INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 09:05 UTC

UAT-8302: China-Nexus APT Expands Government Espionage Across South America and Southeastern Europe

THREAT ACTOR | HIGH | CVSS 7.5

SCC Item ID	SCC-TAC-2026-0014
Type	Threat Actor
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Government entities in South America (late 2024) and southeastern Europe (2025), no specific software products or vendors identified in available source excerpt
Published	2026-05-05T10:19:00
Discovery Source	Rss

Executive Summary

Cisco Talos has identified a China-linked threat actor, UAT-8302, conducting targeted espionage against government entities in South America (late 2024) and southeastern Europe (2025). The group uses custom malware and shared infrastructure consistent with known Chinese state-aligned APT clusters, indicating coordinated, state-directed intelligence collection (full technical report not independently verified at time of publication). Organizations supporting government clients, diplomatic missions, or policy functions in these regions face elevated risk of data exfiltration and persistent network compromise.

Technical Analysis

UAT-8302 is a China-nexus APT attributed by Cisco Talos based on infrastructure overlap and malware family similarities with known Chinese threat clusters. No specific CVEs or affected software products are identified in available source material. The CVSS base score of 7.5 referenced in discovery data appears to reflect a campaign-level risk rating, not a discrete vulnerability, and cannot be independently verified against a specific CVE. The group's TTPs map to MITRE ATT&CK techniques spanning initial access via phishing (T1566), command execution (T1059), application-layer C2 (T1071), credential dumping (T1003), lateral movement via remote services (T1021), archive collection (T1560), exfiltration over C2 (T1041), ingress tool transfer (T1105), obfuscated files (T1027), persistence via boot/logon autostart (T1547) and scheduled tasks (T1053), and discovery via system info (T1082) and file enumeration (T1083). Custom malware families are deployed post-compromise; specific malware names and IOCs are not available in accessible source material. Attribution

confidence is medium; Cisco Talos is an authoritative secondary source, but the full technical report was not directly accessible for independent verification.

Action Checklist

1. Step 1: Containment. If your organization operates in or supports government entities in South America or southeastern Europe, audit outbound connections for anomalous application-layer C2 patterns (T1071). Block known Chinese APT infrastructure ranges using current threat intelligence feeds from CISA and Cisco Talos. Restrict lateral movement paths by enforcing least-privilege on remote service accounts (T1021).
2. Step 2: Detection. Review EDR and SIEM telemetry for the 13 mapped MITRE techniques: focus on scheduled task creation (T1053), new autostart registry entries (T1547), credential access attempts (T1003), and archive staging activity (T1560). Search for ingress tool transfer events (T1105) and obfuscated payload execution (T1027). Correlate against Cisco Talos threat intelligence for UAT-8302 infrastructure indicators when the full report becomes accessible.
3. Step 3: Eradication. No specific patch or CVE remediation applies. Remove any identified persistence mechanisms (T1547, T1053). Rotate credentials on systems showing signs of credential access (T1003). Audit and remove unauthorized remote access tools or staged archives.
4. Step 4: Recovery. Validate that all identified persistence mechanisms are removed and credential rotation is complete. Monitor for re-compromise via the same TTPs for a minimum of 30 days post-remediation. Confirm C2 communications have ceased by reviewing network flow data against known APT infrastructure indicators.
5. Step 5: Post-Incident. Assess gaps in detection coverage for the 13 mapped techniques. Evaluate whether network segmentation limits lateral movement from internet-facing systems. Conduct a tabletop exercise simulating a phishing-initiated intrusion to test playbook coverage for state-sponsored espionage scenarios.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if network flow analysis confirms active C2 beacon traffic to UAT-8302 infrastructure, if credential access artifacts (Event ID 4656/4663 against lsass.exe) are found on systems processing classified or sensitive government information, or if the organization is subject to FISMA, NIS2, or equivalent national cybersecurity regulatory frameworks that mandate breach notification within defined timeframes upon confirmation of state-sponsored intrusion.

