Se encontraron cinco extensiones falsas para el navegador web Google Chrome que se hacen pasar por espectadores de Netflix y otras empresas para rastrear la actividad de navegación de los usuarios y las ganancias de los programas de afiliados minoristas.

> *«Las extensiones ofrecen varias funciones, como permitir a los usuarios ver programas de Netflix juntos, cupones de sitios web y tomar capturas de pantalla de un sitio web. Este último toma prestadas varias frases de otra extesión popular llamada GoFullPage»,* dijeron los investigadores de McAfee, Oliver Devane y Vallabh Chole.

Los complementos del navegador en cuestión, disponibles a través de Chrome Web Store y descargados 1.4 millones de veces, son los siguientes:

- Netflix Party (mmnbenehknklpbendgmgngeaignppnbe) – 800,000 descargas
- Netflix Party (flijnhifgdcbhglkneplegafminjnhn) – 300,000 descargas
- FlipShope – Extensión de rastreador de precios (adikhbfjdbjkhelbdnffogkobkekkkej) – 80,000 descargas
- Captura de pantalla de página completa: captura de pantalla (pojgkmkfincpdkdgjepkmdekcahmckjp) – 200,000 descargas
- Ventas Flash de AutoBuy (gbnahglfafmhaehbdmjedfhdmimjcbed) – 20,000 descargas

Las extensiones están diseñadas para cargar una pieza de JavaScript que es responsable de controlar los sitios web visitados e inyectar código malicioso en los portales de comercio electrónico, lo que permite a los atacantes ganar dinero por medio de programas de afiliados por las compras realizadas por las víctimas.

> *«Cada sitio web visitado se envía a servidores propiedad del creador de la extensión. Hacen esto para que puedan insertar código en los sitios web de comercio electrónico que se visitan. Esta acción modifica las cookies en el sitio para*

> *que los autores de la extensión reciban el pago del afiliado por cualquier artículo comprado»,* dijeron los investigadores.

También se incorpora una técnica que retrasa la actividad maliciosa por 15 días desde el momento de la instalación de la extensión para evitar que se levanten banderas rojas.

Los hallazgos siguen al descubrimiento de 13 extensiones del navegador Chrome en marzo de 2022, que fueron atrapadas redirigiendo a los usuarios de Estados Unidos, Europa e India a sitios de phishing extrayendo información confidencial.

Al momento de escribir, tres de las cuatro extensiones todavía están disponibles en la tienda web, siendo Netflix Party el único plugin que se eliminará. Se recomienda a los usuarios de las extensiones instaladas que las eliminen manualmente de su navegador web Chrome para mitigar más riesgos.