INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-01 07:07 UTC

China-Nexus APT Campaign Hits Southeast Asia Critical Infrastructure With Novel Backdoor

THREAT CAMPAIGN | **CRITICAL** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0603
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	Critical infrastructure organizations across Southeast Asia, including at least two state-owned entities; specific products and versions not disclosed in available source material
Published	2026-06-30T21:00:01
Discovery Source	Rss

Executive Summary

According to a Dark Reading report (not yet independently confirmed by CISA or affected entities), a China-linked threat actor has reportedly compromised at least 10 organizations across Southeast Asia, including two state-owned entities. The campaign deploys a previously undocumented backdoor targeting critical infrastructure, with the objective of establishing persistent, covert access within sensitive networks. Organizations operating critical infrastructure in Southeast Asia, or those with regional supply chain dependencies, face elevated risk of targeted intrusion.

Technical Analysis

According to Dark Reading (T2 source), a China-nexus threat actor has conducted targeted intrusions against at least 10 Southeast Asian organizations, deploying a novel, undocumented backdoor. No CVE identifier has been assigned. A CVSS base score of 7.5 was ingested from metadata but cannot be independently verified against a primary advisory, as no vendor PSIRT notice or CISA advisory has been identified in available source material; this score should be treated as unverified. The backdoor aligns with CWE-506 (Embedded Malicious Code) and CWE-912 (Hidden Functionality), consistent with nation-state implant tradecraft. Observed MITRE ATT&CK techniques include: T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1059 (Command and Scripting Interpreter), T1543.003 (Windows Service creation), T1021.002 (SMB/Windows Admin Shares), T1003.001 (LSASS Memory credential access), T1071/T1071.001 (Application Layer Protocol, web traffic), T1573 (Encrypted Channel), T1560 (Archive Collected Data), T1053.005 (Scheduled Task), T1587.001 (Malware development), T1195 (Supply Chain Compromise). Threat actor assessment: China-linked (specific group unattributed). Attribution to a China-nexus actor is asserted by the reporting source only;

independent corroboration has not been confirmed in available data. Confidence in core campaign claim: MEDIUM. Specific affected products and versions are not disclosed in available source material.

