INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-05 06:57 UTC

TA4922 Extends Global Reach Beyond East Asia: What Security Teams Outside the Region Need to Track

THREAT ACTOR | MEDIUM | CVSS 5.0

SCC Item ID	SCC-TAC-2026-0023
Type	Threat Actor
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Not specified, sector and regional targeting expansion noted; specific products/systems not identified in available source data
Published	2026-06-04T17:23:59
Discovery Source	Rss

Executive Summary

China-linked threat actor TA4922, assessed as one of the most operationally diverse cybercrime groups currently active, is expanding its geographic targeting beyond its traditional East Asia focus. Organizations in previously low-priority regions, including North America, Europe, and other non-East Asian markets, should now treat TA4922 as an active threat requiring reassessment. The primary business risk is unauthorized access to systems and data through phishing, credential abuse, and exploitation of internet-facing services, though specific targeting criteria for newly affected regions remain unconfirmed.

Technical Analysis

TA4922 is a China-linked threat actor with a history of broad operational activity across cybercrime and likely espionage-adjacent campaigns, per Dark Reading (2026-06-04). The group is extending geographic targeting beyond East Asia. The MITRE ATT&CK techniques associated with this actor in the source data are: T1566 (Phishing), T1078 (Valid Accounts), T1190 (Exploit Public-Facing Application), T1583 (Acquire Infrastructure), and T1588 (Obtain Capabilities). No specific CVEs, malware families, command-and-control infrastructure, or confirmed TTPs were extractable from available source material. Confidence in technical specifics is low. No CVSS vector, EPSS score, or KEV entry applies to this actor-level item.

Action Checklist

1. Step 1: Reassessment. Review your organization's current threat model and determine whether TA4922 was previously excluded from your threat actor watchlist based on regional assumptions. Update your risk register to reflect potential geographic expansion to North America and Europe. Based on TA4922's historical targeting pattern, government, defense, technology, and financial services are elevated-risk sectors; however, no confirmed sector expansion data is available from current sources.
2. Step 2: Detection. Review logs for indicators consistent with MITRE T1566 (phishing delivery), T1078 (use of valid credentials from compromised accounts), and T1190 (exploitation attempts against internet-facing applications). Establish or verify alerting on: authentication anomalies (off-hours logins, impossible travel, new device registrations); spearphishing email headers and attachment execution chains; and scanning or exploitation attempts against external-facing services. Per NIST AU-6, audit records should be reviewed for indications of inappropriate or unusual activity. Per CIS 8.2, confirm audit logging is enabled across all enterprise assets.
3. Step 3: Hardening. Apply MFA to all externally exposed applications (CIS 6.3), remote network access (CIS 6.4), and administrative accounts (CIS 6.5). Review and enforce least privilege access (NIST AC-6) and disable dormant accounts inactive for 45 or more days (CIS 5.3). Validate that internet-facing application patch levels are current per CIS 7.3 and CIS 7.4. No specific patch or CVE remediation is applicable to this actor-level item.
4. Step 4: Verification. After hardening, verify MFA enforcement across all external-facing systems. Confirm that account inventories (CIS 5.1) are current and dormant accounts have been addressed. Review authentication logs for residual anomalies. Confirm audit logging coverage per CIS 8.2 and NIST AU-2. Monitor for follow-on activity consistent with T1583 and T1588 (infrastructure acquisition and capability staging), which may indicate pre-operational targeting.
5. Step 5: Post-Incident Controls. This advisory exposes a common gap: threat actor watchlists based on historical regional targeting rather than current operational scope. Formalize a process for periodic threat actor reassessment tied to intelligence updates. Map TA4922 TTPs (T1566, T1078, T1190) to existing detection rules and validate coverage. Document any gaps as risk register items. Per NIST AU-6, establish a recurring review cadence for threat intelligence-driven audit analysis.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to senior leadership and legal/privacy counsel immediately if authentication logs reveal successful T1078-consistent logins from TA4922-attributed IP ranges, if any external-facing application shows T1190-consistent exploitation artifacts in WAF or web server logs, or if the organization operates in government, defense, financial services, or critical infrastructure sectors where a nation-state-linked actor breach may trigger mandatory regulatory notification obligations.

