INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 07:17 UTC

UNC6508 Turned Google Workspace Against Its Users: Inside a 26-Month Espionage Campaign Targeting US and Canadian Research Networks

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0478
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	REDCap (Research Electronic Data Capture), all versions deployed at affected institutions; Google Workspace (admin-level content compliance feature)
Published	2026-06-15T15:44:06
Discovery Source	Rss

Executive Summary

A China-linked threat actor, UNC6508, ran a 26-month espionage campaign against U.S. and Canadian medical, academic, and military research institutions by first compromising REDCap research data servers, then abusing a native Google Workspace administrative feature to silently redirect sensitive email to attacker-controlled accounts. Because the technique exploits built-in platform functionality rather than malware, it left no traditional forensic artifacts and evaded standard endpoint and network controls throughout the campaign. Organizations holding clinical trial data, defense research, or academic intellectual property face material risk of sustained, undetected data loss with significant regulatory, legal, and reputational consequences.

Technical Analysis

UNC6508 (Google GTIG attribution, high confidence) executed a multi-stage intrusion chain spanning approximately September 2023 through November 2025. Initial access was achieved by exploiting REDCap servers. All publicly released versions of REDCap are considered potentially affected due to authentication weaknesses (CWE-287) and code integrity gaps (CWE-494); no specific version range was disclosed in available source material. Exploitation leveraged CWE-287 (improper authentication) and CWE-494 (download of code without integrity check) to establish server-level footholds (T1190, T1505.003). Credential harvesting (CWE-522, T1003, T1078, T1078.002) then enabled privilege escalation to Google Workspace administrator level. At that point, attackers configured native Workspace content compliance rules (T1114.003) to silently BCC

inbound and outbound email to an attacker-controlled Gmail account (T1020, T1071.003), requiring no custom mail server implant. Additional techniques included account discovery (T1087), account creation (T1136), account manipulation (T1098), trusted relationship abuse (T1199), data from cloud storage (T1530), and authentication modification (T1556). The attack chain produces no malware artifacts on mail infrastructure, no anomalous network egress patterns, and is undetectable by standard EDR or network monitoring. No CVE identifiers are assigned to this campaign; exploitation centers on configuration abuse and credential compromise rather than a patchable software vulnerability. GTIG reports infrastructure disruption; no vendor patch addresses the core technique, which is replicable by any attacker achieving Workspace admin access.

