INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-21 18:37 UTC

Chinese APT Targets Indian Banking Sector and South Korean Policy Institutions with Dated Tactics

THREAT CAMPAIGN | MEDIUM | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0195
Type	Threat Campaign
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Indian banking sector (institutions unspecified); South Korean policy and government-adjacent organizations (unspecified)
Published	2026-04-21T08:00:00
Discovery Source	Rss

Executive Summary

A Chinese state-linked APT group is conducting active intelligence collection against Indian financial institutions and South Korean policy organizations, using dated tactics that suggest either a deliberate low-cost approach or an assessment that target defenses are weak. No specific institutions have been named and attribution to a specific APT group has not been confirmed. The primary business risk is unauthorized access to sensitive financial and policy data, with potential for follow-on espionage or disruption.

Technical Analysis

Source reporting (Dark Reading, T3) describes a Chinese state-linked APT campaign targeting Indian banking sector organizations and South Korean government-adjacent policy institutions. No CVEs, CWEs, or confirmed malware families are associated with this campaign in available reporting. MITRE ATT&CK techniques mapped from behavioral indicators include: T1566 (Phishing, likely initial access), T1078 (Valid Accounts, possible credential abuse), T1071 (Application Layer Protocol, C2 communication), T1027 (Obfuscated Files or Information), T1589 (Gather Victim Identity Information, reconnaissance), T1005 (Data from Local System, collection), and T1083 (File and Directory Discovery, collection). The campaign is characterized by reliance on outdated tooling. Specific group attribution (e.g., APT41, APT10, Mustang Panda) is not confirmed. Attribution confidence: low. Targeting scope confidence: medium. All source URLs for this item are T3 (secondary publications); no primary source corroboration from CISA, named vendor threat intelligence reports, or

government advisories is available. Technical specifics should be treated as unverified until primary source confirmation. CVSS scoring is not applicable to campaign-level threat activity; severity is assigned editorially based on target criticality and attack scope.

Action Checklist

1. Step 1: Scoping. Determine whether your organization operates in Indian banking or South Korean policy sectors, or maintains partnerships, data-sharing relationships, or network connectivity with organizations in those sectors. Expand monitoring posture if any nexus exists.
2. Step 2: Detection. Review email gateway logs for spear-phishing indicators (T1566): unexpected senders from free or lookalike domains targeting finance or policy staff. Check authentication logs for anomalous use of valid credentials (T1078): off-hours logins, impossible travel, or access from unexpected geolocations. Monitor outbound traffic for C2 patterns over standard application protocols (T1071): unusual HTTP/S, DNS, or SMTP traffic volumes to unfamiliar external destinations.
3. Step 3: Hardening. Enforce MFA on all externally facing systems and privileged accounts to reduce valid account abuse risk (T1078). Audit and remove unused or dormant accounts. Deploy or verify email security controls (SPF, DKIM, DMARC) to reduce phishing delivery success (T1566). Restrict file and directory enumeration permissions on sensitive systems (T1083, T1005).
4. Step 4: Threat Hunting. Run hunts for obfuscated script execution (T1027) in endpoint telemetry: PowerShell with encoded commands, unusual parent-child process chains, or living-off-the-land binaries used outside normal workflows. Cross-reference outbound connection destinations against known Chinese state-linked C2 infrastructure using your threat intelligence platform.
5. Step 5: Post-Incident Controls. Document gaps in visibility identified during hunting. If no SIEM coverage exists for the mapped ATT&CK techniques, prioritize detection rule development. Report any confirmed indicators to CISA (for US-nexus organizations) or the relevant national CERT. Contribute confirmed IOCs to your threat intelligence sharing community (ISAC, if applicable).

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if hunting identifies confirmed T1027 obfuscated execution or T1078 valid account abuse on systems handling sensitive financial data or policy documents, or if outbound connections to Chinese-attributed C2 infrastructure are confirmed — at that point this transitions from campaign awareness to active incident and triggers NIST IR-6 (Incident Reporting) obligations and potential sector-specific breach notification requirements (e.g., RBI guidelines for Indian banking entities, or FSC/KISA requirements for South Korean policy organizations).

