INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-15 13:47 UTC

UNC6508: PRC Espionage Campaign Weaponizes REDCap to Steal Defense and Medical Research Across North America

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0463
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	REDCap (Research Electronic Data Capture), Google Workspace, AWS Elastic Beanstalk, enterprise identity providers (IdPs), specific versions not publicly disclosed in available reporting
Published	2026-06-15T14:00:00+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Google's Threat Intelligence Group has disclosed a sustained PRC-linked espionage campaign by UNC6508 that operated undetected for over a year inside North American medical, academic, and military research institutions. The group exploited REDCap research data platforms to gain initial access, deployed custom persistence malware called INFINITERED, and exfiltrated sensitive data by manipulating enterprise email compliance rules, a technique not previously widely documented in public threat intelligence. Organizations conducting defense research, Indo-Pacific policy analysis, AI development, uncrewed vehicle programs, or clinical medical research face the highest risk of prior or ongoing compromise.

Technical Analysis

UNC6508 (PRC-nexus) gained initial access by exploiting REDCap (Research Electronic Data Capture) deployments via T1190 (Exploit Public-Facing Application), likely targeting misconfigured or unpatched instances. Post-exploitation included web shell deployment (T1505.003), credential dumping (T1003), keylogging (T1056.001), and account manipulation (T1098) to achieve persistence and lateral movement. The group deployed custom malware designated INFINITERED, classified under CWE-506 (Embedded Malicious Code), to maintain persistent access. A novel exfiltration technique involved manipulating enterprise email compliance rules (T1114.003) to silently redirect or copy outbound communications, undocumented in public

threat intelligence at time of disclosure. Additional TTPs include masquerading (T1036), artifact hiding (T1564), data archiving prior to exfiltration (T1560), and exfiltration over alternative protocols (T1048). The campaign also shows indicators consistent with supply chain compromise analogs (T1195) and use of valid accounts (T1078) for sustained access. No CVE identifier has been assigned; no vendor patch is publicly available as of this report. Specific REDCap versions affected have not been publicly disclosed. CWE coverage includes CWE-287 (Improper Authentication), CWE-312 (Cleartext Storage of Sensitive Information), CWE-506 (Embedded Malicious Code), and CWE-693 (Protection Mechanism Failure). Source: Google Cloud Threat Intelligence blog.