Recovery Notes	Post-containment recovery for UAT-8302 intrusions must account for the possibility of multiple persistence mechanisms installed in layers — validate eradication by checking all five Windows autostart categories (Run keys, Scheduled Tasks, Services, WMI subscriptions, and startup folder entries) against a clean baseline before restoring any affected system to production. Given UAT-8302's focus on government espionage and intelligence collection, verify that no sensitive documents, credential stores, or network topology data were staged in archive form (T1560) and exfiltrated prior to detection by reviewing proxy and DLP logs for large outbound transfers to non-standard destinations during the suspected intrusion window. Maintain heightened monitoring for re-compromise using the full 13-technique TTP profile for a minimum of 30 days, as Chinese state-aligned APT clusters frequently re-establish footholds via secondary implants or previously compromised third-party access paths not identified in initial triage.
Forensic Artifacts	Windows Task Scheduler Operational Log (Microsoft-Windows-TaskScheduler/Operational.evtx) and task XML definitions under C:\Windows\System32\Tasks\ — UAT-8302 persistence via T1053 (Scheduled Task) will leave task entries with creation timestamps, author fields, and action paths that identify the malicious executable and its drop location | HKLM\Software\Microsoft\Windows\CurrentVersion\Run and HKCU equivalent registry hive exports — UAT-8302 T1547 (Boot/Logon Autostart) entries will appear here with value names and data paths pointing to custom malware components, preservable via 'reg export' or Sysinternals Autoruns CSV output before eradication | LSASS-targeted Windows Security Event Log entries (Event ID 4656, 4663 with lsass.exe as Object Name, and Event ID 4624 Type 9 logons) — UAT-8302 credential access via T1003 produces a specific sequence of handle-open and read events against the LSASS process that document both the time and the source process used for credential harvesting | Network pcap or NetFlow records on egress interfaces filtered to destination IPs/domains in the Cisco Talos UAT-8302 indicator set — application-layer C2 (T1071) produces periodic beacon intervals with consistent payload sizing that are identifiable in flow data even when content is encrypted, and these records establish the full duration of C2 activity for the incident timeline | Master File Table ($MFT) and Windows Prefetch files (C:\Windows\Prefetch\) from affected hosts — T1560 archive staging activity leaves $MFT entries recording the creation time, size, and path of staged archive files (e.g., .rar, .zip, .7z), while Prefetch records execution of archiving utilities (rar.exe, 7z.exe) with timestamps that correlate staging activity to the broader intrusion timeline

Per-Action IR Details

Step 1: Containment — If your organization operates in or supports government entities in South America or southeastern Europe, audit outbound connections for anomalous application-layer C2 patterns (T1071). Block known Chinese APT infrastructure ranges using current threat intelligence feeds from CISA and Cisco Talos. Restrict lateral movement paths by enforcing least-privilege on remote service accounts (T1021).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment, Eradication, and Recovery: Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-6 (Least Privilege), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Use Windows Firewall with Advanced Security (netsh advfirewall) or Linux iptables to block outbound connections to IP ranges published in Cisco Talos UAT-8302 indicators. Run 'netstat -ano' on suspected hosts and cross-reference PIDs against Sysmon Event ID 3 (Network Connection) logs filtering on destination ASNs associated with Chinese state infrastructure. For remote service account restriction, enumerate over-privileged accounts with

PowerShell: 'Get-ADGroupMember -Identity "Remote Desktop Users" | Select Name, SamAccountName' and remove any non-essential members immediately.

Evidence: Before blocking, capture full NetFlow or pcap (Wireshark/tcpdump) on perimeter egress points preserving application-layer payloads from any active C2 sessions — UAT-8302 is known to use application-layer protocols (T1071) that may blend with legitimate HTTP/S or DNS traffic, so raw packet capture is essential to characterize the C2 channel. Preserve Windows Security Event Log entries for Event ID 4624/4625 (logon success/failure) and Event ID 4648 (explicit credential use) on remote service accounts flagged during the least-privilege audit, as these document the lateral movement footprint prior to restriction enforcement.

Step 2: Detection — Review EDR and SIEM telemetry for the 13 mapped MITRE techniques: focus on scheduled task creation (T1053), new autostart registry entries (T1547), credential access attempts (T1003), and archive staging activity (T1560). Search for ingress tool transfer events (T1105) and obfuscated payload execution (T1027). Correlate against Cisco Talos threat intelligence for UAT-8302 infrastructure indicators when the full report becomes accessible.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Signs of an Incident and Incident 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), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon with SwiftOnSecurity or olafhartong config to capture: Event ID 1 (Process Create) for LOLBins spawning under scheduled task host (schtasks.exe, taskeng.exe); Event ID 13 (Registry Value Set) for HKLM\Software\Microsoft\Windows\CurrentVersion\Run and HKCU autostart key modifications (T1547); Event ID 11 (File Create) for archive creation via rar.exe, 7z.exe, or PowerShell Compress-Archive (T1560); Event ID 7 (Image Load) for DLL side-loading indicators consistent with UAT-8302 custom malware delivery. For credential access (T1003), query Windows Security Event Log for Event ID 4656 and 4663 filtering on lsass.exe as the object, or use Sysinternals ProcMon to detect LSASS handle opens. Apply the public Sigma rule 'proc_creation_win_lsass_dump' for offline log analysis without EDR.