Recovery Notes	If active compromise is confirmed during hunting, prioritize credential rotation for all accounts with access to financial or policy data stores before restoring affected systems, given the APT's focus on T1078 valid account abuse for persistence. Monitor re-imaged systems for 30 days post-recovery using Sysmon and PowerShell Script Block Logging, specifically watching for the same T1027 and T1071 patterns that may indicate the actor retained access through a secondary persistence mechanism (T1053 scheduled tasks or T1547 registry run keys) not identified during eradication. Given the intelligence collection focus of this campaign, verify that no sensitive financial or policy documents were staged in unusual temporary directories (C:\Users*\AppData\Local\Temp\ or C:\ProgramData\) prior to exfiltration, as T1005 (Data from Local System) and T1083 (File and Directory Discovery) were mapped in this advisory.
Forensic Artifacts	Email gateway logs with full SMTP envelope headers and attachment hashes for the 90 days preceding detection — specifically preserve any .doc/.xls/.pdf attachments delivered to finance or policy staff from external senders, as Chinese APT spear-phishing (T1566.001) in this campaign likely uses lure documents themed around Indian financial regulation or South Korean policy matters | Windows Security Event Log Event IDs 4624/4625/4648 (logon events) for all privileged and externally-facing accounts — off-hours authentication or logons from .cn or VPN-masked geolocations corroborate T1078 valid account abuse as the APT's post-phishing persistence method | Sysmon Event ID 1 (Process Create) logs capturing full command-line arguments — parent-child chains showing Office or browser processes spawning PowerShell with -EncodedCommand flags are the primary forensic indicator of T1027 obfuscated execution following document-based initial access in this campaign | DNS resolver query logs and proxy access logs for the 30 days preceding detection — Chinese state-linked APT C2 over T1071 (Application Layer Protocol) typically produces low-volume, periodic outbound queries to actor-registered domains; preserving these logs before they rotate is time-critical | Scheduled task XML files from C:\Windows\System32\Tasks\ and registry key HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks — Chinese APT groups using dated tactics commonly establish persistence via T1053.005 (Scheduled Task) after initial access, and these artifacts survive reboots and partial log clearing

Per-Action IR Details

Step 1: Scoping — Determine whether your organization operates in Indian banking or South Korean policy sectors, or maintains partnerships, data-sharing relationships, or network connectivity with organizations in those sectors. Expand monitoring posture if any nexus exists.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and defining monitoring scope before active compromise is detected

Controls: NIST IR-4 (Incident Handling) — establish scope boundaries for incident handling capability, NIST SI-4 (System Monitoring) — expand monitoring posture based on threat landscape assessment, NIST RA-3 (Risk Assessment) — assess organizational exposure to this campaign based on sector nexus, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — identify assets with connectivity to Indian banking or South Korean policy sector partners, CIS 3.2 (Establish and Maintain a Data Inventory) — identify sensitive financial or policy data holdings that would be of intelligence value to Chinese state-linked APT

Compensating: With no SIEM, run a manual asset and partnership audit: query Active Directory with 'Get-ADComputer -Filter * -Properties * | Select Name, Description, LastLogonDate' to identify systems with cross-border connectivity. Review firewall egress rules and VPN split-tunnel configs for routes to .in or .kr address space. Document any shared API keys, data feeds, or email relay relationships with in-scope sector partners in a simple spreadsheet. This can be completed by a 2-person team in 2-4 hours.

Evidence: Before scoping decisions are finalized, preserve a point-in-time snapshot of: current firewall connection state tables (run 'netstat -ano' on internet-facing hosts and save output), BGP/routing tables showing external peering relationships, and the current list of active VPN tunnels or site-to-site connections. These establish a clean baseline against which later anomalies tied to Chinese APT C2 infrastructure can be measured.