Action Checklist

1. Step 1: Containment. Immediately isolate REDCap instances from the public internet; restrict access to known, authenticated IP ranges via firewall rules (NIST AC-17, CIS 4.4). Suspend or rotate credentials for all REDCap administrative and privileged accounts. Audit enterprise identity provider (IdP) tokens and active sessions for anomalous access patterns tied to REDCap-integrated accounts (NIST AC-2).
2. Step 2: Detection. Audit all enterprise email compliance and transport rules in Google Workspace and connected mail systems for unauthorized additions or modifications (MITRE T1114.003); alert on any rule created by non-administrative accounts or outside change-control windows (NIST AU-6, CIS 8.2). Search endpoint and server logs for INFINITERED indicators: unusual process execution from REDCap application directories, unexpected scheduled tasks or init-config modifications, and anomalous outbound connections on non-standard ports (MITRE T1048). Review AWS Elastic Beanstalk environment logs for web shell artifacts and unexpected file writes.
3. Step 3: Eradication. Remove any unauthorized email compliance rules identified in detection (T1114.003 remediation). Hunt for and remove INFINITERED persistence mechanisms: review system startup configurations, scheduled tasks, cron jobs, and web-accessible directories for unauthorized files (NIST SI-4 analog). Rotate all credentials for REDCap, Google Workspace, AWS, and connected IdPs. Enforce MFA on all externally exposed applications and administrative accounts (CIS 6.3, CIS 6.5).
4. Step 4: Recovery. Validate that all email compliance rules match an approved baseline before restoring mail flow (NIST AU-12 analog; CIS 8.2). Confirm REDCap and connected cloud services show no residual unauthorized accounts or sessions (NIST AC-2, CIS 5.1). Restore REDCap instances from known-clean backups if system file analysis confirms tampering. Monitor for re-infection indicators, specifically re-appearance of unauthorized email rules, new scheduled tasks, or outbound traffic to previously flagged destinations, for a minimum of 30 days post-remediation (NIST AU-6).
5. Step 5: Post-Incident. Conduct a gap assessment against NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges) to determine whether REDCap accounts had excessive access that enabled lateral movement. Review data classification and access controls on research data repositories (NIST AC-3, CIS 3.3) to confirm sensitive defense and clinical data is segmented. Implement user account permission audits for all research platform accounts. Establish ongoing monitoring of open-source and threat intelligence feeds for UNC6508 IOC updates (NIST AU-13). Brief research data custodians on the email compliance rule manipulation technique; this is a novel persistence/exfiltration vector that existing playbooks likely do not cover.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and institutional research security officer if any of the following are confirmed: (1) UNC6508 IOCs (INFINITERED artifacts, unauthorized email compliance rules, or C2 IP matches) are found on systems storing HIPAA-covered clinical trial data, CUI-designated defense research, or export-controlled research data — all three categories carry mandatory breach notification timelines under HIPAA, DFARS 252.204-7012, and EAR/ITAR respectively; (2) lateral movement evidence exists beyond the REDCap host into IRB data repositories, grant management systems, or faculty research drives; or (3) the team cannot confirm a clean backup predating the intrusion, requiring a rebuild-from-scratch decision that exceeds the team's authorization.
Recovery Notes	Before restoring REDCap to production, verify the restored instance against the vendor's published SHA-256 package manifest for the specific REDCap version deployed — UNC6508 placed web shells and modified application files, so byte-level verification against the vendor distribution is mandatory, not optional. Conduct a parallel Google Workspace compliance rule audit on a 24-hour cycle for the first 30 days post-recovery using a scripted `gam` diff against the approved baseline, as re-establishment of email exfiltration rules is the lowest-cost re-entry action available to the actor if any credential or access path was missed during eradication. Given GTIG's reporting of a 12+ month undetected dwell, treat the first 90 days post-recovery as an elevated monitoring period — UNC6508 has demonstrated patience and the operational security to avoid triggering standard alerting thresholds.
Forensic Artifacts	Google Workspace Admin Audit Log — filter for `gmail.settings` change events (action type: CREATE_RULE, UPDATE_RULE) across the full suspected intrusion window; the actor email, source IP, and rule payload in these events are primary evidence of the novel email compliance rule exfiltration technique attributed to UNC6508 and have no prior public documentation | REDCap application directory file system timeline — forensic timestomping analysis of all PHP files under the REDCap document root (e.g., `/var/www/redcap/` or `C:\xampp\htdocs\redcap\`) for files created or modified after the known-clean deployment date; INFINITERED persistence and web shell artifacts will appear as anomalous entries in this timeline | REDCap web server access logs (Apache/Nginx) — look for POST requests to non-standard REDCap API endpoints or survey paths from non-institutional IPs, particularly requests with anomalous Content-Type headers or oversized payloads consistent with web shell command execution or data staging prior to exfiltration | AWS Elastic Beanstalk environment logs and AWS CloudTrail — specifically `PutObject` and `GetObject` S3 API calls, `AssumeRole` events, and any `CreateDeployment` actions in Elastic Beanstalk not tied to approved change records; UNC6508 leveraged Elastic Beanstalk infrastructure, making these logs critical for reconstructing the cloud-side attack path | Host memory image (RAM acquisition) from REDCap application server — INFINITERED's in-memory components, decrypted C2 configuration (including C2 IP/domain and communication protocol), injected code regions, and active network socket state are only recoverable from a live memory capture taken before isolation or reboot; this is the highest-value single artifact for threat intelligence on this previously undocumented malware family

Per-Action IR Details

Step 1: Containment — Immediately isolate REDCap instances from the public internet; restrict access to known, authenticated IP ranges via firewall rules (NIST AC-17, CIS 4.4). Suspend or rotate credentials for all REDCap administrative and privileged accounts (D3-CRO). Audit enterprise identity provider (IdP) tokens and active sessions for anomalous access patterns tied to REDCap-integrated accounts (NIST AC-2).

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-2 (Account Management), NIST AC-12 (Session Termination), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Use iptables or Windows Firewall (netsh advfirewall) to allowlist only known IP ranges to REDCap's application port (typically TCP 443/80) before any credential rotation. Export current IdP session tokens via Google Workspace Admin SDK (`gam all users show tokens`) or equivalent LDAP query to establish a session baseline before invalidation. A 2-person team should split: one handles firewall ACL changes, the other exports the IdP session snapshot simultaneously.

Evidence: BEFORE isolating or rotating credentials, capture: (1) active network connections to the REDCap host (`netstat -ano` on Windows or `ss -antp` on Linux) to record established sessions and external IPs communicating with the REDCap application process; (2) running process list with parent-child relationships (`Get-WmiObject Win32_Process | Select ProcessId,ParentProcessId,Name,CommandLine` or `ps auxf`) to identify any INFINITERED-spawned child processes under the REDCap application worker; (3) full list of active IdP OAuth/SAML tokens and last-used timestamps from Google Workspace Admin Console or AWS IAM before revocation; (4) REDCap application server memory image if INFINITERED indicators are already suspected — volatile memory will contain injected code, decrypted C2 configuration, and active connection state that disappears on isolation.

