



Muchas compañías como Air Canada, Hollister y Expedia están registrando cada toque y golpe que se hace en sus aplicaciones para iPhone. El usuario nunca se da cuenta de que eso está ocurriendo.

La mayoría de dichas aplicaciones recopilan datos de los usuarios y algunas, monetizan sus datos sin el consentimiento del usuario. Según TechCrunch, varias aplicaciones para iPhone de hoteles, viajes, aerolíneas, operadores de telefonía, bancos y financieros, saben exactamente cómo se utilizan sus apps.

Lo peor es que aunque las aplicaciones están destinadas a enmascarar ciertos campos, algunos exponen datos confidenciales de forma inadvertida.

Aplicaciones como Abercrombie & Fitch, Hotels.com y Singapore Airlines también utilizan Glassbox, una compañía de análisis de experiencia del cliente, que es una de las pocas empresas que permite a los desarrolladores integrar tecnología de «reproducción de sesión» en sus apps.

Dichas repeticiones de sesión permiten a los desarrolladores de aplicaciones grabar la pantalla y reproducirlas para ver cómo interactúan sus usuarios con la aplicación para averiguar si algo no funcionó o si hubo un error. Cada pulsación, pulsación de botón y entrada de teclado se registra, se captura y se envía a los desarrolladores de aplicaciones.

Glassbox tuiteó recientemente algo referente a su servicio:

«Imagina que tu sitio web o aplicación móvil pueda ver exactamente lo que hacen tus clientes en tiempo real y por qué lo hicieron».

The App Analyst, experto que publican sus análisis de aplicaciones populares en su blog, descubrió que la app para iPhone de Air Canada no ocultaba correctamente las peticiones de la sesión cuando se enviaban, exponiendo los números de pasaportes y datos de tarjetas de crédito en cada sesión de repetición. Unas semanas antes, Air Canada afirmó que su



aplicación tenía una violación de datos, lo que expuso a más de 20 mil perfiles.

«Esto les permite a los empleados de Air Canada, y a cualquier otra persona capaz de acceder a la base de datos de captura de pantalla, ver información de la tarjeta de crédito y la contraseña sin cifrar», dijo el experto a TechCrunch.

The App Analyst examinó una muestra de aplicaciones que Glassbox incluyó en su sitio web como clientes. Mediante Charles Proxy, una herramienta de hombre-en-el-medio utilizada para interceptar los datos enviados desde la aplicación, el investigador podría examinar qué datos estaban saliendo del dispositivo.

No todas las apps filtraban datos enmascarados, ninguna de las aplicaciones que se examinaron mostró que se estaba grabando la pantalla del usuario y mucho menos enviarla a cada compañía o directamente a la nube de Glassbox.

Esto sería un problema en caso de que alguno de los clientes de Glassbox no esté ocultando los datos correctamente.

«Dado que estos datos a menudo se envían de vuelta a los servidores de Glassbox, no me sorprendería si ya hubieran tenido instancias de que capturaron información bancaria y contraseñas confidenciales», dijo el experto.

The App Analyst afirmó que mientras Hollister y Abercrombie & Fitch enviaban sus repeticiones de sesión a Glassbox, otros como Expedia y Hotels.com prefirieron capturar y enviar datos de repetición de sesión a un servidor en su propio dominio. Aseguró también que los datos estaban «en su mayoría confusos», pero en algunos casos vio direcciones de correo electrónico y códigos postales. El investigador dijo que Singapore Airlines también recopiló datos de repetición de sesión, pero los envió a la nube de Glassbox.



Sin analizar los datos de cada aplicación, es imposible saber si una app está grabando las pantallas de un usuario sobre cómo la está utilizando. Además, esto no se encuentra en las políticas de privacidad de las apps.

Las apps que se envían a la App Store de Apple deben tener una política de privacidad, pero ninguna de las aplicaciones que revisamos deja claro en sus políticas que registran la pantalla de un usuario. Glassbox no requiere ningún permiso especial de Apple o del usuario, por lo que no existe forma de que el usuario lo sepa.

La política de Expedia no menciona la grabación de su pantalla, ni la política de Hotels.com. En el caso de Air Canada, no se pudo detectar una sola línea en sus términos y condiciones de iOS o en su política de privacidad que sugiere que la aplicación de iPhone envía datos de pantalla a la aerolínea.

Abercrombie respondió a la solicitud de comentarios al respecto, afirmando que Glassbox *«ayuda a respaldar una experiencia de compra perfecta, lo que nos permite identificar y abordar cualquier problema que los clientes puedan encontrar en su experiencia digital»*.

*«Creo que los usuarios deberían tener un papel activo en la forma en que comparten sus datos, y el primer paso para esto es que las empresas compartan de forma directa cómo recopilan los datos de sus usuarios y con quién los comparten»*, dijo The App Analyst.

Glassbox por su parte, dijo que no obliga a sus clientes a mencionar su uso en su política de privacidad.

*«Glassbox tiene una capacidad única para reconstruir la vista de la aplicación móvil en un formato visual, que es otra vista de los análisis. Glassbox SDK puede interactuar solo con la aplicación nativa de nuestros clientes y, técnicamente, no puede romper el límite de la aplicación. Glassbox no tiene acceso a ella»*, dijo un



| portavoz de la compañía.

Glassbox es uno de los muchos servicios de reproducción de sesiones en el mercado. Appsee comercializa su tecnología de «grabación de usuario» que permite a los desarrolladores *«ver su aplicación a través de los ojos de su usuario»*, mientras que UXCam afirma que les permite a los desarrolladores *«ver grabaciones de las sesiones de sus usuarios, incluidos todos sus gestos y eventos desencadenados»*.

Esta no es una industria que podría desaparecer pronto, las compañías confían en este tipo de datos de repetición de sesión para comprender por qué no funcionan las cosas, lo que puede ser costoso en situaciones de altos riesgos.

Pero el hecho de que los desarrolladores de apps no lo divulguen solo sirve para mostrar qué tan polémico es esto.