labs and Broadcom Symantec advisories for any published IOC lists before deploying signature-based detections.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`raw.githubusercontent.com (attacker-controlled repositories — specific paths not confirmed in available sources)`	GitHub abused as C2 channel for command retrieval and data exfiltration (T1102.002). Specific repository URLs not available in current source set.	LOW
URL	`api.dropboxapi.com (attacker-controlled storage — specific paths not confirmed in available sources)`	Dropbox abused as C2 and staging channel (T1102). Specific endpoint paths not available in current source set.	LOW
DOMAIN	`No confirmed C2 domains available in current source set`	Source quality score 0.48. Validate against FortiGuard Labs (fortinet.com/blog/threat-research/dprk-related-campaigns-with-lnk-and-github-c2) and Broadcom advisories for published IOCs.	LOW

Framework Mappings

MITRE-ATTACK

- **T1102.002** — Bidirectional Communication
- **T1041** — Exfiltration Over C2 Channel
- **T1560** — Archive Collected Data
- **T1036** — Masquerading
- **T1105** — Ingress Tool Transfer
- **T1027** — Obfuscated Files or Information
- **T1574.002** — DLL Side-Loading
- **T1071.001** — Web Protocols
- **T1059.001** — PowerShell
- **T1053.005** — Scheduled Task
- **T1204.002** — Malicious File
- **T1059.005** — Visual Basic
- **T1497.001** — System Checks
- **T1102** — Web Service
- **T1218** — System Binary Proxy Execution
- **T1566.001** — Spearphishing Attachment
- **T1564.001** — Hidden Files and Directories

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **SI-3** — Malicious Code Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1102.002	Bidirectional Communication	Command-And-Control
T1041	Exfiltration Over C2 Channel	Exfiltration
T1560	Archive Collected Data	Collection
T1036	Masquerading	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1574.002	DLL Side-Loading	Persistence
T1071.001	Web Protocols	Command-And-Control
T1059.001	PowerShell	Execution
T1053.005	Scheduled Task	Execution
T1204.002	Malicious File	Execution
T1059.005	Visual Basic	Execution
T1497.001	System Checks	Defense-Evasion
T1102	Web Service	Command-And-Control
T1218	System Binary Proxy Execution	Defense-Evasion
T1566.001	Spearphishing Attachment	Initial-Access
T1564.001	Hidden Files and Directories	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/dprk-linked-hackers-use-github-as...	T3
DPRK-Related Campaigns with LNK and GitHub C2 | FortiGuard Labs	https://www.fortinet.com/blog/threat-research/dprk-related-campaign...	T3
Malicious LNK Delivery and GitHub-Based C2 Observed in New ...	https://www.broadcom.com/support/security-center/protection-bulleti...	T3
Malicious LNK files, GitHub leveraged in South Korea-targeted ...	https://www.scworld.com/brief/malicious-lnk-files-github-leveraged-...	T3
GitHub Abused As C2 Server In New North Korea-Related LNK ...	https://cyberpress.org/github-c2-in-lnk-phishing/	T3

Generated 2026-04-06 18:18 UTC by TJS Security Command Center