Action Checklist

1. Step 1: Containment, Immediately audit all Google Workspace content compliance rules (Admin Console > Apps > Google Workspace > Gmail > Compliance > Content compliance). Remove any rules not explicitly authorized by your security or mail administration team. Revoke and rotate credentials for all Workspace super-admin and delegated admin accounts. Suspend any admin accounts created outside your documented provisioning process (CIS 5.1, CIS 5.4, NIST AC-2).
2. Step 2: Detection, Query Workspace Admin Audit logs for content compliance rule creation or modification events; filter on actor accounts outside your known admin population and events occurring outside business hours. Review Gmail log search for unexpected BCC delivery routes to external Gmail addresses. On REDCap servers, examine Apache/nginx web server logs, REDCap application audit logs, and OS authentication logs (syslog, /var/log/auth.log on Linux; Event Viewer on Windows) for unauthorized authentication attempts, suspicious file uploads to web-accessible directories, and web shell indicators (unexpected .php or .jsp files in htdocs/webroot with eval, base64_decode, or system() function calls consistent with T1505.003). Cross-reference against NIST AU-6 review cadence requirements.
3. Step 3: Eradication, Harden REDCap server authentication: enforce strong authentication per CWE-287 remediation guidance from your REDCap instance documentation; remove any unauthorized files or web shells identified during log review. Enforce MFA on all Workspace admin accounts (CIS 6.5, D3-MFA). Remove attacker-created accounts and compliance rules identified in Step 2. Rotate all service account credentials and OAuth tokens associated with Workspace admin roles (D3-CRO).
4. Step 4: Recovery, Re-validate the complete list of authorized Workspace content compliance rules against a known-good baseline. Confirm no residual unauthorized admin or forwarding rules remain. Enable enhanced Workspace audit logging and route logs to your SIEM with alerting on compliance rule changes (NIST AU-9, AU-12, CIS 8.2). Verify REDCap server integrity against a clean baseline build. Monitor for re-access attempts from previously identified infrastructure.
5. Step 5: Post-Incident, Conduct a privileged access review across all SaaS platforms to identify accounts with admin rights that were not provisioned through formal processes (NIST AC-2, AC-6, CIS 5.1, CIS 5.4). Implement change alerting for Workspace admin configuration modifications. Assess REDCap deployment hardening against CWE-287, CWE-494, and CWE-522. Develop or update a playbook specifically addressing SaaS administrative configuration abuse as an exfiltration vector. Review email data handling practices against applicable regulatory requirements given the research data types involved.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to legal counsel, institutional privacy officer, and CISA (via CISA's 24/7 line 1-888-282-0870) if any evidence confirms that REDCap research data — particularly data containing human subjects PII, PHI, or export-controlled research — was accessed or exfiltrated via the BCC compliance rule route, as this triggers mandatory breach notification under HIPAA, FERPA, and/or Canadian PIPEDA, and may constitute a reportable incident under federal research security requirements (NSF, NIH, or DoD grant conditions).
Recovery Notes	After eradicating UNC6508's persistence mechanisms, re-introduce REDCap to production only after a clean-baseline rebuild with file integrity verification against Vanderbilt's official distribution checksums — do not restore from a snapshot taken during the compromise window. Given UNC6508's demonstrated 26-month dwell time and the use of native platform functionality rather than malware, maintain heightened monitoring of Workspace Admin Audit logs for `CREATE_EMAIL_ROUTE` events and REDCap authentication logs for credential-stuffing patterns for a minimum of 180 days post-recovery. Coordinate with peer research institutions and sector ISACs (Health-ISAC, REN-ISAC) to share IOCs from attacker-controlled Gmail addresses and source infrastructure identified during the investigation, as UNC6508's targeting pattern suggests parallel campaigns against other research networks may be active.
Forensic Artifacts	Google Workspace Admin Audit Log entries (Admin Console > Reporting > Audit > Admin): specifically events with event name 'CREATE_EMAIL_ROUTE' or 'CHANGE_EMAIL_SETTING' including actor account, source IP, timestamp, and the full rule definition — this is the primary artifact documenting UNC6508's silent BCC exfiltration configuration. | Gmail Log Search export (Admin Console > Reporting > Email Log Search): envelope-level delivery records showing BCC routing to external Gmail addresses for research staff accounts over the full campaign window, revealing the scope of email data exfiltrated to attacker-controlled accounts. | REDCap web server access logs (`/var/log/apache2/access.log` or `/var/log/nginx/access.log`): POST requests to non-standard PHP file paths in REDCap's document upload or temp directories, particularly requests from external IPs with anomalous user-agent strings, documenting the initial web shell deployment used to establish the REDCap foothold. | REDCap filesystem: PHP files in `/var/www/html/redcap/edocs/`, `/temp/`, or application root modified after the last verified clean deployment, identified via `find` with `-newer` flag and confirmed via `grep` for obfuscated PHP execution functions (eval, base64_decode, system) — physical evidence of the T1505.003 web shell implant. | Google Workspace Directory (Admin Console > Directory > Users): export of all accounts with super-admin or delegated admin roles including creation date, last login, and recovery email addresses — attacker-created admin accounts used to configure the content compliance rules will appear here with creation timestamps correlating to the initial REDCap compromise date and out-of-process provisioning metadata.

Per-Action IR Details

Step 1: Containment — Immediately audit all Google Workspace content compliance rules (Admin Console > Apps > Google Workspace > Gmail > Compliance > Content compliance). Remove any rules not explicitly authorized by your security or mail administration team. Revoke and rotate credentials for all Workspace super-admin and delegated admin accounts. Suspend any admin accounts created outside your documented provisioning process (CIS 5.1, CIS 5.4, NIST AC-2).

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-12 (Session Termination), CIS 5.1 (IG1/IG2/IG3) — Establish and Maintain an Inventory of Accounts, CIS 5.4 (IG1/IG2/IG3) — Restrict Administrator Privileges to Dedicated Administrator Accounts, CIS 6.2 (IG1/IG2/IG3) — Establish an Access Revoking Process

Compensating: Export the full content compliance rule list via the Admin SDK Reports API using `gam print adminaudit` (GAM — Google Apps Manager, free open-source tool). Pipe output to a CSV and diff against a previously exported baseline: `gam print adminaudit | diff baseline_compliance_rules.csv -`. For credential rotation without enterprise PAM, use Google's Admin Console bulk password reset under Directory > Users, and manually document each reset with a timestamp. A 2-person team can assign one analyst to audit rules and the other to simultaneously work through account suspension using `gam suspend user ` for each out-of-process account.