Recovery Notes	Following hardening, maintain elevated authentication log monitoring for a minimum of 30 days, with daily manual review of Windows Security Event IDs 4624, 4625, and 4648 for anomalous source IPs or credential reuse patterns consistent with TA4922's T1078 technique. Verify that no credential material was exfiltrated prior to MFA enforcement by auditing for T1555 (Credentials from Password Stores) and T1003 (OS Credential Dumping) artifacts — specifically, check for LSASS memory access events in Sysmon Event ID 10 and unexpected access to the Windows Credential Manager vault at %APPDATA%\Microsoft\Credentials\. Given TA4922's operational diversity, treat any single confirmed indicator as a potential indicator of a broader campaign and do not reduce monitoring posture until 30 days of clean telemetry are confirmed.
Forensic Artifacts	Email gateway logs with full header metadata (sender IP, SPF/DKIM/DMARC results, X-Originating-IP) for inbound messages matching TA4922 spearphishing delivery patterns (T1566) — retain original EML files with cryptographic hash for any suspicious messages flagged during the detection review window | Windows Security Event Log entries: Event ID 4624 (Successful Logon, Logon Types 3 and 10), Event ID 4625 (Failed Logon), Event ID 4648 (Explicit Credential Logon), and Event ID 4768/4769 (Kerberos TGT/service ticket requests) — specifically filtered for source IPs outside expected geographies, which is the primary forensic signal for T1078 credential abuse by an actor newly targeting your region | Sysmon Event ID 1 (Process Creation) logs filtered for suspicious parent-child relationships consistent with T1566 execution chains: office applications (winword.exe, excel.exe, powershell.exe as parent) spawning cmd.exe, wscript.exe, mshta.exe, or rundll32.exe — these represent the post-delivery execution stage of a TA4922 phishing lure | Web server access logs (IIS: C:\inetpub\logs\LogFiles\W3SVC**.log; Apache: /var/log/apache2/access.log; Nginx: /var/log/nginx/access.log) and WAF block/allow logs reviewed for automated scanning signatures, path traversal sequences, and exploitation attempt patterns against external-facing services consistent with T1190 — preserve raw logs before any log rotation occurs | Passive DNS and proxy/firewall outbound connection logs for the 30 days preceding the reassessment, reviewed for connections to newly registered domains (registration age under 90 days), domains using bulletproof hosting ASNs historically associated with China-nexus infrastructure, or domains typosquatting your organization — this is the primary artifact class for detecting T1583/T1588 pre-operational staging activity that may have already begun

Per-Action IR Details

Step 1: Reassessment — Review your organization's current threat model and determine whether TA4922 was previously excluded from your threat actor watchlist based on regional assumptions. Update your risk register to reflect potential geographic expansion. Priority sectors include government, defense, technology, and financial services based on TA4922's historical targeting pattern, though no confirmed sector expansion data is available from current sources.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing and maintaining IR capability, threat modeling, and intelligence-driven readiness

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: A 2-person team can conduct threat model reassessment using the free MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) to layer TA4922-associated technique coverage — specifically T1566, T1078, and T1190 — against current detection controls. Export the layer as JSON and diff against your existing coverage matrix. Document gaps directly in a shared risk register (Google Sheets or a markdown file in a Git repo suffices). Schedule a 30-minute review cadence tied to CISA and MITRE ATT&CK update cycles.

Evidence: Before updating the risk register, preserve a snapshot of the current threat actor watchlist and any prior risk assessments that explicitly excluded East Asia-origin actors. Capture the date-stamped version of your existing threat model document and any prior CISA or threat intelligence feeds that informed regional scoping decisions. This establishes a defensible before/after baseline if a future incident traces back to a pre-expansion TA4922 campaign.

Step 2: Detection — Review logs for indicators consistent with MITRE T1566 (phishing delivery), T1078 (use of valid credentials from compromised accounts), and T1190 (exploitation attempts against internet-facing applications). Enable or verify alerting on: authentication anomalies (off-hours logins, impossible travel, new device registrations); spearphishing email headers and attachment execution chains; and scanning or exploitation attempts against external-facing services. Per NIST AU-6, audit records should be reviewed for indications of inappropriate or unusual activity. Per CIS 8.2, confirm audit logging is enabled across all enterprise assets.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring for indicators, correlating events, and triaging potential incidents

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with the SwiftOnSecurity or Olaf Hartong configuration baseline to capture Process Creation (Event ID 1), Network Connection (Event ID 3), and File Creation Time (Event ID 2) events — these will surface T1566 attachment execution chains and T1078 lateral movement via pass-the-hash or token manipulation. For T1190, parse web server access logs (IIS: C:\inetpub\logs\LogFiles\; Apache/Nginx: /var/log/apache2/access.log or /var/log/nginx/access.log) using grep or PowerShell Select-String for anomalous URI patterns, large POST bodies, and scanner fingerprints. Use Sigma rules mapped to T1566, T1078, and T1190 (available at github.com/SigmaHQ/sigma) converted to Windows Event Log or syslog queries via sigma-cli. For impossible travel detection without a SIEM, export authentication logs daily and run a PowerShell diff on source IP geolocation using a free MaxMind GeoLite2 database.

