INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 07:16 UTC

UNC6508 Targets Medical Research with REDCap-Specific Malware, Exfiltrates Data via Email Compliance Rules

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0477
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	REDCap (medical/scientific research data platform, exposed internet-facing servers); Google Workspace (content compliance rules feature abused for exfiltration)
Published	2026-06-15T10:00:00
Discovery Source	Rss

Executive Summary

A China-linked threat group designated UNC6508 compromised at least one North American medical research organization by exploiting internet-exposed REDCap servers, maintaining undetected access for more than two years, from September 2023 through November 2025. The group deployed a purpose-built backdoor called InfiniteRed, harvested credentials, and exfiltrated sensitive research data by abusing Google Workspace content compliance rules, a novel technique not previously seen from China-nexus actors. Medical and scientific research institutions running internet-facing REDCap installations face immediate risk of data theft, prolonged silent access, and potential loss of proprietary research assets.

Technical Analysis

UNC6508 exploited exposed REDCap servers, a widely used medical and scientific research data management platform, to gain initial access, likely via missing authentication controls (CWE-306) or SQL injection weaknesses in input handling (CWE-89). Post-exploitation activity included deployment of the InfiniteRed backdoor (T1505.003), credential harvesting from stored credentials (T1555, CWE-312), keylogging (T1056.001), and file discovery (T1083). The actor created rogue accounts (T1136), used obfuscation and encoding (T1027, T1140), and staged exfiltration via archive compression (T1560). The novel exfiltration vector abused Google Workspace content compliance rules to silently forward email copies to adversary-controlled destinations (T1114.003), a technique not previously attributed to PRC-linked actors. Lateral movement used proxy infrastructure (T1090.002) and valid accounts (T1078). Malware was staged via remote file transfer

(T1105). No CVE has been assigned to the REDCap access vector. CWE mapping: CWE-306 (missing authentication), CWE-312 (cleartext credential storage), CWE-89 (SQL injection), CWE-494 (insufficient download integrity verification). Google Threat Intelligence Group (GTIG) identified the campaign and released YARA rules and IOCs. Dwell time exceeded 26 months. No patch has been issued for REDCap at this time; remediation requires configuration hardening and access controls.

Action Checklist

1. Step 1: Containment, Immediately restrict external access to all internet-facing REDCap servers; place them behind a VPN or require network-level authentication. Audit firewall rules and confirm no REDCap administrative interfaces are publicly reachable. Block known UNC6508 IOCs released by GTIG at perimeter and endpoint controls.
2. Step 2: Detection, Hunt for InfiniteRed malware using YARA rules published by Google Threat Intelligence Group. Review REDCap server logs for unauthorized account creation (T1136), unexpected file access (T1083), and anomalous inbound connections. In Google Workspace Admin Console, audit all active content compliance rules for unauthorized forwarding destinations, alert on any rule created or modified since September 2023. Review AU-6 (Audit Record Review) logs and correlate with GTIG-released IOCs for IPs, domains, and file hashes.
3. Step 3: Eradication, Remove any unauthorized user accounts from REDCap and Google Workspace. Delete malicious content compliance rules identified in Google Workspace. Wipe and reimage compromised REDCap server instances where InfiniteRed infection is confirmed. Rotate all credentials stored in or accessible from REDCap environments, including service accounts and API keys (per IA-4, Identifier Management). Enforce MFA on all REDCap administrative and Google Workspace accounts (per IA-2, Multi-factor Authentication; CIS 6.3, CIS 6.5).
4. Step 4: Recovery, Validate REDCap servers against a known-good configuration baseline before returning to production (per CM-2, Baseline Configuration). Confirm no residual persistence mechanisms exist, including unauthorized scheduled tasks, startup configurations, or web shells. Re-enable access incrementally, monitoring AU-2 (Event Logging) and AU-6 (Audit Record Review) for anomalous activity. Verify Google Workspace content compliance rules match only authorized configurations.
5. Step 5: Post-Incident, Conduct a full access review against AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges). Assess whether REDCap servers require internet exposure or can be moved to internal-only access. Implement continuous monitoring of Google Workspace admin activity logs per AU-6. Establish a vulnerability management process per CIS 7.1 covering research platforms. Review data classification for all data hosted in REDCap to quantify what was at risk, and report to relevant oversight bodies if regulated research data was exfiltrated.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to legal counsel, the IRB, and institutional HIPAA/research compliance officer if REDCap-hosted data includes human subjects research records, protected health information, or federally funded research data, as the two-year undetected dwell time and confirmed exfiltration via Google Workspace compliance rules likely triggers HIPAA Breach Notification Rule obligations and may require NIH/sponsor reporting under federal grant terms.
Recovery Notes	Before returning any REDCap server to production, validate the rebuilt instance against the official REDCap version checksum from Vanderbilt's REDCap Consortium and confirm all content compliance rules in Google Workspace have been audited and match a documented authorized baseline. Monitor REDCap Admin audit logs and Google Workspace Admin activity logs at least daily for 90 days post-recovery, specifically watching for recurrence of UNC6508 TTPs: new user account creation in REDCap, API token generation events, and any new Gmail content compliance rule targeting external domains. Given the two-year dwell time, assume UNC6508 may have established secondary persistence paths not yet identified and treat any anomalous REDCap administrative action during the monitoring window as a potential re-intrusion indicator requiring immediate triage.
Forensic Artifacts	REDCap `redcap_log_event` database table: contains timestamped records of all user actions within REDCap projects including account creation, data access, and configuration changes — the primary artifact for reconstructing UNC6508's two-year activity timeline within the platform. | InfiniteRed backdoor binary and associated files in REDCap web-accessible directories (e.g., `edocs/`, `temp/`, `modules/`, or custom external module paths): YARA-scannable artifacts that establish the malware's deployment location, compile timestamp, and embedded C2 configuration. | Google Workspace Admin SDK Reports API logs (`application=admin`, `eventName=CREATE_GMAIL_SETTING` and `CHANGE_GMAIL_SETTING`): the definitive source for identifying when UNC6508-created content compliance rules were installed, what filter criteria they used, and the external forwarding destination where exfiltrated research data was sent. | Linux cron jobs (`/var/spool/cron/`, `/etc/cron.d/`, `crontab -l` for all service accounts including `www-data`) and systemd unit files (`/etc/systemd/system/`): persistence mechanism artifacts specific to InfiniteRed's likely server-side implant behavior on a Linux-hosted REDCap instance with multi-year dwell time. | REDCap `redcap_user_information` and `redcap_user_rights` tables: document all accounts and their project-level permissions; accounts created or granted elevated rights between September 2023 and November 2025 that are not in the authorized user roster are direct indicators of UNC6508 credential harvesting and unauthorized account creation activity.