Evidence: Preserve Windows Security Event Log (Security.evtx), System Event Log (System.evtx), and Task Scheduler operational log (Microsoft-Windows-TaskScheduler/Operational.evtx) with timestamps intact before any remediation — UAT-8302 persistence via T1053 and T1547 will leave specific task XML definitions under C:\Windows\System32\Tasks\ and registry run keys that document initial foothold timing. Collect prefetch files from C:\Windows\Prefetch\ for executables matching ingress tool transfer (T1105) drop locations, and capture MFT ($MFT) entries to reconstruct file creation timelines for staged archives (T1560), which UAT-8302 uses prior to exfiltration.

Step 3: Eradication — No specific patch or CVE remediation applies. Remove any identified persistence mechanisms (T1547, T1053). Rotate credentials on systems showing signs of credential access (T1003). Audit and remove unauthorized remote access tools or staged archives.

NIST Phase: Eradication

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

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST IA-5 (Authenticator Management), CIS 5.2 (Use Unique Passwords), CIS 5.3 (Disable Dormant Accounts), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: Remove scheduled tasks created by UAT-8302 malware using 'schtasks /delete /tn [taskname] /f' after enumerating all tasks with 'schtasks /query /fo LIST /v' and comparing against a known-good baseline. Clean autostart registry keys with 'reg delete HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v [ValueName] /f'. For credential rotation on compromised government workstations, use 'net user [username] [newpassword]' for local accounts and force AD password resets via 'Set-ADAccountPassword' in PowerShell for domain accounts; prioritize service accounts that had remote access rights per Step 1 audit. Use ClamAV with a YARA rule set (e.g., from Cisco Talos's public YARA repository) to scan for UAT-8302 custom malware artifacts before declaring systems clean.

Evidence: Before deleting persistence entries, image the relevant registry hives (SYSTEM, SOFTWARE, NTUSER.DAT) using reg.exe export or Sysinternals Autoruns with '/accepteula /a /c' to CSV — this preserves the

exact autorun entries and their creation metadata for the incident record. Collect the full content of C:\Windows\System32\Tasks\ task XML files and any staged archive files (T1560) from their identified drop paths before deletion, as these files may contain embedded C2 configuration strings or staging directory paths specific to UAT-8302 operations that inform post-incident intelligence sharing.

Step 4: Recovery — Validate that all identified persistence mechanisms are removed and credential rotation is complete. Monitor for re-compromise via the same TTPs for a minimum of 30 days post-remediation. Confirm C2 communications have ceased by reviewing network flow data against known APT infrastructure indicators.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Eradication and Recovery: Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Run Sysinternals Autoruns on each remediated host and diff the output against a clean baseline image using FC or diff to confirm no residual T1547/T1053 entries survived eradication. For the 30-day re-compromise monitoring window, configure a cron job or Windows Scheduled Task to run daily osquery queries against the autorun tables (SELECT * FROM startup_items; SELECT * FROM scheduled_tasks;) and alert on any new entries. Validate C2 cessation by running daily tcpdump captures on egress points filtered to the UAT-8302 infrastructure indicator set published by Cisco Talos and CISA, storing captures for 30 days for retrospective analysis if re-compromise is suspected.

Evidence: Before declaring recovery complete, collect a final NetFlow summary from your perimeter device or Linux 'ss -tunp' / Windows 'netstat -ano' output on all remediated hosts and compare against pre-containment baseline to confirm elimination of C2 beacon intervals — UAT-8302 C2 over application-layer protocols (T1071) often exhibits periodic beacon timing that would persist in flow data if any implant survived eradication. Retain all credential rotation timestamps and new password hash records (from AD audit logs, Event ID 4723/4724) as documented evidence that the T1003 credential access vector has been closed, which will be required for any regulatory or leadership reporting.

