Dos extensiones de Google Chrome para bloqueo de anuncios muy utilizadas que se imitan como AdBlock y uBlock Origin, fueron atrapadas rellenando cookies en el navegador web de millones de usuarios para generar ingresos de afiliados a partir de esquemas de referencia de forma fraudulenta.

No hay duda de que las extensiones web agregan muchas funciones útiles a los navegadores web, lo que hace que su experiencia en línea sea excelente y ayuda a la productividad, pero al mismo tiempo, pueden representar grandes amenazas tanto para la privacidad como para la seguridad.

Al ser el enlace más débil con sobrepeso en el modelo de seguridad del navegador, las extensiones se ubican entre la aplicación del navegador e Internet, desde donde buscan los sitios web que se visitan y luego, pueden interceptar, modificar y bloquear cualquier solicitud, en función de las actividades para las que fueron diseñadas.

Además de las extensiones que se crean con fines maliciosos, en los últimos años también se ha visto que algunas de las extensiones legítimas más populares de Chrome y Firefox se vuelven deshonestas luego de obtener una base de usuarios masiva o ser pirateadas.

Descubiertos por investigadores de Adguard, las dos extensiones de Chrome que se mencionan a continuación, se encontraron utilizando los nombres de dos extensiones de bloqueo de anuncios reales y muy populares, en un intento de engañar a la mayoría de los usuarios para que las descarguen.

- AdBlock by AdBlock, Inc. – Más de 800 mil usuarios
- uBlock by Charlie Lee – Más de 850 mil usuarios

Aunque estas extensiones estaban funcionando completamente como cualquier otro bloqueador de anuncios al eliminar los anuncios de páginas que se visitan, los investigadores los vieron realizando *«relleno de cookies»* como un esquema de fraude publicitario para generar ingresos para sus desarrolladores.

¿Qué es el relleno de cookies?

Cookie Stuffing o Cookie Dropping, es uno de los tipos más populares de esquemas de fraude en el que un sitio web o extensión de navegador deja caer un puñado de cookies afiliadas en el navegador web de los usuarios sin su permiso.

Estas cookies de seguimiento de afiliados luego realizan un seguimiento de las actividades de navegación de los usuarios, y si hacen compras en línea, los rellenadores de cookies reclaman comisiones por ventas en las que en realidad no tuvieron parte, robando potencialmente el crédito por la atribución de otra persona de forma fraudulenta.

Se descubrió que las dos extensiones de bloqueo de anuncios descubiertas por los investigadores enviaban una solicitud a una URL para cada nuevo dominio que los usuarios visitaban después de instalarse por aproximadamente 55 horas, en un intento de recibir enlaces de afiliación de los sitios que los usuarios visitaban.

Las dos extensiones, con más de 1.6 millones de usuarios activos, estaban rellenando cookies de 300 sitios web de los sitios más populares de Alexa Top 10000, incluidos Teamviewer, Microsoft, LinkedIn, Aliexpress y booking.com, que potencialmente generaban millones de dólares al mes para sus desarrolladores, según los investigadores.

> *«En realidad, tiene un lado positivo. Ahora que se descubre este esquema de fraude, los propietarios de los programas de afiliados pueden seguir el rastro del dinero y descubrir quién está detrás de este esquema. Otra cosa interesante acerca de esta extensión es que contiene mecanismos de autoprotección. Por ejemplo, detecta si una consola del desarrollador está abierta, para terminar toda actividad sospechosa»,* dijeron los investigadores.

Google eliminó ambas extensiones de la Chrome Web Store

A pesar de haber recibido múltiples informes sobre cómo estas extensiones engañan a los

usuarios en los nombres de otras extensiones más populares, Google no las eliminó de Chrome Web Store, ya que la política de Google permite que varias extensiones tengan el mismo nombre.

Sin embargo, después de que los investigadores de AdGuard informaron sus hallazgos sobre el comportamiento malicioso de las dos extensiones, el gigante tecnológico eliminó las extensiones maliciosas de su tienda.

Debido a que la extensión del navegador toma permiso para acceder a todas las páginas web que se visitan, podría robar las contraseñas de cuentas, por lo que se recomienda instalar la cantidad menor de extensiones posible y solo de desarrolladores confiables.