Evidence: Before revoking admin credentials or removing compliance rules, capture a full export of the current Workspace Admin Audit log (Admin Console > Reporting > Audit > Admin) filtered for 'Email settings changed' and 'Content compliance rule created/modified' events — this is the only record of UNC6508's rule configuration. Export Gmail log search results (Admin Console > Reporting > Email Log Search) showing BCC routing to external addresses for the past 26 months. Screenshot or API-export the exact rule configuration (conditions, actions, target recipient list) of every content compliance rule present, as removing rules before documentation destroys evidence of the attacker's exfiltration routing logic.

Step 2: Detection — Query Workspace Admin Audit logs for content compliance rule creation or modification events; filter on actor accounts outside your known admin population and events occurring outside business hours. Review Gmail log search for unexpected BCC delivery routes to external Gmail addresses. On REDCap servers, examine web server and application logs for unauthorized authentication attempts, file uploads, and web shell artifacts consistent with T1505.003. Cross-reference against NIST AU-6 review cadence requirements.

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-3 (Content Of Audit Records), CIS 8.2 (IG1/IG2/IG3) — Collect Audit Logs

Compensating: Use the free GAM tool to pull Admin Audit logs via CLI: `gam report admin start 2023-01-01 end 2025-03-04 > admin_audit.csv`, then filter for `EMAIL_SETTINGS_CHANGED` and `CREATE_EMAIL_ROUTE` event names using `grep -E 'EMAIL_SETTINGS|CREATE_EMAIL_ROUTE|CHANGE_EMAIL_SETTING' admin_audit.csv`. For REDCap web shell detection without EDR, run `find /var/www/html/redcap -name '*.php' -newer /var/www/html/redcap/redcap_vX.X.X.zip -exec md5sum {} \;` to identify PHP files modified after the last known-good deployment, and cross-reference against Apache access logs at `/var/log/apache2/access.log` for POST requests to unexpected PHP paths. Use `grep -E 'POST.*(upload|shell|cmd|exec)' /var/log/apache2/access.log` as an initial triage filter.

Evidence: This is a detection/analysis step that does not alter live state on the REDCap host if performed read-only; however, if the REDCap server is suspected to be actively compromised, acquire a RAM image using LiME (Linux Memory Extractor) and capture `netstat -ano` and `ss -tulnp` output BEFORE any log review that involves interactive login to the host. Key artifacts to collect: Workspace Admin Audit log entries showing the actor email, source IP, and timestamp of content compliance rule creation events; Gmail log search entries showing envelope-level BCC routing to attacker-controlled external Gmail addresses (format: `@gmail.com`); REDCap Apache or Nginx access logs (`/var/log/apache2/access.log` or `/var/log/nginx/access.log`) for POST requests to non-standard PHP files, especially in `/edocs/`, `/temp/`, or `/htdocs/` directories; REDCap application authentication logs for credential stuffing patterns against `/redcap/login.php`.

Step 3: Eradication — Harden REDCap server authentication: enforce strong authentication per CWE-287 remediation guidance from your REDCap instance documentation; remove any unauthorized files or web shells identified during log review. Enforce MFA on all Workspace admin accounts (CIS 6.5, D3-MFA). Remove attacker-created accounts and compliance rules identified in Step 2. Rotate all service account credentials and OAuth tokens associated with Workspace admin roles (D3-CRO).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST SI-2 (Flaw Remediation), CIS 6.5 (IG1/IG2/IG3) — Require MFA for Administrative Access, CIS 5.3 (IG1/IG2/IG3) — Disable Dormant Accounts, CIS 4.7

(IG1/IG2/IG3) — Manage Default Accounts on Enterprise Assets and Software

Compensating: For REDCap web shell removal without EDR, after forensic imaging use `find /var/www/html/redcap -type f -name '*.php' | xargs grep -lE '(eval|base64_decode|system|passthru|shell_exec)' > suspected_webshells.txt` and manually review each file. For MFA enforcement on Workspace admin accounts without a commercial MFA platform, enable Google's built-in 2-Step Verification enforcement at the OU level (Admin Console > Security > 2-Step Verification > Enforcement) — this is free and native. For OAuth token revocation, use `gam revoke ` or navigate Admin Console > Security > API Controls > Domain-wide Delegation and remove any unrecognized delegated credentials.

