Se han descubierto dos kits de desarrollo de software de terceros integrados por más de cientos de miles de aplicaciones de Android que tienen acceso no autorizado a los datos de los usuarios asociados con sus cuentas de redes sociales conectadas.

Twitter publicó en su blog ayer, que un SDK desarrollado por OneAudience contiene un componente que viola la privacidad y que puede haber transmitido algunos de los datos personales de sus usuarios a los servidores de OneAudience.

Luego de la divulgación de Twitter, Facebook lanzó hoy una declaración que revela que un SDK de otra compañía, Mobiburn, también está bajo investigación por una actividad maliciosa similar que podría haber expuesto a sus usuarios conectados con ciertas aplicaciones de Android a empresas de recolección de datos.

Tanto OneAudiencie como Mobiburn son servicios de monetización de datos que pagan a los desarrolladores para que integren sus SDK en las aplicaciones, que luego recopilan los datos de comportamiento de los usuarios y luego los utilizan con los anunciantes para el marketing dirigido.

En general, no se supone que los kits de desarrollo de software de terceros utilizados con fines publicitarios, tengan acceso a la información de identificación personal de los usuarios, contraseñas de cuenta o tokens de acceso secreto generados durante el proceso *«Iniciar sesión con Facebook» o «Iniciar sesión con Twittwer».*

Sin embargo, según los informes, ambos SDK maliciosos contenían la capacidad de recopilar datos no autorizados de forma sigilosa, a los que de otro modo solo había autorizado los desarrolladores de aplicaciones para acceder desde sus cuentas de Twitter o Facebook.

> *«Este problema no se debe a una vulnerabilidad en el software de Twitter, sino a la falta de aislamiento entre los SDK dentro de una aplicación»,* dijo Twitter.

Debido a esto, el rango de datos expuestos se basa en el nivel de acceso que los usuarios

afectados habían proporcionado al conectar sus cuentas de redes sociales a las aplicaciones vulnerables.

Estos datos generalmente incluyen las direcciones de correo electrónico de los usuarios, los nombres de usuario, fotos, tweets, así como tokens de acceso secreto que podrían haber sido mal utilizados para tomar el control de las cuentas de redes sociales conectadas.

> *«Si bien no tenemos evidencia que sugiera que esto se utilizó para tomar el control de una cuenta de Twitter, es posible que una persona pueda hacerlo. Tenemos evidencia de que este SDK se usó para acceder a los datos personales de las personas para al menos algunos titulares de cuentas de Twitter que usan Android, sin embargo, no tenemos evidencia de que la versión iOS de este SDK malicioso esté dirigido a personas que usan Twitter para iOS»,* dijo Twitter.

Twitter también informó a Google y Apple acerca de los SDK maliciosos y sugirió a los usuarios que simplemente eviten descargar aplicaciones de tiendas de apps de terceros y revisen periódicamente las aplicaciones autorizadas.

Mientras tanto, en un comunicado proporcionado a CNBC, Facebook confirmó que ya había eliminado las aplicaciones de su plataforma por violar sus políticas y emitió cartas de cese y desistimiento contra One Audience y Mobiburn.

> *«Los investigadores de seguridad nos notificaron recientemente sobre dos actores malos, One Audience y Mobiburn, que pagaban a los desarrolladores para que usaran kits de desarrollo de software malicioso (SDK) en varias aplicaciones disponibles en tiendas de apps populares»,* dijo Facebook.

Por su parte, OneAudience anunció que cerró su SDK y también proporcionó una declaración en la que dice: *«estos datos nunca fueron destinados a ser recopilados, nunca agregados a*

nuestra base de datos y nunca utilizados».

> *«Actualizamos de forma proactiva nuestro SDK para asegurarnos de que esta información no se pudiera recopilar el 13 de noviembre de 2019. Luego enviamos la nueva versión del SDK a nuestros socios desarrolladores y exigimos que actualicen a esta nueva versión»,* dijo OneAudience.