Step 5: Post-Incident — Assess gaps in detection coverage for the 13 mapped techniques. Evaluate whether network segmentation limits lateral movement from internet-facing systems. Conduct a tabletop exercise simulating a spearphishing-initiated intrusion to test playbook coverage for state-sponsored espionage scenarios.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned and Evidence Retention

Controls: NIST IR-4 (Incident Handling), NIST IR-3 (Incident Response Testing), NIST IR-8 (Incident Response Plan), NIST CA-7 (Continuous Monitoring), NIST SC-7 (Boundary Protection), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: Map your current Sysmon and Windows Event Log collection against the full UAT-8302 MITRE ATT&CK technique list using the free ATT&CK Navigator (available at attack.mitre.org/resources/attack-navigator) to visualize detection gaps — export the layer JSON and annotate which techniques had no log coverage during this incident. For the tabletop, use the CISA Tabletop Exercise Package (CTEP) framework adapted to a spearphishing scenario targeting government-adjacent personnel, scripting the inject sequence to follow UAT-8302's observed kill chain: spearphish → initial access → scheduled task persistence → credential dumping → lateral movement to document stores → archive and stage for exfiltration.

Evidence: Compile the complete incident timeline from all preserved log sources (Sysmon EVTX, NetFlow, task XML files, registry hive exports, MFT extracts) into a single chronological record per NIST 800-61r3 §4 evidence retention guidance — for a state-sponsored espionage case of this severity, retain all raw evidence for a minimum of 3 years to support potential law enforcement referral or inter-agency intelligence sharing with CISA or relevant national CERTs. Document specifically which of the 13 mapped MITRE techniques produced no alert, produced a low-fidelity alert, or produced a high-fidelity alert, as this gap analysis directly informs Sysmon rule tuning and future Sigma detection rule

development for UAT-8302 follow-on campaigns.

Detection Guidance

No confirmed IOCs are available in accessible source material; the full Cisco Talos report was not directly accessible for independent verification. Detection should focus on behavioral indicators mapped to the 13 MITRE ATT&CK techniques. Key detection priorities: (1) Scheduled task creation and autostart registry modifications on government-adjacent systems (T1053, T1547); monitor Windows Event IDs 4698, 4702, and registry audit events. (2) Credential access attempts including LSASS memory access and SAM database reads (T1003); monitor Sysmon Event ID 10 and Windows Event ID 4656. (3) Outbound connections over uncommon application-layer protocols or to low-reputation infrastructure (T1071); review proxy and firewall logs for beaconing patterns. (4) Archive creation in unusual directories followed by exfiltration (T1560, T1041); monitor for rar/zip creation in temp or user directories. (5) Lateral movement via SMB, RDP, or WMI from workstations to servers (T1021). Once the full Cisco Talos UAT-8302 report is available, retrieve infrastructure IOCs and update block lists and detection rules accordingly.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`[not available]`	No IOCs were extractable from accessible source material. Full Cisco Talos UAT-8302 report was not directly accessible. Obtain IOCs directly from Cisco Talos Threat Intelligence portal when report is available.	LOW

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1071** — Application Layer Protocol
- **T1560** — Archive Collected Data
- **T1041** — Exfiltration Over C2 Channel
- **T1566** — Phishing
- **T1003** — OS Credential Dumping
- **T1021** — Remote Services
- **T1027** — Obfuscated Files or Information
- **T1082** — System Information Discovery
- **T1083** — File and Directory Discovery
- **T1105** — Ingress Tool Transfer
- **T1547** — Boot or Logon Autostart Execution

- **T1053** — Scheduled Task/Job

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **AC-6** — Least Privilege
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **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
T1059	Command and Scripting Interpreter	Execution
T1071	Application Layer Protocol	Command-And-Control
T1560	Archive Collected Data	Collection
T1041	Exfiltration Over C2 Channel	Exfiltration
T1566	Phishing	Initial-Access
T1003	OS Credential Dumping	Credential-Access
T1021	Remote Services	Lateral-Movement
T1027	Obfuscated Files or Information	Defense-Evasion
T1082	System Information Discovery	Discovery

Technique ID	Technique Name	Tactic
T1083	File and Directory Discovery	Discovery
T1105	Ingress Tool Transfer	Command-And-Control
T1547	Boot or Logon Autostart Execution	Persistence
T1053	Scheduled Task/Job	Execution

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/china-linked-uat-8302-targets.html	T3
Unveiling the Sophisticated Attack of DoNot APT Group on ... - Trellix	https://www.trellix.com/blogs/research/from-click-to-compromise-unv...	T3
I'd come running back to EU again: TA416 resumes European ...	https://www.proofpoint.com/us/blog/threat-insight/id-come-running-b...	T3
The Shadow Campaigns: Uncovering Global Espionage	https://unit42.paloaltonetworks.com/shadow-campaigns-uncovering-glo...	T3
[PDF] IDENTIFYING EMERGING CYBER SECURITY THREATS ... - ENISA	https://www.enisa.europa.eu/sites/default/files/publications/ENISA%...	T1

Generated 2026-05-06 09:05 UTC by TJS Security Command Center