Action Checklist

1. Step 1: Containment. Identify and isolate any systems exhibiting anomalous outbound encrypted communications or unexpected scheduled task creation, particularly in critical infrastructure segments with regional Southeast Asia exposure. Apply network segmentation to limit lateral movement consistent with NIST AC-4 (Information Flow Enforcement). Restrict SMB (port 445) access between non-essential systems per CIS Benchmark 4.4.
2. Step 2: Detection. Hunt for indicators of the MITRE techniques reported: review Windows Event Logs for unauthorized service creation (T1543.003, Event ID 7045), scheduled task creation (T1053.005, Event IDs 4698/4702), and LSASS access patterns (T1003.001, Event ID 10 via Sysmon). Query EDR telemetry for anomalous SMB lateral movement (T1021.002) and encrypted outbound C2 traffic on non-standard ports (T1071, T1573). No specific IOCs (hashes, IPs, domains) are available in current source material; monitor for undisclosed IOC releases from CISA or the original reporting source per NIST AU-6 (Audit Record Review, Analysis, and Reporting). Monitor for unauthorized local account activity per NIST AC-2 (Account Management).
3. Step 3: Eradication. No vendor patch or specific remediation advisory exists for this backdoor, as no CVE has been assigned and the malware is undocumented in available sources. If compromise is suspected, remove identified malicious scheduled tasks and services, revoke and rotate any credentials that may have been exposed, and audit all accounts with administrative privileges per NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts). Engage threat intelligence sources for IOC updates as they become available.
4. Step 4: Recovery. Validate that no unauthorized services or scheduled tasks remain on affected systems. Confirm outbound network traffic baselines have returned to normal. Re-enable systems only after endpoint integrity validation per NIST SI-7 (Software, Firmware, and Information Integrity). Monitor reintroduced systems closely for 30 days per NIST SI-4 (System Monitoring). Retain forensic artifacts per NIST AU-11 (Audit Record Retention) to support potential incident investigation.
5. Step 5: Post-Incident. Review network segmentation and least-privilege posture for critical infrastructure assets per NIST AC-6 and CIS 6.5 (Require MFA for Administrative Access). Assess supply chain access paths per T1195 (Supply Chain Compromise) tradecraft. Establish a process for ingesting and acting on threat intelligence from CISA and sector-specific ISACs per NIST AU-13 (Monitoring for Information Disclosure). Document gaps in detection coverage exposed by this campaign and update detection rules accordingly.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior leadership, legal counsel, and relevant national CERT or government cybersecurity authority if forensic evidence confirms active C2 communication, credential harvesting from privileged accounts, lateral movement into OT/ICS network segments, or any data exfiltration from state-owned or critical infrastructure systems — all of which trigger mandatory incident notification obligations under most critical infrastructure sector regulations and elevate the incident to a potential national security matter given confirmed China-nexus APT attribution.
Recovery Notes	Restored systems must not be returned to critical infrastructure segments until a clean-baseline diff confirms removal of all scheduled tasks, services, and binaries associated with the novel backdoor, and until credential rotation for all accounts with any access to affected hosts is verified complete. Given that China-nexus APT groups are known to establish multiple redundant persistence mechanisms and to re-compromise environments where initial access vectors remain viable, monitor reintroduced hosts with enhanced Sysmon and network telemetry for a minimum of 30 days and maintain heightened alerting thresholds on scheduled task creation, new service installation, and outbound encrypted sessions to previously unseen IP addresses. Retain all forensic artifacts for no less than 12 months and coordinate with your national CERT and sector ISAC to share sanitized IOCs and TTPs that may protect peer critical infrastructure organizations from this ongoing campaign.
Forensic Artifacts	Scheduled task XML definitions from '%SystemRoot%\System32\Tasks\' and registry key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\' — the novel backdoor's primary persistence mechanism based on reported TTPs; compare creation timestamps against known software deployment windows to identify anomalous entries. | Windows Security Event Log entries for Event IDs 7045 (service installation), 4698/4702 (scheduled task creation/modification), 4624/4648 (interactive and network logon events), and 4672 (special privilege logon) scoped to the dwell period — these establish the attacker's access timeline and credential use patterns across the compromised critical infrastructure environment. | Sysmon Event ID 10 (process access) logs filtered for LSASS as the target process — China-nexus APT operators routinely harvest credentials from LSASS memory using tools such as Mimikatz or custom loaders; these logs identify which source processes accessed LSASS and whether credential theft preceded lateral movement. | Full RAM captures (WinPmem or Magnet RAM Capture) from hosts with confirmed anomalous outbound encrypted communications — the undocumented backdoor's decryption keys, C2 protocol state, injected shellcode, and in-memory configuration are recoverable only from live memory and are the primary source for IOC development given the absence of published signatures. | Network flow records (NetFlow/IPFIX) and Zeek/Wireshark packet captures from critical infrastructure segment boundary interfaces, filtered for outbound TLS sessions on non-standard ports with JA3 fingerprints not matching known-good enterprise software — these establish C2 infrastructure attribution and data exfiltration volume, both critical for regulatory reporting and potential government notification under applicable critical infrastructure protection frameworks.

Per-Action IR Details

Step 1: Containment — Identify and isolate any systems exhibiting anomalous outbound encrypted communications or unexpected scheduled task creation, particularly in critical infrastructure segments with regional Southeast Asia exposure. Apply network segmentation to limit lateral movement consistent with NIST AC-4 (Information Flow Enforcement). Restrict SMB (port 445) access between non-essential systems per CIS 4.4 (Implement and Manage a Firewall on Servers).

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: On Windows hosts, run 'Get-NetTCPConnection | Where-Object {$_.State -eq "Established"} | Sort-Object RemoteAddress' to identify active outbound connections on non-standard ports. Cross-reference remote IPs against known-bad ASNs associated with China-nexus C2 infrastructure using free tools such as IPDB or AbuseIPDB CLI. Use Windows Firewall (`netsh advfirewall firewall add rule`) to block port 445 between OT/IT boundary hosts immediately. Deploy Wireshark on network taps at critical infrastructure segment boundaries to capture and inspect encrypted outbound sessions for anomalous JA3/JA3S fingerprints characteristic of custom backdoor TLS stacks.