Evidence: Before removing web shells from the REDCap server, acquire a full forensic disk image of the affected REDCap host using `dd if=/dev/sda of=/mnt/evidence/redcap_disk.img bs=4M` or `dc3dd` with hash verification. Before revoking OAuth tokens and rotating service account credentials, export the complete list of current OAuth grants and delegated admin credentials via Admin Console > Security > API Controls so the attacker's specific OAuth application entry and scope grants are preserved as evidence. Capture the web shell file content, permissions (`ls -la`), and inode timestamps (`stat `) before deletion, as modification timestamps may reflect the initial REDCap compromise date and anchor the campaign timeline.

Step 4: Recovery — Re-validate the complete list of authorized Workspace content compliance rules against a known-good baseline. Confirm no residual unauthorized admin or forwarding rules remain. Enable enhanced Workspace audit logging and route logs to your SIEM with alerting on compliance rule changes (NIST AU-9, AU-12, CIS 8.2). Verify REDCap server integrity against a clean baseline build. Monitor for re-access attempts from previously identified infrastructure.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-12 (Audit Record Generation), NIST AU-11 (Audit Record Retention), CIS 8.2 (IG1/IG2/IG3) — Collect Audit Logs, CIS 4.6 (IG1/IG2/IG3) — Securely Manage Enterprise Assets and Software

Compensating: For teams without a SIEM, use Google Workspace Alerts Center (Admin Console > Alerts) and enable the 'Admin settings changed' alert — this provides free near-real-time notification of content compliance rule modifications. Export weekly Admin Audit logs via GAM cron job (`gam report admin > /logs/workspace_admin_$(date +%F).csv`) and diff against the validated baseline using a simple bash script. For REDCap integrity verification without a commercial FIM tool, use `aide --init` to build a fresh AIDE (Advanced Intrusion Detection Environment, free) database post-rebuild, then run `aide --check` daily to detect any subsequent unauthorized file modifications.

Evidence: Before declaring recovery complete and returning REDCap to production, verify that the rebuilt REDCap instance's file hashes match the official REDCap distribution checksums published by Vanderbilt's REDCap Consortium. Monitor Workspace Admin Audit logs specifically for `CREATE_EMAIL_ROUTE` and `CHANGE_EMAIL_SETTING` events for a minimum of 90 days post-recovery, as UNC6508's 26-month dwell time indicates persistent re-entry attempts are likely. Retain all collected Workspace audit logs and REDCap server logs for a minimum of 3 years given the research institution context and potential HIPAA/FERPA regulatory requirements.

Step 5: Post-Incident — Conduct a privileged access review across all SaaS platforms to identify accounts with admin rights that were not provisioned through formal processes (NIST AC-2, AC-6, CIS 5.1, CIS 5.4). Implement change alerting for Workspace admin configuration modifications. Assess REDCap deployment hardening against CWE-287, CWE-494, and CWE-522. Develop or update a playbook specifically addressing SaaS administrative configuration abuse as an exfiltration vector. Develop or update a playbook specifically addressing SaaS administrative configuration abuse as an exfiltration vector. Review email data handling practices against applicable regulatory requirements given the research data types involved.

NIST Phase: Post Incident

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

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 5.1 (IG1/IG2/IG3) — Establish and Maintain an Inventory of Accounts, CIS 5.4

(IG1/IG2/IG3) — Restrict Administrator Privileges to Dedicated Administrator Accounts, CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process, CIS 6.1 (IG1/IG2/IG3) — Establish an Access Granting Process

Compensating: For the privileged access review across SaaS platforms without a commercial CASB or IGA tool, use GAM to enumerate all super-admin and delegated admin accounts: `gam print admins > workspace_admins.csv` and diff against HR provisioning records. For the REDCap hardening assessment without a commercial vulnerability scanner, use Nikto (`nikto -h https://`) for web application surface review and manually audit REDCap's `database.php` and `ldap.php` configuration files for plaintext credentials and insecure authentication settings. Document the new SaaS admin configuration abuse playbook using the NIST 800-61r3 playbook template structure, capturing the specific Admin Audit log event names and Gmail log search queries developed during this incident as detection signatures.