Per-Action IR Details

Step 1: Containment — Immediately restrict external access to all internet-facing REDCap servers; place them behind a VPN or require network-level authentication. Audit firewall rules and confirm no REDCap administrative interfaces are publicly reachable. Block known UNC6508 IOCs released by GTIG at perimeter and endpoint controls.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement), NIST SC — System and Communications Protection (family-level: enforce network boundary controls to restrict REDCap administrative interface exposure), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Use iptables or Windows Firewall (netsh advfirewall) to immediately block all inbound traffic to REDCap's default port (typically TCP 443/80) from non-VPN source ranges. Run `netstat -ano | findstr :443` (Windows) or `ss -tnp | grep :443` (Linux) to enumerate active connections before blocking. Paste GTIG-released IP IOCs into a

deny ACL on your perimeter firewall or host-based firewall rule set. A 2-person team can accomplish this with a pre-staged block-list script run under sudo/admin.

Evidence: Before restricting access, capture volatile network state: run `netstat -ano` / `ss -tnp` and `Get-NetTCPConnection` to document all established and listening connections on the REDCap host; dump active session tokens from the REDCap application session store (typically a database table or PHP session files under `/tmp` or the REDCap `temp/` directory); export current firewall rule sets (`iptables -L -n -v` or `netsh advfirewall firewall show rule name=all`). These artifacts establish which external IPs held live sessions at time of containment and will be destroyed the moment network access is severed.

Step 2: Detection — Hunt for InfiniteRed malware using YARA rules published by Google Threat Intelligence Group. Review REDCap server logs for unauthorized account creation (T1136), unexpected file access (T1083), and anomalous inbound connections. In Google Workspace Admin Console, audit all active content compliance rules for unauthorized forwarding destinations — alert on any rule created or modified since September 2023. Review AU-6 (Audit Record Review) logs and correlate with GTIG-released IOCs for IPs, domains, and file hashes.

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: Run the GTIG-released InfiniteRed YARA rules via `yara -r infinitered.yar /var/www/html/redcap/` (Linux) or `yara64.exe -r infinitered.yar C:\inetpub\wwwroot\redcap\` (Windows) against the REDCap web root. For Google Workspace, use the free Admin SDK Reports API (`GET /admin/reports/v1/activity/users/all/applications/admin`) filtered by `eventName=CREATE_GMAIL_SETTING` and `eventName=CHANGE_GMAIL_SETTING` from 2023-09-01 to present to surface content compliance rule creation/modification events. Parse REDCap's `redcap_log_event` database table for `action` values containing 'Created' or 'Modified' paired with user accounts not in the authorized administrator list.

