Cuáles son las extensiones de Chrome que podrían estar robando tus datos de Google y Telegram, según un informe

16/04/2026

Un informe de la firma de seguridad Socket, reproducido por The Hacker News, detectó 108 extensiones maliciosas en la tienda de Chrome que ejecutan ataques tipo ‘prompt injection’ y sustraen datos de usuarios de Google y Telegram. Estas extensiones de Chrome concentran vectores de robo y control que pasan desapercibidos para consumidores y administradores.

Extensiones con alto riesgo

Socket atribuye las piezas a cinco editoras —Yana Project, GameGen, SideGames, Rodeo Games e InterAlt— y advierte que ya acumulan casi **20.000 descargas**. Se publicitan como complementos para **Telegram**, **TikTok** y **YouTube**, herramientas de traducción o juegos de tragaperras, tácticas que facilitan obtener permisos peligrosos en el navegador.

La más grave, según el informe, es una extensión para Telegram: extrae el token que usa la app para autenticar la sesión, lo manda a un script en segundo plano y lo reenvía a un servidor C2. Esa cadena permite **robar inicios de sesión de Telegram cada 15 segundos**, según la investigación de Socket, lo que eleva el riesgo operativo.

Del total, **54 extensiones** explotan OAuth2 para apropiarse de cuentas de Google; otras **45 incorporan una puerta trasera universal** que abre URL arbitrarias al iniciar el navegador. Esos mecanismos facilitan la exfiltración de información y la carga de contenido malicioso sin interacción del usuario.

Cómo operan los ataques

El resto del conjunto monta infraestructuras para sortear controles: **introducen publicidad en YouTube, eliminan barreras de TikTok, inyectan scripts en cada página visitada, reenvían solicitudes de traducción y lanzan direcciones externas al arrancar el navegador**. Esa diversidad complica la detección manual en muchas extensiones de Chrome.

El ataque conocido como '**prompt injection**' busca manipular modelos de lenguaje mediante entradas diseñadas para anular controles. IBM lo resume así: "**el ataque aprovecha las limitaciones de diseño de los sistemas de procesamiento del lenguaje natural de la inteligencia artificial**", y aclara que "la vulnerabilidad permite a los prompt hackers anular las instrucciones de programación originales mediante la incorporación de comandos maliciosos en consultas aparentemente inocentes".

Fuente: La 100