Step 2: Detection — Audit all enterprise email compliance and transport rules in Google Workspace and connected mail systems for unauthorized additions or modifications (MITRE T1114.003); alert on any rule created by non-administrative accounts or outside change-control windows (NIST AU-6, CIS 8.2). Search endpoint and server logs for INFINITERED indicators: unusual process execution from REDCap application directories, unexpected scheduled tasks or init-config modifications (D3-SICA), and anomalous outbound connections on non-standard ports (MITRE T1048). Review AWS Elastic Beanstalk environment logs for web shell artifacts and unexpected file writes (D3-SFA).

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), CIS 8.2 (Collect Audit Logs)

Compensating: For Google Workspace without a SIEM: use `gam` (open-source Google Workspace CLI) to pull all transport/compliance rules — `gam all users show filters` and `gam show gmailsettings` — then diff the output against a known-good baseline or change-control log. For INFINITERED on the REDCap host: deploy Sysmon (Event ID 1 for process creation, Event ID 3 for network connections, Event ID 11 for file creation) filtering on the REDCap application directory (e.g., `C:\xampp\htdocs\redcap\` or `/var/www/redcap/`). Write a Sigma rule targeting process creation where `ParentImage` matches the REDCap PHP/Apache process and `CommandLine` contains base64 strings or unusual interpreter calls. For AWS Elastic Beanstalk: pull environment logs via `eb logs` CLI and grep for POST requests to non-application endpoints or unusual file extensions (`.php`, `.jsp`, `.ashx`) written outside the deployment package.

Evidence: This is a read-only detection step, but preserve all log data before any subsequent eradication action. Specifically preserve: (1) Google Workspace Admin Audit Log export covering the full suspected dwell period (12+ months per GTIG reporting) — filter for `gmail.settings` change events and record `actor.email`, `timestamp`, and `events.parameters` for each rule modification; (2) REDCap web server access logs (Apache/Nginx) for the same period — look for POST requests to REDCap survey or API endpoints from non-institutional IP ranges, particularly at off-hours consistent with PRC time zones (UTC+8); (3) AWS Elastic Beanstalk environment event history and EC2 instance system logs for unexpected file-write events or `eb deploy` actions not tied to approved change records; (4) Sysmon Event ID 1 and 3 logs showing processes spawned from REDCap application directories with outbound connections on non-standard ports — INFINITERED reportedly uses non-standard egress to evade port-based filtering.

Step 3: Eradication — Remove any unauthorized email compliance rules identified in detection (T1114.003 remediation). Hunt for and remove INFINITERED persistence mechanisms: review system startup configurations (D3-SICA), scheduled tasks, cron jobs, and web-accessible directories for unauthorized files (NIST SI-4 analog; no mapped control for INFINITERED-specific removal — reference vendor and GTIG guidance). Rotate all credentials for REDCap, Google Workspace, AWS, and connected IdPs (D3-CRO,

D3-CH). Enforce MFA on all externally exposed applications and administrative accounts (CIS 6.3, CIS 6.5, D3-MFA).

NIST Phase: Eradication

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

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), CIS 5.2 (Use Unique Passwords), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For INFINITERED persistence removal without EDR: enumerate all scheduled tasks (`schtasks /query /fo LIST /v > tasks_baseline.txt` on Windows; `crontab -l` and `cat /etc/cron.*/*` on Linux) and diff against a pre-incident baseline. Enumerate web-accessible directories under the REDCap document root for files with modification timestamps post-initial-access date and unknown hashes — use `find /var/www/redcap -newer /var/www/redcap/redcap_v/index.php -type f` on Linux. Write a YARA rule targeting INFINITERED's known behavioral signatures (e.g., PHP stagers, unusual base64-encoded payloads in `.php` files) from GTIG's published IOCs and scan the full REDCap directory. For Google Workspace rule removal: use `gam` to delete unauthorized transport rules by rule ID. Credential rotation across REDCap, Google Workspace, and AWS should be coordinated simultaneously to prevent re-authentication by the actor using cached tokens.

