Una amenaza de publicidad maliciosa está presenciando un nuevo aumento en la actividad desde su aparición a inicios del año.

Nombrado como ChromeLoader, el malware es un *«secuestrador de navegador generalizado y persistente que modifica la configuración del navegador de sus víctimas y redirige el tráfico del usuario a sitios web de publicidad»,* dijo Aedan Russell, de Red Canary.

ChromeLoader es una extensión falsa del navegador Chrome, y generalmente se distribuye en forma de archivos ISO a través de sitios de pago por instalación y publicaciones en redes sociales que anuncian códigos QR para videojuegos pirateados y películas pirateadas.

Aunque funciona principalmente secuestrando las consultas de búsqueda de los usuarios a Google, Yahoo y Bing, y redirigiendo el tráfico a un sitio web publicitario, también se destaca por el uso de PowerShell para inyectarse en el navegador y agregar la extensión.

El malware, también conocido como Choziosi Loader, fue documentado por primera vez por G DATA a inicios de febrero.

> *«Por ahora, el único propósito es obtener ingresos a través de anuncios no solicitados y secuestro de motores de búsqueda. Pero los cargadores a menudo no se adhieren a una carga útil a largo plazo y los autores de malware mejoran sus proyectos con el tiempo»,* dijo Karsten Hahn de G DATA.

Otra característica de ChromeLoader es su capacidad para redirigir a las víctimas fuera de la página de extensiones de Chrome («chrome://extensiones») en caso de que intenten eliminar el complemento.

Además, los investigadores detectaron una versión macOS del malware que funciona contra los navegadores Chrome y Safari, convirtiendo a ChromeLoader en una amenaza multiplataforma.

> *«Si se aplica a una amenaza de mayor impacto, como un recolector de credenciales o spyware, este comportamiento de PowerShell podría ayudar al malware a establecerse inicialmente y pasar desapercibido antes de realizar una actividad más abiertamente maliciosa, como filtrar datos de las sesiones del navegador de un usuario»*, dijo Russell.