Evidence: This step is primarily read-only analysis, but before executing any follow-on containment actions: acquire a full memory image of the REDCap server using winpmem (Windows) or LiME kernel module (Linux) to capture InfiniteRed's in-memory footprint, injected code, and any decrypted C2 configuration that may not persist on disk; export REDCap's `redcap_log_event` and `redcap_user_information` database tables in their live state; pull Google Workspace Admin audit logs in raw JSON form via the Reports API before any rules are deleted, as deletion removes the forwarding destination from the audit trail.

Step 3: Eradication — Remove any unauthorized user accounts from REDCap and Google Workspace. Delete malicious content compliance rules identified in Google Workspace. Wipe and reimage compromised REDCap server instances where InfiniteRed infection is confirmed. Rotate all credentials stored in or accessible from REDCap environments, including service accounts and API keys (D3-CRO — Credential Rotation). Enforce MFA on all REDCap administrative and Google Workspace accounts (D3-MFA — Multi-factor Authentication; CIS 6.3, CIS 6.5).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST IA — Identification and Authentication (family-level: enforce MFA on REDCap admin and Google Workspace accounts per IA control family mandate), CIS 5.3 (Disable Dormant Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Export the REDCap `redcap_user_information` table and diff against your authorized user roster to identify rogue accounts created by UNC6508. For credential rotation without a PAM tool, use a scripted approach: generate new API tokens via REDCap's API endpoint (`POST /api/ with token&content=generateNextRecordName` is not relevant — use the Admin interface under Control Center > API Token Manager to revoke and regenerate all tokens). For Google Workspace MFA enforcement on a budget, enable the free Google 2-Step Verification

enforcement policy in Admin Console under Security > 2-Step Verification > Enforcement for the entire domain.

Evidence: Before reimaging REDCap servers: acquire full disk image using `dd if=/dev/sda of=/mnt/evidence/redcap_disk.img bs=4M status=progress` or FTK Imager; capture InfiniteRed binary and all files in the REDCap `temp/`, `edocs/`, and `modules/` directories (UNC6508 likely staged the backdoor within the web-accessible directory tree); export the complete REDCap database (`mysqldump --all-databases`); document all cron jobs (`crontab -l -u www-data`), systemd unit files (`systemctl list-units --type=service`), and web server config files (`/etc/apache2/` or `/etc/nginx/`) that could harbor InfiniteRed persistence mechanisms before the reimage destroys them.

Step 4: Recovery — Validate REDCap servers against a known-good configuration baseline before returning to production. Confirm no residual persistence mechanisms exist, including unauthorized scheduled tasks, startup configurations (D3-SICA — System Init Config Analysis), or web shells. Re-enable access incrementally, monitoring AU-2 (Event Logging) and AU-6 (Audit Record Review) for anomalous activity. Verify Google Workspace content compliance rules match only authorized configurations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST CM — Configuration Management (family-level: validate REDCap server configuration against documented secure baseline per CM family), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Validate the restored REDCap server against the CIS Benchmark for the underlying OS (CIS Apache HTTP Server Benchmark or CIS Ubuntu/RHEL) using the free CIS-CAT Lite scanner. For web shell detection on the rebuilt server, run `find /var/www/html/redcap/ -name '*.php' -newer /var/www/html/redcap/redcap_v*/index.php` to flag PHP files modified after the known-good REDCap installation date. Monitor Google Workspace content compliance rules daily for 30 days post-recovery using the Admin SDK Reports API cron job, alerting on any `CREATE_GMAIL_SETTING` event.

Evidence: This step returns systems to production and alters live state; before re-enabling external access, re-run the GTIG InfiniteRed YARA rules against the freshly restored REDCap web root to confirm clean state; verify file integrity of REDCap core files using MD5/SHA256 hashes from the official REDCap distribution package (available from Vanderbilt's REDCap Consortium); snapshot the current Google Workspace content compliance rule configuration in JSON form as a baseline artifact for future comparison.

Step 5: Post-Incident — Conduct a full access review against AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges). Assess whether REDCap servers require internet exposure or can be moved to internal-only access. Implement continuous monitoring of Google Workspace admin activity logs per AU-6. Establish a vulnerability management process per CIS 7.1 covering research platforms. Review data classification for all data hosted in REDCap to quantify what was at risk, and report to relevant oversight bodies if regulated research data was exfiltrated.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct the access review by exporting REDCap's `redcap_user_rights` and `redcap_user_roles` tables and comparing each user's assigned project-level privileges against their documented job function — flag any account with `design` or `user_rights` privileges not justified by role. For continuous Google Workspace monitoring without a SIEM, deploy a free Apps Script trigger (`ScriptApp.newTrigger('checkComplianceRules').timeBased().everyHours(24).create()`) that calls the Admin SDK Reports API nightly and emails the security team on any new `GMAIL_SETTING` event. For data classification, query the REDCap `redcap_metadata` table for fields tagged with IRB-sensitive identifiers (e.g., fields containing 'SSN',

'DOB', 'MRN') to scope PHI/PII exposure.