Evidence: BEFORE isolating any host, capture: (1) full RAM image using WinPmem or Magnet RAM Capture to preserve backdoor in-memory artifacts, decrypted C2 channel state, and injected thread evidence; (2) 'Get-NetTCPConnection -State Established' and 'netstat -ano' output to record active C2 sessions before network cut; (3) 'Get-ScheduledTask | Export-Csv' to snapshot all registered scheduled tasks in their live state; (4) running process list via 'Get-Process' and 'tasklist /svc' to map service-hosted backdoor processes. This APT campaign uses a novel, undocumented backdoor — in-memory artifacts are the primary forensic evidence and are non-recoverable after isolation.

Step 2: Detection — Hunt for indicators of the MITRE techniques reported: review Windows Event Logs for unauthorized service creation (T1543.003, Event ID 7045), scheduled task creation (T1053.005, Event IDs 4698/4702), and LSASS access patterns (T1003.001, Event ID 10 via Sysmon). Query EDR telemetry for anomalous SMB lateral movement (T1021.002) and encrypted outbound C2 traffic on non-standard ports (T1071, T1573). No specific IOCs (hashes, IPs, domains) are available in current source material; monitor for undisclosed IOC releases from CISA or the original reporting source per NIST AU-6 (Audit Record Review, Analysis, and Reporting). Apply D3-LAM (Local Account Monitoring) to identify unauthorized local account activity.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation)

Compensating: Deploy Sysmon with SwiftOnSecurity or Olaf Hartong's modular config to capture Event ID 7045 (service install), Event IDs 4698/4702 (scheduled task create/modify), and Event ID 10 (LSASS process access). Use Sigma rule 'proc_creation_win_lsass_dump_comsvcs' and 'win_susp_scheduled_task_creation' translated to PowerShell Get-WinEvent queries: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4698}'. For network detection without a SIEM, run Zeek (formerly Bro) on a span port at the critical infrastructure segment boundary and alert on outbound TLS sessions with SNI mismatch or to IPs in APNIC-allocated ranges not matching legitimate business partners. Use osquery scheduled query 'SELECT * FROM scheduled_tasks' to baseline and diff task state daily.

Evidence: This is an analysis-only step that does not alter live host state; standard volatile capture order applies if a confirmed host is later acted upon. Log sources to review: Windows Security Event Log (Event IDs 4698, 4702, 7045, 4624, 4625, 4672), Sysmon Event ID 10 (LSASS access targeting process handle grants from unexpected parent processes), Sysmon Event ID 3 (network connection) filtered on non-standard ports with outbound direction, Windows Task Scheduler operational log at 'Microsoft-Windows-TaskScheduler/Operational', and SMB session logs via 'Microsoft-Windows-SMBServer/Security'. For this campaign specifically, prioritize scheduled task XML files stored at '%SystemRoot%\System32\Tasks\' for tasks created outside of patch windows or software deployment cycles — the novel backdoor is likely establishing persistence through this mechanism.

Step 3: Eradication — No vendor patch or specific remediation advisory exists for this backdoor, as no CVE has been assigned and the malware is undocumented in available sources. If compromise is suspected, remove identified malicious scheduled tasks and services, revoke and rotate any credentials that may have been exposed (consistent with D3-CRO, Credential Rotation), and audit all accounts with administrative privileges per NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts). Engage threat intelligence sources for IOC updates as they become available.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST AC-6 (Least Privilege), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Use 'schtasks /delete /tn "" /f' to remove identified malicious scheduled tasks after documenting their XML definition. Remove rogue services via 'sc delete ' after capturing the binary path for YARA scanning. For credential rotation without a PAM tool, use Active Directory's 'Set-ADAccountPassword' for domain accounts and 'net user ' for local accounts, prioritizing accounts that had interactive or network logon sessions (Event ID 4624 Type 3/10) on compromised hosts. Run ClamAV with a custom YARA rule targeting the backdoor's known behavioral characteristics (persistence via scheduled tasks, encrypted outbound on non-standard ports) across all critical infrastructure hosts in the affected segment.