Evidence: For T1566: Collect email gateway logs (header metadata including sender IP, Return-Path, X-Originating-IP, and DKIM/SPF results), mail client attachment execution chains from Sysmon Event ID 1 filtered on parent processes winword.exe, excel.exe, or outlook.exe spawning cmd.exe, powershell.exe, or wscript.exe. For T1078: Capture Windows Security Event Log Event ID 4624 (Successful Logon) with Logon Type 3 or 10 from external IPs, Event ID 4625 (Failed Logon) clusters preceding a successful 4624, and Event ID 4648 (Logon using explicit credentials). For T1190: Collect web application firewall (WAF) logs and IDS/IPS alerts showing scanning signatures, path traversal patterns, or SQL injection strings against external-facing services. Preserve all raw logs with cryptographic hash (SHA-256) before any analysis to maintain evidentiary integrity.

Step 3: Hardening — Apply MFA to all externally exposed applications (CIS 6.3), remote network access (CIS 6.4), and administrative accounts (CIS 6.5). Review and enforce least privilege access (NIST AC-6) and disable dormant accounts inactive for 45 or more days (CIS 5.3). Validate that internet-facing application patch levels are current per CIS 7.3 and CIS 7.4. No specific patch or CVE remediation is applicable to this actor-level item.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Executing containment strategies to limit the actor's ability to exploit valid credentials and public-facing attack surfaces

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For MFA without enterprise tooling, enable TOTP-based MFA on VPN concentrators (most support RFC 6238 natively) and deploy Authelia or Authentik as a free self-hosted MFA/SSO gateway in front of web-exposed applications. For dormant account enumeration on Windows AD, run: Get-ADUser -Filter {LastLogonDate -lt (Get-Date).AddDays(-45) -and Enabled -eq $true} | Select Name, LastLogonDate, SamAccountName and pipe to a CSV for manual review. For Linux, use: lastlog | awk '$4 != "Never" {print}' and cross-reference /etc/passwd enabled

accounts. For least-privilege enforcement without PAM tooling, audit local administrator group membership weekly via: Get-LocalGroupMember -Group Administrators on each endpoint using a scheduled PowerShell task pushing results to a shared network log path.

Evidence: Before disabling accounts or enforcing MFA, capture a full export of all active accounts with last-logon timestamps, group memberships, and assigned privileges (Active Directory: Get-ADUser -Filter * -Properties LastLogonDate, MemberOf, PasswordLastSet | Export-CSV). Document the pre-hardening state of MFA enrollment per application. For internet-facing services, run an authenticated vulnerability scan using OpenVAS or Greenbone Community Edition and archive the report — this establishes patch-level baseline and documents any exploitable condition TA4922 could have leveraged via T1190 prior to remediation.

Step 4: Verification — After hardening, verify MFA enforcement across all external-facing systems. Confirm that account inventories (CIS 5.1) are current and dormant accounts have been addressed. Review authentication logs for residual anomalies. Confirm audit logging coverage per CIS 8.2 and NIST AU-2. Monitor for follow-on activity consistent with T1583 and T1588 (infrastructure acquisition and capability staging), which may indicate pre-operational targeting.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Verifying system integrity, confirming hardening effectiveness, and monitoring for re-compromise or ongoing pre-operational targeting

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 8.2 (Collect Audit Logs)

Compensating: Verify MFA enforcement by attempting authentication to each external-facing application without an MFA token from an out-of-band test account — document pass/fail per system. For T1583/T1588 monitoring (TA4922 infrastructure staging), configure passive DNS monitoring using SecurityTrails free tier or VirusTotal passive DNS to track newly registered domains typosquatting your organization's name or brand — TA4922 pre-operational staging often involves lookalike infrastructure. Use osquery with the dns_resolvers and listening_ports tables scheduled daily to detect unexpected outbound DNS changes or new listener processes that could indicate a staged implant activating. Subscribe to free threat intel feeds (CISA Known Exploited Vulnerabilities catalog, AbuseIPDB) and automate daily ingestion via a Python script that diffs against your firewall deny-list.