Evidence: Assemble the post-incident evidence package: the full timeline reconstructed from REDCap `redcap_log_event` timestamps spanning September 2023 through November 2025; Google Workspace Admin audit log exports showing all content compliance rule creation/modification events and the email addresses to which research data was forwarded; the InfiniteRed binary and any recovered C2 configuration for sharing with CISA and sector ISAC partners; a data inventory report from the REDCap database quantifying the number of records, projects, and data fields potentially exfiltrated — this is required for IRB notification and potential HIPAA breach assessment if the data included human subjects research data.

Detection Guidance

Primary detection path: Deploy GTIG-released YARA rules against REDCap server file systems and memory to identify InfiniteRed malware variants. Cross-reference GTIG-published IOCs (IPs, domains, file hashes) against firewall, proxy, and endpoint logs covering September 2023 forward. In Google Workspace, navigate to Admin Console > Apps > Google Workspace > Gmail > Compliance and audit all content compliance rules for unauthorized recipient forwarding addresses; any rule not matching documented business purpose warrants immediate investigation. Review Google Workspace Admin audit logs for rule creation or modification events. On REDCap servers, examine web server access logs for unusual POST activity, unexpected file uploads, and access to administrative endpoints from external IPs. Hunt for evidence of T1505.003 (web shell deployment) by performing file system analysis on web-accessible directories. Monitor for new local account creation (T1136) and review authentication logs for use of valid credentials from unusual source IPs (T1078). Check for obfuscated scripts and encoded payloads in REDCap server directories (T1027). Behavioral indicators include: outbound connections to unknown external hosts from REDCap servers, email forwarding rules created by non-administrative accounts or with no matching configuration change request in your ticketing system, and credential access from unexpected geographic locations.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`See GTIG published IOC release`	InfiniteRed malware family file hashes published by Google Threat Intelligence Group — retrieve from GTIG advisory at cloud.google.com/blog/topics/threat-intelligence/prc-targets-us-medical-research	HIGH
DOMAIN	`See GTIG published IOC release`	Command-and-control domains associated with UNC6508 InfiniteRed campaign — retrieve from GTIG advisory	HIGH
IP	`See GTIG published IOC release`	UNC6508 infrastructure IPs identified by GTIG — retrieve from GTIG advisory for perimeter blocking	HIGH
URL	`See GTIG published IOC release`	Staging URLs used for InfiniteRed payload delivery (T1105) — retrieve from GTIG advisory	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1056.001** — Keylogging
- **T1078** — Valid Accounts
- **T1505.003** — Web Shell
- **T1027** — Obfuscated Files or Information
- **T1136** — Create Account
- **T1140** — Deobfuscate/Decode Files or Information
- **T1041** — Exfiltration Over C2 Channel
- **T1105** — Ingress Tool Transfer
- **T1555** — Credentials from Password Stores
- **T1190** — Exploit Public-Facing Application
- **T1083** — File and Directory Discovery
- **T1546** — Event Triggered Execution
- **T1560** — Archive Collected Data
- **T1114.003** — Email Forwarding Rule
- **T1059.004** — Unix Shell
- **T1090.002** — External Proxy

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-2** — Baseline Configuration
- **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
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **CM-3** — Configuration Change Control
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures
- **A03:2021** — Injection

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **16.10** — Apply Secure Design Principles in Application Architectures

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1056.001	Keylogging	Collection
T1078	Valid Accounts	Defense-Evasion
T1505.003	Web Shell	Persistence
T1027	Obfuscated Files or Information	Defense-Evasion
T1136	Create Account	Persistence
T1140	Deobfuscate/Decode Files or Information	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1105	Ingress Tool Transfer	Command-And-Control
T1555	Credentials from Password Stores	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1083	File and Directory Discovery	Discovery

Technique ID	Technique Name	Tactic
T1546	Event Triggered Execution	Privilege-Escalation
T1560	Archive Collected Data	Collection
T1114.003	Email Forwarding Rule	Collection
T1059.004	Unix Shell	Execution
T1090.002	External Proxy	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/chinese-hackers-brea...	T3
Public and Private Medical Community Targeted by China-Nexus ...	https://cloud.google.com/blog/topics/threat-intelligence/prc-target...	T3
Deep dive into Google Workspace security: How to make ... - YouTube	https://www.youtube.com/watch?v=6N1MTmNSZAw	T3
Google security overview	https://docs.cloud.google.com/docs/security/overview/whitepaper	T3
Google Workspace Security Features: What to Turn On First (2025)	https://material.security/workspace-resources/google-workspace-secu...	T3

Generated 2026-06-16 07:16 UTC by TJS Security Command Center