Evidence: BEFORE removing persistence mechanisms or rotating credentials, capture: (1) full disk image or targeted forensic copy of REDCap application directories and system startup locations (Windows: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, `HKLM\SYSTEM\CurrentControlSet\Services`; Linux: `/etc/init.d/`, `/etc/systemd/system/`, `/etc/cron.*`) to preserve INFINITERED binary artifacts for hash extraction and YARA rule development; (2) memory acquisition of the REDCap application server using Volatility-compatible tools (WinPmem on Windows, LiME kernel module on Linux) — INFINITERED may operate partially in-memory or decrypt configuration at runtime; (3) export all current Google Workspace compliance/transport rules with full metadata (creator account, creation timestamp, rule conditions and actions) before deletion — these are primary evidence of the novel exfiltration technique and will be needed for regulatory notification and threat intelligence sharing; (4) AWS CloudTrail logs covering IAM role assumption, S3 access, and Elastic Beanstalk deployment events for the full dwell period before any credential rotation invalidates the audit trail correlation.

Step 4: Recovery — Validate that all email compliance rules match an approved baseline before restoring mail flow (NIST AU-12 analog; CIS 8.2). Confirm REDCap and connected cloud services show no residual unauthorized accounts or sessions (NIST AC-2, CIS 5.1). Restore REDCap instances from known-clean backups if system file analysis (D3-SFA) confirms tampering. Monitor for re-infection indicators — specifically, re-appearance of unauthorized email rules, new scheduled tasks, or outbound traffic to previously flagged destinations — for a minimum of 30 days post-remediation (NIST AU-6).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 8.2 (Collect Audit Logs)

Compensating: For email rule baseline validation without a SIEM: script a daily `gam` export of all Google Workspace transport/compliance rules to a version-controlled file (git repo) and configure a cron job to alert on any diff. For REDCap backup validation: before restoring, compute SHA-256 hashes of all application PHP files in the restored backup and compare against the REDCap vendor-released package hash manifest for the installed version — flag any file whose hash does not match the vendor distribution. For 30-day re-infection monitoring without EDR: configure Sysmon Event ID 1 and 11 alerting on the REDCap host filtered to the application directory and known INFINITERED file path patterns, forwarding to a free ELK stack or even a monitored syslog server.

Evidence: During recovery validation, document and retain: (1) the verified-clean file hash manifest for the restored REDCap instance as a forensic baseline for future incident comparison; (2) a timestamped export of all Google Workspace compliance rules post-cleanup to serve as the new approved baseline — this is the reference document for the 30-day re-infection monitoring window; (3) network flow logs (AWS VPC Flow Logs, or NetFlow/PCAP at the perimeter if on-premises) covering the first 72 hours post-restoration to establish a clean traffic baseline and confirm

absence of outbound connections to previously flagged UNC6508 C2 infrastructure; (4) AWS CloudTrail and IAM Access Analyzer findings post-credential rotation to confirm no residual access paths exist via misconfigured role trust policies or overly permissive bucket policies that UNC6508 may have established during the intrusion.

Step 5: Post-Incident — Conduct a gap assessment against NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges) to determine whether REDCap accounts had excessive access that enabled lateral movement. Review data classification and access controls on research data repositories (NIST AC-3, CIS 3.3) to confirm sensitive defense and clinical data is segmented. Implement user account permission audits (D3-UAP) for all research platform accounts. Establish ongoing monitoring of open-source and threat intelligence feeds for UNC6508 IOC updates (NIST AU-13). Brief research data custodians on the email compliance rule manipulation technique — this is a novel persistence/exfiltration vector that existing playbooks likely do not cover.

NIST Phase: Post Incident

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AU-13 (Monitoring For Information Disclosure), CIS 3.3 (Configure Data Access Control Lists), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For the privilege gap assessment without a PAM tool: export all REDCap user roles and permissions via the REDCap API (`/api/?token=&content=user`) and cross-reference against the principle of least privilege — flag any non-administrative account holding REDCap System Administrator, Super User, or API Import/Export rights. For ongoing UNC6508 IOC monitoring without a commercial TI platform: subscribe to CISA advisories (free), configure Google Alerts on 'UNC6508' and 'INFINITERED', and monitor GTIG's published indicator feeds via Mandiant Advantage Free tier or OpenCTI (open-source). For the playbook update: create a specific detection runbook entry for Google Workspace transport rule auditing triggered by any rule creation event outside a defined change-control window — this vector is documented as novel and will not exist in pre-2025 playbook libraries.

Evidence: Post-incident documentation must preserve: (1) the final lessons-learned report capturing the complete UNC6508 dwell timeline reconstructed from Google Workspace Admin Audit Logs, REDCap access logs, and AWS CloudTrail — this timeline is essential for regulatory breach notification (HIPAA, FISMA, or state research data protection laws may apply given the defense and medical research context); (2) a complete inventory of all data repositories the compromised REDCap accounts had access to, with data classification labels, to scope the potential exfiltration impact for notification purposes; (3) before and after privilege comparison for all REDCap accounts as evidence of the control gap that enabled UNC6508's lateral movement, retained for audit and compliance records; (4) the INFINITERED binary samples and YARA rules developed during the investigation, submitted to VirusTotal and shared with sector ISACs (Health-ISAC, DIB-ISAC) given the targeted sectors.

