Detectan una extensión de Chrome que secuestra el navegador y roba todas las contraseñas

25/01/2026

Una extensión web, que se presenta como un bloqueador de anuncios legítimo, comenzó a atacar a usuarios de navegadores basados en Chromium.

El complemento no solo provoca que Chrome y Edge se congelen, sino que además instala malware para robar información sensible, incluidas contraseñas de todo tipo de cuentas y credenciales de acceso a billeteras virtuales y homebanking.

La amenaza fue identificada por investigadores de la empresa de ciberseguridad *Huntress*, que atribuyen el ataque a ciberdelincuentes conocidos con el seudónimo KongTuke.

Una extensión de Chrome secuestra tu navegador y roba todas tus contraseñas. (Foto: Reuters/Dado Ruvic).

La técnica utilizada recibe el nombre de**ClickFix**y, en esta variante específica, fue **bautizada como CrashFix** por la forma en que simula fallos críticos del navegador para manipular a las víctimas.

Así funciona la extensión falsa que imita a un bloqueador popular

El complemento malicioso **se distribuye bajo el nombre *NexShield* y se hace pasar por *uBlock Origin Lite***, una versión real y confiable de un bloqueador de anuncios ampliamente utilizado. Según el análisis de *Huntress*, la extensión **aparece entre los primeros resultados** cuando los usuarios buscan alternativas para **bloquear publicidad**, lo que aumenta de forma considerable su tasa de instalación.

Una vez añadida al navegador, *NexShield* **no muestra comportamientos sospechosos inmediatos**. Durante aproximadamente una hora **permanece inactiva**, una estrategia

que refuerza su apariencia legítima y reduce las probabilidades de que el usuario la elimine de manera preventiva.

El ataque se activa después de ese período inicial. En ese momento, la extensión comienza a **consumir de forma excesiva recursos del sistema** y satura la **CPU** y la memoria hasta provocar un bloqueo total del navegador. Para el usuario, la situación se asemeja a un **fallo técnico grave**, sin señales claras de que se trate de una acción intencional.

Luego de forzar el cierre y reiniciar el navegador, **aparece un mensaje de advertencia falso**. El aviso indica que el cierre anterior fue "anómalo" y sugiere realizar un escaneo de seguridad para corregir el supuesto problema. Minutos después, se muestra una nueva pantalla con instrucciones detalladas para "solucionar el error", que incluyen **copiar y ejecutar un comando en el sistema operativo.**

Ese paso es clave para el ataque. Al ejecutar el comando, la víctima descarga e **instala un *script* malicioso** que opera en segundo plano. De acuerdo con los investigadores, este malware permite el **robo de datos almacenados en el equipo** y otorga control remoto al atacante, lo que expone contraseñas, información personal y otros datos críticos.

Qué hacer si la extensión está instalada en Chrome o Edge

Ante la sospecha de tener instalada *NexShield* u otra extensión que imite a *uBlock Origin Lite*, **el primer paso es eliminarla de inmediato desde el administrador de extensiones del navegador.** En Chrome y Edge, basta con ingresar a la sección de complementos, identificar el nombre sospechoso y quitarlo por completo.

Después de desinstalar la extensión, **se recomienda ejecutar un**

análisis completo del sistema con una herramienta de seguridad confiable, ya que el ataque incluye la descarga de malware que puede seguir activo en segundo plano.

También es importante **cambiar todas las contraseñas** utilizadas desde el navegador afectado, en especial las vinculadas a correos electrónicos, cuentas financieras, billeteras virtuales y *homebanking*.

Cuáles son las señales que permiten detectar una extensión maliciosa

Algunas extensiones presentan **indicios claros de riesgo** incluso cuando se distribuyen a través de tiendas oficiales.

Uno de los primeros puntos a revisar son los permisos solicitados: un bloqueador de anuncios no debería requerir acceso total al sistema, a todos los sitios visitados ni a la ejecución de procesos externos al navegador.

El comportamiento también es una señal relevante. Consumo excesivo de CPU o memoria, bloqueos inesperados del **navegador** o mensajes de error que aparecen sin una acción previa del usuario pueden indicar que el complemento ejecuta funciones ajenas a su propósito original.

Otro indicio es la **aparición de mensajes que solicitan acciones manuales fuera del navegador**. Ninguna extensión legítima debería pedir que el usuario copie y ejecute comandos en el sistema operativo para “corregir errores” o “restablecer la seguridad”. Ese tipo de indicaciones suele formar parte de **esquemas de ingeniería social orientados a instalar malware de forma encubierta.**

Un recordatorio sobre los riesgos de las extensiones

El caso de *NexShield* deja en evidencia uno de los **vectores de ataque más subestimados por los usuarios**: las extensiones de navegador. Si bien se distribuyen a través de tiendas oficiales y utilizan nombres similares a herramientas conocidas, estos complementos pueden convertirse en puertas de entrada para campañas de **robo de información** a gran escala.

Es importante también que **ningún bloqueador de anuncios legítimo debería solicitar la ejecución manual de comandos** ni provocar fallos deliberados del sistema. Revisar el nombre exacto del desarrollador, la cantidad de descargas y los permisos solicitados son una de las pocas barreras efectivas frente a este tipo de engaños.

Fuente: TN