Evidence: After hardening and before declaring the environment clean, collect: (1) a post-hardening authentication log export covering the 72 hours following MFA enforcement to identify any accounts still authenticating without MFA — this surfaces bypasses or missed coverage; (2) Windows Security Event Log Event ID 4720 (account created) and Event ID 4722 (account enabled) from the hardening window to detect any accounts created or re-enabled during the activity period; (3) DNS query logs from your internal resolver for the same 72-hour window, reviewed for queries to newly registered domains or domains with low Alexa/Tranco rank that could indicate T1583 staging infrastructure being contacted by a previously installed implant.

Step 5: Post-Incident Controls — This advisory exposes a common gap: threat actor watchlists based on historical regional targeting rather than current operational scope. Formalize a process for periodic threat actor reassessment tied to intelligence updates. Map TA4922 TTPs (T1566, T1078, T1190) to existing detection rules and validate coverage. Document any gaps as risk register items. Per NIST AU-6, establish a recurring review cadence for threat intelligence-driven audit analysis.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned, detection improvement, threat intelligence integration, and policy updates to prevent recurrence

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a formal 60-minute lessons-learned session within 5 business days of completing hardening. Use the MITRE ATT&CK Navigator to produce a TA4922 TTP coverage heatmap: layer T1566 (Phishing), T1078 (Valid Accounts), and T1190 (Exploit Public-Facing Application) against your current Sigma rule library and document which techniques have zero, partial, or full detection coverage. Publish detection gaps as issues in your Git-based risk

register. For recurring threat intelligence review, configure a free RSS aggregator (e.g., FreshRSS self-hosted) subscribed to CISA advisories, MITRE ATT&CK update feeds, and relevant ISACs to alert the team when TA4922-linked TTPs are updated or new infrastructure IOCs are published. Set a calendar-enforced quarterly threat actor watchlist review tied to ATT&CK release cycles.

Evidence: Archive the complete audit trail from this reassessment cycle: the before/after threat model snapshots (Step 1), the raw and analyzed log exports from detection review (Step 2), the pre/post account inventory exports and vulnerability scan reports (Step 3), and the MFA enforcement verification results (Step 4). Retain per NIST AU-11 (Audit Record Retention) requirements and your organization's records retention policy — recommended minimum 12 months for threat-actor-driven reviews to support future forensic timelines. This package constitutes the evidentiary record if a future TA4922 intrusion is discovered and attribution or regulatory notification is required.

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) are available for TA4922's expanded campaign from current source data. Detection should focus on behavioral indicators mapped to the associated MITRE techniques. For T1566 (Phishing): review email gateway logs for lookalike sender domains, suspicious attachment types (ISO, LNK, Office macros), and links to newly registered domains. For T1078 (Valid Accounts): alert on authentication from new geographic locations, impossible travel events, and account activity outside business hours. For T1190 (Exploit Public-Facing Application): monitor WAF and IDS logs for scanning patterns, unusual parameter injection, and error-rate spikes on internet-facing applications. For T1583/T1588 (Infrastructure and Capability Acquisition): monitor for newly observed infrastructure communicating with internal assets, particularly domains registered within 30 days. Per NIST AU-6, schedule regular threat-intelligence-driven review of audit records. Per NIST SI-4, network monitoring should be validated as active on perimeter and internal segments. D3-LAM (Local Account Monitoring) and D3-MFA (Multi-factor Authentication) are the most directly applicable D3FEND countermeasures given the T1078 association.

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1583** — Acquire Infrastructure
- **T1588** — Obtain Capabilities

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege

- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1583	Acquire Infrastructure	Resource-Development
T1588	Obtain Capabilities	Resource-Development

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/threat-intelligence/china-ta4922-cyberc...	T3
Vulnerability In Apache Commons Text Library	https://northwave-cybersecurity.com/threat-response/vulnerability-i...	T3
Security Notice: Apache commons-text vulnerability (CVE-2022 ...	https://support.xmatters.com/hc/en-us/articles/13843436346139-Secur...	T3
Vulnerability (Text4Shell) (CVE-2022-42889) - Cloudera Community	https://community.cloudera.com/t5/Support-Questions/Vulnerability-T...	T3
CVE-2022-42889 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2022-42889	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-05 06:57 UTC by TJS Security Command Center