Detection Guidance

Primary detection focus areas for UNC6508 TTPs: (1) Email compliance rule anomalies, query Google Workspace Admin audit logs for CreateRule, UpdateRule, or equivalent transport rule modification events outside approved change windows; alert on any rule created by non-admin users or rules that forward, BCC, or redirect mail to external addresses (T1114.003). (2) REDCap web shell indicators, monitor web server access logs for POST requests to unexpected file paths within the REDCap application directory; use system file analysis to baseline and alert on new or modified files in web-accessible directories, particularly .php files not present in the vendor distribution. (3) INFINITERED persistence, apply system init config analysis to detect modifications to startup scripts, cron jobs, or scheduled tasks on REDCap host systems; flag processes spawning from web server worker accounts (e.g., www-data, apache) that execute shell commands. (4) Credential theft indicators, alert on T1003 (OS Credential Dumping) signatures: access to /etc/shadow, LSASS memory reads, or tools consistent with credential harvesting executing from application user contexts. (5)

Exfiltration patterns, monitor outbound traffic for T1048 (Exfiltration Over Alternative Protocol): large data transfers on non-standard ports, DNS tunneling patterns, or traffic to cloud storage endpoints not in an approved allowlist. (6) Valid account abuse, flag logins from REDCap or IdP accounts at unusual hours, from unexpected geolocations, or accessing data repositories outside normal research workflow patterns (T1078). Behavioral baseline deviation across these vectors is the most reliable indicator given the campaign's extended undetected operational window.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`not disclosed in available public reporting`	UNC6508 C2 infrastructure — specific IOCs not publicly released at time of this report; monitor Google Cloud Threat Intelligence blog for IOC releases	LOW
HASH	`not disclosed in available public reporting`	INFINITERED malware sample hashes — not publicly released at time of this report; request from Google GTIG directly if you are an affected institution	LOW
URL	`not disclosed in available public reporting`	REDCap exploitation paths and web shell drop locations — specific paths not publicly documented; hunt using behavioral indicators described in detection_guidance	LOW

Framework Mappings

MITRE-ATTACK

- **T1567** — Exfiltration Over Web Service
- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application
- **T1056.001** — Keylogging
- **T1003** — OS Credential Dumping
- **T1098** — Account Manipulation
- **T1505.003** — Web Shell
- **T1114.003** — Email Forwarding Rule
- **T1078** — Valid Accounts
- **T1583** — Acquire Infrastructure
- **T1564** — Hide Artifacts
- **T1560** — Archive Collected Data
- **T1048** — Exfiltration Over Alternative Protocol
- **T1547** — Boot or Logon Autostart Execution

- **T1036** — Masquerading
- **T1588** — Obtain Capabilities
- **T1195** — Supply Chain Compromise
- **T1114** — Email Collection

NIST-800-53R5

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

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

NIST-CSF-2

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

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567	Exfiltration Over Web Service	Exfiltration
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1056.001	Keylogging	Collection
T1003	OS Credential Dumping	Credential-Access
T1098	Account Manipulation	Persistence
T1505.003	Web Shell	Persistence
T1114.003	Email Forwarding Rule	Collection
T1078	Valid Accounts	Defense-Evasion
T1583	Acquire Infrastructure	Resource-Development
T1564	Hide Artifacts	Defense-Evasion
T1560	Archive Collected Data	Collection
T1048	Exfiltration Over Alternative Protocol	Exfiltration
T1547	Boot or Logon Autostart Execution	Persistence
T1036	Masquerading	Defense-Evasion
T1588	Obtain Capabilities	Resource-Development
T1195	Supply Chain Compromise	Initial-Access
T1114	Email Collection	Collection

Sources

Source	URL	Tier
Threat Intelligence	https://cloud.google.com/blog/topics/threat-intelligence/prc-target...	T3
	https://www.sentinelone.com/blog/12-months-of-fighting-cybercrime-d...	T3

Source	URL	Tier
	https://carnegieendowment.org/research/2022/09/the-artificial-intel...	T3
	https://thehackernews.com/2025/04/weekly-recap-vpn-exploits-oracles...	T3
Public and Private Medical Community Targeted by China-Nexus ...	https://cloud.google.com/blog/topics/threat-intelligence/prc-target...	T3

Generated 2026-06-15 13:47 UTC by TJS Security Command Center