Step 2: Detection — Review email gateway logs for spear-phishing indicators (T1566): unexpected senders from free or lookalike domains targeting finance or policy staff. Check authentication logs for anomalous use of valid credentials (T1078): off-hours logins, impossible travel, or access from unexpected geolocations. Monitor outbound traffic for C2 patterns over standard application protocols (T1071): unusual HTTP/S, DNS, or SMTP traffic volumes to unfamiliar external destinations.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlating indicators across email, authentication, and network telemetry consistent with APT spear-phishing and valid account abuse TTPs

Controls: NIST AU-2 (Event Logging) — ensure email gateway, authentication, and proxy logs capture fields sufficient to detect T1566, T1078, and T1071, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — conduct targeted review of email and auth logs for indicators specific to this campaign, NIST SI-4 (System Monitoring) — monitor outbound HTTP/S, DNS, and SMTP for C2 beaconing patterns consistent with dated Chinese APT tooling, NIST IR-5 (Incident Monitoring) — track and document observed indicators tied to T1566, T1078, and T1071 for this campaign, CIS 8.2 (Collect Audit Logs) — verify that email gateway, IdP/SSO, and proxy logs are being collected and retained

Compensating: For email: export mail server logs (Exchange: Get-MessageTrackingLog; O365: Search-UnifiedAuditLog) and grep for domains registered within the last 90 days or containing 'bank', 'reserve', 'ministry', 'policy' as lookalike strings. For auth anomalies without a SIEM: run 'Get-ADUser -Filter * | Get-ADObject -Properties LastLogonDate,BadPwdCount' and cross-reference logon timestamps against business hours. For C2 detection: run Zeek (free) on a network tap or span port and use the 'conn.log' to identify outbound connections with low byte counts and regular intervals (classic beaconing) to non-categorized IP space. Sigma rule 'proc_creation_win_powershell_encoded_param.yml' from the SigmaHQ repository applied to Windows Event Log 4688 will catch encoded PowerShell execution without EDR.

Evidence: Preserve before analysis: (1) Raw email gateway logs including full SMTP envelope headers and attachment metadata for the past 30 days — specifically look for .doc/.xls/.pdf attachments sent to finance or policy staff from external senders; (2) Windows Security Event Log Event ID 4624 (Successful Logon) and 4625 (Failed Logon) with Logon Type 3 (Network) and 10 (RemoteInteractive) for all privileged accounts; (3) Proxy or firewall logs capturing full URI paths for outbound HTTP/S — Chinese APT tooling using T1071 often uses specific URI patterns (e.g., '/update', '/check', '/report') with regular beacon intervals; (4) DNS query logs from the recursive resolver for queries to newly registered domains or domains with low Alexa/Umbrella rank.

Step 3: Hardening — Enforce MFA on all externally facing systems and privileged accounts to reduce valid account abuse risk (T1078). Audit and remove unused or dormant accounts. Deploy or verify email security controls (SPF, DKIM, DMARC) to reduce phishing delivery success (T1566). Restrict file and directory enumeration permissions on sensitive systems (T1083, T1005).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Implementing preventive hardening measures to reduce attack surface while active campaign is ongoing, prioritizing valid account abuse (T1078) as the primary initial access vector

Controls: NIST IR-4 (Incident Handling) — containment actions to reduce exposure during active campaign, NIST AC-2 (Account Management) — audit and disable dormant accounts exploitable via T1078, NIST IA-5 (Authenticator Management) — enforce MFA to neutralize stolen credential use against externally facing systems, NIST SI-2 (Flaw Remediation) — verify SPF/DKIM/DMARC controls are correctly configured to reduce T1566 delivery, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA on all internet-facing applications targeted by this campaign, CIS 6.5 (Require MFA for Administrative Access) — enforce MFA for all administrative accounts given APT focus on privileged credential abuse (T1078), CIS 5.3 (Disable Dormant Accounts) — remove accounts inactive for 45+ days that represent low-friction targets for credential stuffing, CIS 4.7 (Manage Default Accounts on Enterprise Assets and

Software) — audit and disable default service accounts on banking-sector-facing systems

Compensating: MFA without commercial tooling: deploy Duo Free tier (up to 10 users) or configure TOTP via privacyIDEA (open source) against VPN and OWA/O365 ADFS. Dormant account audit: 'Search-ADAccount -AccountInactive -TimeSpan 45 -UsersOnly | Disable-ADAccount' run with review before execution. DMARC verification: use 'dig TXT yourdomain.com' to confirm p=reject policy is set; use MXToolbox (free, web-based) to validate SPF flattening and DKIM selector alignment. File enumeration restriction (T1083/T1005): use 'icacls' on Windows to audit and remove broad Read permissions from finance data directories — 'icacls C:\FinanceData /inheritance:d' followed by explicit ACL assignment.