Evidence: Compile the complete incident timeline from Workspace Admin Audit log exports and REDCap server logs, correlating the earliest detected content compliance rule creation event against the REDCap initial compromise indicators to establish the full 26-month intrusion timeline for the lessons-learned record. Preserve all attacker-created account identifiers, external BCC destination addresses, and compliance rule configurations as threat intelligence artifacts for sharing with CISA, the FBI Cyber Division, and sector-specific ISACs (such as the Health-ISAC or REN-ISAC for research and education networks) per NIST 800-61r3 §4 information sharing guidance. Document the regulatory notification obligations triggered by potential exposure of research subjects' data under HIPAA (if PHI was processed in REDCap), FERPA (if student research data was involved), or applicable Canadian provincial privacy law (PIPEDA/provincial health privacy acts) given the campaign's targeting of Canadian institutions.

Detection Guidance

Primary detection surface is Google Workspace Admin Audit Logs. Query for event name 'CREATE_GMAIL_SETTING' and 'CHANGE_GMAIL_SETTING' with setting name containing 'content_compliance' or 'routing'; flag any event where the actor is not in your authorized admin inventory or where the destination includes external Gmail addresses (gmail.com domains not owned by your organization). Secondary surface: Gmail log search for BCC delivery to external accounts on messages that did not have BCC set by the sender. On REDCap hosts, look for web shells (unexpected PHP files in web root, particularly with eval, base64_decode, or system() patterns, T1505.003), anomalous authentication log entries (failed then successful logins from unfamiliar IPs, CWE-287 pattern), and outbound connections to uncommon external hosts. For credential compromise detection, review Workspace login audit logs for admin-role logins from new geolocations or devices. Behavioral indicator: any content compliance rule routing email to an account outside your organization's verified domain space is a high-confidence indicator of compromise. Consult Google Threat Intelligence Group and vendor threat reports (Mandiant, CrowdStrike, etc.) for campaign-specific infrastructure indicators if available.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`gmail.com (attacker-controlled account — specific address not publicly disclosed)`	Google Workspace content compliance rules configured to BCC email to an attacker-controlled Gmail account; specific address not released in available source material	LOW

Framework Mappings

MITRE-ATTACK

- **T1505.003** — Web Shell
- **T1087** — Account Discovery
- **T1098** — Account Manipulation
- **T1199** — Trusted Relationship
- **T1003** — OS Credential Dumping
- **T1136** — Create Account
- **T1530** — Data from Cloud Storage
- **T1071.003** — Mail Protocols
- **T1556** — Modify Authentication Process
- **T1078.002** — Domain Accounts
- **T1190** — Exploit Public-Facing Application
- **T1020** — Automated Exfiltration
- **T1078** — Valid Accounts
- **T1114.003** — Email Forwarding Rule

NIST-800-53R5

- **CM-2** — Baseline Configuration
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures
- **A04:2021** — Insecure Design

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
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **5.2** — Use Unique Passwords
- **8.2** — Collect Audit Logs
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1505.003	Web Shell	Persistence
T1087	Account Discovery	Discovery
T1098	Account Manipulation	Persistence
T1199	Trusted Relationship	Initial-Access
T1003	OS Credential Dumping	Credential-Access
T1136	Create Account	Persistence
T1530	Data from Cloud Storage	Collection
T1071.003	Mail Protocols	Command-And-Control
T1556	Modify Authentication Process	Credential-Access
T1078.002	Domain Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1020	Automated Exfiltration	Exfiltration

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1114.003	Email Forwarding Rule	Collection

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/chinese-hackers-abused-google-wor...	T3
A built-in Google Workspace feature became a Chinese espionage ...	https://thenextweb.com/news/chinese-hackers-unc6508-google-workspac...	T3
REDCap	https://project-redcap.org/	T3
Research Electronic Data Capture (REDCap) - PMC - NIH	https://pmc.ncbi.nlm.nih.gov/articles/PMC5764586/	T1
REDCap | GW Information Technology	https://it.gwu.edu/redcap	T1

Generated 2026-06-16 07:17 UTC by TJS Security Command Center