Evidence: BEFORE revoking credentials or removing services/tasks, capture: (1) a copy of the malicious scheduled task XML from '%SystemRoot%\System32\Tasks\' and registry key 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks'; (2) the binary or script referenced in the task/service definition — hash it (SHA-256 via 'Get-FileHash') and submit to VirusTotal or an internal sandbox before deletion; (3) Windows Security Event Log entries for Event ID 4624 (logon) and 4648 (explicit credential use) scoped to the accounts being rotated, to establish the full scope of credential exposure; (4) LSASS minidump (if legally and operationally authorized) to assess whether credential material was extracted by the threat actor prior to your response. China-nexus APT operators typically harvest credentials for re-use across the broader campaign — scope of credential exposure must be understood before rotation to avoid missing exposed service accounts.

Step 4: Recovery — Validate that no unauthorized services or scheduled tasks remain on affected systems. Confirm outbound network traffic baselines have returned to normal. Re-enable systems only after endpoint integrity validation consistent with D3-SFA (System File Analysis). Monitor reintroduced systems closely for 30 days per NIST SI-4 (system monitoring). Retain forensic artifacts per NIST AU-11 (Audit Record Retention) to support potential incident investigation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-11 (Audit Record Retention), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Validate integrity of returned systems using NIST's free SCAP-validated tool (OpenSCAP) to compare current system state against a known-good configuration baseline. Use 'Get-ScheduledTask | Where-Object {$_.TaskPath -notlike "\Microsoft*"} | Select TaskName, TaskPath, State' to enumerate all non-Microsoft scheduled tasks and verify against your pre-incident baseline. Monitor reintroduced hosts for 30 days using Sysmon with enhanced network logging (Event ID 3) and route Sysmon logs to a centralized syslog server (rsyslog or Windows Event Forwarding) for correlation. Retain all collected forensic artifacts — RAM images, task XMLs, binary samples, event log exports — in write-once storage (e.g., WORM drive or immutable S3 bucket) for a minimum of 12 months given the nation-state attribution and potential regulatory or government reporting requirements.

Evidence: This step alters live state by re-enabling systems to production networks. Before reintroduction, perform a final volatile check: re-run 'Get-NetTCPConnection', 'Get-ScheduledTask', and 'Get-Service' snapshots on the restored host and diff against the clean baseline to confirm no residual backdoor components. Verify file system integrity at common China-nexus APT staging paths: '%TEMP%', '%APPDATA%\Microsoft\', 'C:\ProgramData\', and any directories writable by the compromised service account. Confirm that Windows Security Event Log forwarding is active and shipping to your centralized log store before the host is returned to the critical infrastructure segment — loss of log continuity on reintroduced hosts is a known blind spot exploited for re-compromise.

Step 5: Post-Incident — Review network segmentation and least-privilege posture for critical infrastructure assets per NIST AC-6 and CIS 6.5 (Require MFA for Administrative Access). Assess supply chain access paths per T1195 (Supply Chain Compromise) tradecraft. Establish a process for ingesting and acting on threat intelligence from CISA and sector-specific ISACs per NIST AU-13 (Monitoring for Information Disclosure). Document gaps in detection coverage exposed by this campaign and update detection rules accordingly.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-6 (Least Privilege), NIST AU-13 (Monitoring For Information Disclosure), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Conduct a structured lessons-learned session within 2 weeks of containment, documenting: (1) which detection controls failed to fire on the novel backdoor's behavior, (2) which network paths enabled lateral movement into critical infrastructure segments, and (3) which third-party or supply chain access paths were not subject to MFA enforcement. For supply chain access review, enumerate all vendor remote access accounts in Active Directory using 'Get-ADUser -Filter {Description -like "*vendor*" -or Description -like "*contractor*"} | Select Name, Enabled, LastLogonDate' and verify MFA enrollment and least-privilege scope. Subscribe to CISA's Known Exploited Vulnerabilities catalog RSS feed and the relevant sector ISAC (E-ISAC for energy, WaterISAC for water utilities) mailing lists for IOC updates specific to this ongoing China-nexus campaign. Author or update Sigma detection rules targeting the behavioral patterns observed: scheduled task creation outside business hours by SYSTEM or service accounts, outbound TLS to IPs with no DNS resolution history in your environment.