Evidence: Before executing hardening steps, capture: (1) Current Active Directory account state — export 'Get-ADUser -Filter * -Properties Enabled,LastLogonDate,PasswordLastSet,MemberOf | Export-CSV' as a baseline to compare post-incident against any accounts the APT may have created or modified; (2) Current MFA enrollment status for all externally-facing accounts to identify which accounts are currently unprotected and would have been valid targets; (3) SPF/DKIM/DMARC DNS record snapshots as evidence of pre-incident email control posture for any regulatory reporting obligation.

Step 4: Threat Hunting — Run hunts for obfuscated script execution (T1027) in endpoint telemetry: PowerShell with encoded commands, unusual parent-child process chains, or living-off-the-land binaries used outside normal workflows. Cross-reference outbound connection destinations against known Chinese state-linked C2 infrastructure using your threat intelligence platform.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Proactive hunting for T1027 obfuscation and LOLBIN abuse consistent with dated Chinese APT tradecraft, applied before incident declaration to determine if active compromise exists

Controls: NIST SI-4 (System Monitoring) — proactive endpoint telemetry analysis for obfuscated execution and LOLBIN abuse, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — targeted log review for T1027 indicators in process creation and PowerShell logs, NIST IR-4 (Incident Handling) — hunting as a pre-declaration detection activity within the incident handling lifecycle, NIST AU-12 (Audit Record Generation) — verify PowerShell Script Block Logging and process creation logging are enabled to support hunting, CIS 8.2 (Collect Audit Logs) — confirm endpoint process creation and PowerShell logs are being collected prior to hunt execution

Compensating: Without EDR: (1) Deploy Sysmon with SwiftOnSecurity's config (free, GitHub) — Event ID 1 (Process Create) captures full command lines including base64-encoded PowerShell arguments; hunt with: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Message -like "*-enc*" -or $_.Message -like "*-EncodedCommand*"}'. (2) Enable PowerShell Script Block Logging via GPO (HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging, EnableScriptBlockLogging=1) and hunt Event ID 4104 for obfuscated content. (3) For LOLBIN abuse (T1218 sub-techniques common to Chinese APT): hunt Sysmon Event ID 1 for mshta.exe, regsvr32.exe, certutil.exe, or rundll32.exe with unusual parent processes (e.g., Outlook.exe or browser spawning these). (4) For C2 cross-referencing without a TI platform: download the CISA Known Exploited Vulnerabilities catalog and current APT IOC feeds from CISA AIS or the MISP threat sharing community, then cross-reference against your proxy/firewall logs using PowerShell 'Compare-Object'.

Evidence: Preserve before hunting: (1) Windows Event Log 4688 (Process Creation with command line) or Sysmon Event ID 1 — specifically parent-child chains where Office applications (winword.exe, excel.exe) or browser processes spawn cmd.exe, powershell.exe, or wscript.exe, which is a hallmark of document-based spear-phishing initial access (T1566.001) used by Chinese APT groups; (2) PowerShell Event ID 4103 (Module Logging) and 4104 (Script Block Logging) for any sessions containing base64 strings or invocation of Net.WebClient DownloadString — consistent with T1027 and T1059.001; (3) Scheduled Task creation artifacts in Event ID 4698 (A scheduled task was created) and registry key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks' — Chinese APT persistence via T1053.005 is a common follow-on after T1027 execution; (4) Prefetch files at C:\Windows\Prefetch\ for evidence of LOLBIN execution (certutil.exe, mshta.exe) that may not appear in current logs if log rotation has occurred.

