Se ha detectado que un kit de desarrllo de software (SDK) para iOS, utilizado por más de 1200 aplicaciones, con un total de más de mil millones de usuarios móviles, contiene código malicioso con el objetivo de cometer fraudes de clics en anuncios móviles y capturar información confidencial.

Según un informe publicado por la empresa de seguridad cibernética Snyk, Mintegral, una plataforma de publicidad programática móvil, propiedad de la empresa china de tecnología publicitaria móvil, Mobvista, incluye un componente SDK que le permite recopilar URL, identificadores de dispositivo, dirección IP, versión del sistema operativo y otros datos confidenciales de usuario.

El SDK malicioso para iOS fue nombrado como SourMint por los investigadores de Snyk.

> *«El código malicioso puede espiar la actividad del usuario al registrar solicitudes basadas en URL realizadas a través de la aplicación. Esta actividad se registra en un servidor de terceros y podría incluir información de identificación personal (PII) y otra información confidencial»,* dijo Alyssa Miller, de Snyk.
>
> *«Además, el SDK informa de forma fraudulenta los clics de los usuarios en los anuncios, robando ingresos potenciales de las redes publicitarias de la competencia, y en algunos casos, del desarrollador/editor de la aplicación»,* agregó.

Aunque los nombres de las aplicaciones comprometidas que utilizan el SDK no se han revelado, el código fue descubierto en la versión para iOS del SDM Mintegral (6.3.5.0), y la primera versión del SDK malicioso data del 17 de julio de 2019 (5.5.1). Sin embargo, la versión de Android del SDK parece no estar afectada.

Snyk descubrió que el SDK de Mintegral no solo intercepta los clics en anuncios dentro de una aplicación, sino que también usa esa información para atribuir de forma fraudulenta el clic a su red publicitaria, incluso en los casos en que una red publicitaria de la competencia

haya publicado el anuncio.

Cabe mencionar que las aplicaciones que presentan anuncios en la aplicación incluyen SDK de distintas redes publicitarias con la ayuda de mediadores publicitarios.

> *«Cuando el proveedor de atribución intenta hacer coincidir el evento de instalación con las notificaciones de clics registrados, encuentra dos que coinciden. Utilizando un modelo de atribución de último toque, la notificación de clic de Mintegral recibe la atribución y la notificación de clic de la otra red publicitaria».*

Esto significa que Mintegral ha estado robando ingresos publicitarios de otras redes publicitarias, al reclamar los anuncios de una red diferente como propios, además de despojar a los desarrolladores de sus ingresos aún cuando la plataforma no se utiliza para la publicación de anuncios.

> *«En nuestra investigación, descubrimos que una vez que Mintegral SDK está integrado en una aplicación, intercepta los clics incluso si Mintegral no está habilitado para publicar anuncios. En este caso, los ingresos publicitarios que deberían haber regresado al desarrollador o editor a través de una red publicitaria de la competencia, nunca se pagarán al desarrollador»,* dijo Miller.

Algo que causa más polémica, es que el SDK contiene funciones que están diseñadas para espiar todas las comunicaciones de las aplicaciones afectadas, con el alcance de los datos que se recopilan mucho más de lo que se requiere para la atribución de clics legítimos.

La información registrada incluye la versión del sistema operativo, la dirección IP, el estado de carga, la versión del SDK de Mintegral, el tipo de red, el modelo, el nombre del paquete, el

identificador de publicidad (IDFA o identificador para anunciantes) y más.

> *«Los intentos de Mintegral de ocultar la naturaleza de los datos que se capturan, tanto a través de controles anti manipulación como de una técnica de codificación patentada personalizada, recuerdan una funcionalidad similar informada por investigadores que analizaron la aplicación TikTok»*, dijo Miller.

Aunque no existe forma de que los usuarios sepan si están usando una aplicación que incorpora el SDK de Mintegral, es recomendable que los desarrolladores externos revisen sus aplicaciones y eliminen el SDK para evitar la fuga de datos.

Mientras tanto, Apple incluirá nuevas funciones de privacidad en su próxima actualización de iOS 14, que dificulta que las aplicaciones de terceros rastreen a los usuarios al solicitar su consentimiento explícito para publicar anuncios dirigidos.