Google ha eliminado 500 extensiones maliciosas para Chrome de su tienda web luego de descubrir que inyectaban anuncios maliciosos y desviaban los datos de navegación de los usuarios a servidores bajo el control de los atacantes.

Estas extensiones fueron parte de una campaña de publicidad fraudulenta que ha estado funcionando al menos desde enero de 2019, aunque la evidencia señala que la posibilidad de que el actor detrás del esquema haya estado activo desde 2017.

Los hallazgos provienen de una investigación conjunta de los investigadores de seguridad cibernética, Jamila Kaya y Duo Security, de Cisco, que analizaron 70 extensiones de Chrome con más de 1.7 millones de instalaciones.

Al compartir los hallazgos en privado con Google, la compañía identificó 430 extensiones de navegador más problemáticas, que desde entonces fueron desactivadas.

Mediante la herramienta de evaluación de seguridad de extensión de Chrome de Duo Security, CRXcavator, los investigadores determinaron que los complementos del navegador funcionaban al conectar subrepticiamente los clientes del navegador a un servidor de comando y control (C2) controlado por el atacante que permitiría filtrar en privado navegar por los datos sin el conocimiento de los usuarios.

Las extensiones, que funcionan bajo la apariencia de promociones y servicios de publicidad, tenían un código fuente casi idéntico pero diferían en los nombres de las funciones, evadiendo de esta forma los mecanismos de detección de Chrome Web Store.

Además de solicitar permisos extensos que otorgan a los complementos acceso al portapapeles y a todas las cookies almacenadas localmente en el navegador, se conectan de forma periódica a un dominio que comparte el mismo nombre que la extensión, por ejemplo, Mapstrekcom, ArcadeYumcom, para buscar instrucciones sobre cómo desinstalarse del navegador.

Al hacer contacto inicial con el sitio, los complementos posteriormente establecieron

contacto con un dominio C2 codificado, por ejemplo, DTSINCEcom, esperar nuevos comandos, las ubicaciones para cargar datos de usuarios y recibir listas actualizadas de anuncios maliciosos y redireccionar dominios, que posteriormente redirigieron las sesiones de navegación de los usuarios a una combinación de sitios legítimos y de phishing.

> *«Una gran parte de estos son flujos de anuncios benignos, que conducen a anuncios como Macy´s, Dell o Best Buy. Algunos de estos anuncios podrían considerarse legítimos, sin embargo, del 60 al 70 por ciento de las veces que se produce una redirección, los flujos de anuncios hacen referencia a un sitio malicioso»,* dice el informe.

Esta no es la primera vez que se descubren extensiones de robo de datos en el navegador web Chrome. En julio pasado, el investigador de seguridad Sam Jadali y The Washington Post, descubrieron una fuga de datos masiva denominada DataSpii, llevada a cabo por extensiones de Chrome y Firefox instaladas en cuatro millones de computadoras.

Estos complementos recopilaron actividad de navegación, incluyendo información de identificación personal, y la compartieron con un agente de datos externo no identificado que lo pasó a una compañía de análisis llamada Nacho Analytics (ahora cerrada), que luego vendió los datos recopilados a su suscripción de miembros en tiempo casi real.

Como respuesta, Google comenzó a exigir extensiones para solicitar solo acceso a *«menor cantidad de datos»* a partir del 15 de octubre de 2019, prohibiendo cualquier extensión que no tenga una política de privacidad y recopile datos acerca de los hábitos de navegación de los usuarios.