Evidence: No live host state is altered in this phase; evidence focus is on completeness of the forensic record. Verify that the following artifacts are preserved and accessible for post-incident review and any government or regulatory reporting: all Sysmon and Windows Event Log exports from affected hosts covering the full suspected dwell time, network flow records (NetFlow/IPFIX) from the critical infrastructure segment boundary for the same period, copies of all identified malicious scheduled task XMLs and service binaries, and the timeline reconstruction correlating first observed anomaly to containment. Given nation-state attribution and the involvement of state-owned entities in the broader campaign, assess whether mandatory incident reporting obligations apply under applicable national cybersecurity regulations or sector-specific frameworks before closing the incident record.

Detection Guidance

No confirmed IOCs (file hashes, C2 IP addresses, or domains) are available in current source material. Detection should focus on behavioral indicators consistent with the reported MITRE techniques. Hunt priorities: (1) Unauthorized Windows service creation, Event ID 7045, especially services with non-standard names or paths; (2) Scheduled task creation or modification, Event IDs 4698, 4699, 4700, 4702, review task XML for obfuscated commands; (3) LSASS access, Sysmon Event ID 10 with GrantedAccess 0x1010 or 0x1410 targeting lsass.exe; (4) Anomalous SMB lateral movement, Event ID 4624 (logon type 3) combined with remote service/task creation on non-standard hosts; (5) Encrypted C2 traffic, proxy and firewall logs showing sustained encrypted sessions to unfamiliar external hosts, particularly on non-standard ports. Monitor for unauthorized account activity per NIST AC-2 and validate system file integrity per NIST SI-7. Monitor for IOC releases from CISA, sector ISACs, and the original reporting source (Dark Reading / underlying research). This guidance is based on technique-level inference from MITRE ATT&CK mappings; artifact-level signatures are not yet available.

Framework Mappings

MITRE-ATTACK

- **T1543.003** — Windows Service
- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts
- **T1560** — Archive Collected Data
- **T1543** — Create or Modify System Process

- **T1059** — Command and Scripting Interpreter
- **T1021.002** — SMB/Windows Admin Shares
- **T1587.001** — Malware
- **T1195** — Supply Chain Compromise
- **T1003.001** — LSASS Memory
- **T1071** — Application Layer Protocol
- **T1573** — Encrypted Channel
- **T1053.005** — Scheduled Task
- **T1071.001** — Web Protocols

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **CA-7** — Continuous Monitoring

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
T1543.003	Windows Service	Persistence
T1190	Exploit Public-Facing Application	Initial-Access

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1560	Archive Collected Data	Collection
T1543	Create or Modify System Process	Persistence
T1059	Command and Scripting Interpreter	Execution
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1587.001	Malware	Resource-Development
T1195	Supply Chain Compromise	Initial-Access
T1003.001	LSASS Memory	Credential-Access
T1071	Application Layer Protocol	Command-And-Control
T1573	Encrypted Channel	Command-And-Control
T1053.005	Scheduled Task	Execution
T1071.001	Web Protocols	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/threat-intelligence/china-linked-group-...	T2
Vulnerability In Apache Commons Text Library	https://northwave-cybersecurity.com/threat-response/vulnerability-i...	T3
Apache Commons Text vulnerability CVE-2022-42889	https://my.f5.com/manage/s/article/K24823443	T3
Apache Common Text Vulnerability Guidance	https://cloudian.com/blog/apache-common-text-vulnerability-guidance/	T3
CVE-2022-42889 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2022-42889	T1

Generated 2026-07-01 07:07 UTC by TJS Security Command Center