Step 5: Post-Incident Controls — Document gaps in visibility identified during hunting. If no SIEM coverage exists for the mapped ATT&CK techniques, prioritize detection rule development. Report any confirmed indicators to CISA (for US-nexus organizations) or the relevant national CERT. Contribute confirmed IOCs to

your threat intelligence sharing community (ISAC, if applicable).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned, detection gap remediation, and intelligence sharing following hunting and containment activities for this Chinese APT campaign

Controls: NIST IR-4 (Incident Handling) — post-incident review and capability improvement, NIST IR-6 (Incident Reporting) — report confirmed indicators to CISA or national CERT per sector and jurisdictional obligations, NIST IR-8 (Incident Response Plan) — update IR plan to incorporate detection gaps identified during this campaign hunt, NIST SI-5 (Security Alerts, Advisories, and Directives) — participate in ISAC/CERT intelligence sharing to contribute confirmed IOCs from this campaign, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — document log coverage gaps against T1566, T1078, T1071, T1027, T1083, and T1005 as mapped in this advisory, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate detection gap findings into the vulnerability and risk management process, CIS 7.2 (Establish and Maintain a Remediation Process) — prioritize detection rule development for unmapped ATT&CK techniques as a risk-based remediation action

Compensating: Detection rule development without a commercial SIEM: author Sigma rules (free, YAML-based, portable) targeting T1566, T1078, T1071, and T1027 and convert to native Windows Event Log queries using 'sigma convert -t windows-event-log'. Publish to your internal wiki. For CISA reporting: use the CISA online reporting form at cisa.gov/report (no account required); for FS-ISAC members (Indian banking nexus), submit via the FS-ISAC TLP:AMBER sharing channel. For OSINT IOC correlation: configure MISP Community instance (free, open source) to ingest CISA AIS feeds and cross-reference hunting findings. A 2-person team can complete gap documentation and initial Sigma rule drafting in one 4-hour sprint.

Evidence: Before closing post-incident activity: (1) Preserve the complete hunting artifact set — all raw log exports, process trees, and network connection records collected during Steps 2 and 4 — with chain-of-custody documentation in case a confirmed compromise requires formal forensic escalation; (2) Document the specific ATT&CK technique coverage gaps (which of T1566, T1078, T1071, T1027, T1083, T1005 had no detection rule and no log source) as evidence for risk acceptance or remediation prioritization decisions; (3) If any IOCs are confirmed, preserve them in structured format (STIX 2.1 or MISP event) with confidence rating and source attribution before submission to CISA or ISAC — unstructured IOC sharing reduces downstream utility for the sector.

Detection Guidance

No confirmed IOCs are available from current reporting. Detection should focus on behavioral indicators aligned to the mapped ATT&CK techniques. Monitor email gateways for spear-phishing attempts (T1566) targeting finance and policy staff, particularly messages with urgency framing or document attachments. Review Active Directory and SSO logs for valid account misuse (T1078): flag logins outside business hours, from new geolocations, or accessing sensitive file shares without prior history. Inspect proxy and DNS logs for repeated outbound connections to low-reputation or newly registered domains over HTTP/S (T1071). In endpoint telemetry, flag obfuscated script execution (T1027) and unusual file enumeration activity on hosts handling financial data (T1083, T1005). Because no malware family or specific tooling has been confirmed, signature-based detection will not be effective; behavioral and anomaly-based rules are the appropriate detection layer.

Framework Mappings

MITRE-ATTACK

- **T1071** — Application Layer Protocol
- **T1589** — Gather Victim Identity Information
- **T1078** — Valid Accounts

- **T1027** — Obfuscated Files or Information
- **T1566** — Phishing
- **T1005** — Data from Local System
- **T1083** — File and Directory Discovery

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-3** — Malicious Code Protection
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection

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
T1071	Application Layer Protocol	Command-And-Control
T1589	Gather Victim Identity Information	Reconnaissance
T1078	Valid Accounts	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1566	Phishing	Initial-Access
T1005	Data from Local System	Collection
T1083	File and Directory Discovery	Discovery

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/chinese-apt-...	T3
Data Breaches in India's Banking Sector in 2025	https://www.cyberlawconsulting.com/Data_Breaches_in_India_Banking_S...	T3
A Comprehensive Guide to Cybersecurity in Indian Banking System	https://www.researchgate.net/publication/379310667_Fortifying_Finan...	T3
Digital Threats Targeting India - Banking Financial Services and ...	https://www.resecurity.com/blog/article/digital-threats-targeting-i...	T3
Why India's Bank Branches Are the Biggest Cybersecurity Blind Spot	https://medium.com/@emmaken695/why-indias-bank-branches-are-the-big...	T3

Generated 2026-04-21 18:37 UTC by TJS Security Command Center