Una red de extensiones fraudulentas para los navegadores web Chrome y Edge están secuestrando los clics a los enlaces en las páginas de resultados de búsqueda a URL arbitrarias, incluyendo sitios de phishing y anuncios.

Colectivamente denominadas como CacheFlow por Avast, las 28 extensiones, entre ellas Video Downloadwe para Facebook, Vimeo Video Downloader, Instagram Story Downloader, VK Unblock, hicieron uso de un truco engañoso para enmascarar su verdadero propósito: Aprovechar el encabezado HTTP de Cache-Control como un canal encubierto para recuperar comandos de un servidor controlado por un atacante.

Google y Microsoft eliminaron todos los complementos del navegador con puerta trasera a partir del 18 de diciembre de 2020, para evitar que más usuarios los descarguen desde tiendas oficiales.

Según los datos de telemetría recopilados por la compañía, los tres principales países infectados fueron Brasil, Ucrania y Francia, seguidos de Argentina, España, Rusia y Estados Unidos.

La secuencia de CacheFlow comenzó cuando usuarios desprevenidos descargaron una de las extensiones en sus navegadores que, luego de la instalación, enviaron solicitudes de análisis que se asemejan a Google Analytics a un servidor remoto, que luego devolvió un encabezado de Cache-Control especialmente diseñado que contiene comandos ocultos para buscar una carga útil de segunda etapa que funcionó como un descargador para la carga útil final de JavaScript.

Este malware de JavaScript acumuló fechas de nacimiento, direcciones de correo electrónico, geolocalización y actividad del dispositivo, con un enfoque específico en la recopilación de datos de Google.

> *«Para recuperar la fecha de nacimiento, CacheFlow hizo una solicitud XHR a https://myaccount.google.com/birthday y analizó la fecha de nacimiento de la respuesta»,* dijeron los investigadores de Avast, Jan Vojtesek y Jan Rubín.

En el paso final, la carga útil inyectó otra pieza de JavaScript en cada pestaña, utilizándola para secuestrar los clics que conducen a sitios web legítimos, así como para modificar los resultados de búsqueda de Google, Bing o Yahoo para redirigir a la víctima a una URL diferente.

Pero además, las extensiones no solo evitaron infectar a los usuarios que probablemente fueran desarrolladores web, algo que se dedujo al calcular una puntuación ponderada de las extensiones instaladas o al verificar si accedían a sitios web alojados localmente, sino que también se configuraron para no mostrar ningún comportamiento sospechoso durante los primeros tres días posteriores a la instalación.

Avast dijo que los innumerables trucos empleados por los autores de malware para escapar de la detección pueden haber sido un factor crucial que le permitió ejecutar código malicioso en segundo plano e infectar sigilosamente a millones de víctimas, con evidencia que sugiere que la campaña puede haber estado activa desde al menos octubre de 2017.

> *«Por lo general, confiamos en que las extensiones instaladas desde las tiendas de navegadores oficiales son seguras. Pero ese no es siempre el caso, como descubrimos recientemente. CacheFlow se destacó particularmente por la forma en que las extensiones maliciosas intentaban ocultar su comando y controlar el tráfico en un canal encubierto utilizando el encabezado HTTP Cache-Control de sus solicitudes de análisis. Creemos que es una técnica nueva»,* dijeron los investigadores.

Se puede acceder a la lista completa de indicadores de compromiso (IoC) asociados con la campaña.