Facebook ha estado pagando en secreto a personas para que instalen una VPN de *«Investigación de Facebook»,* que le permite a la compañía tomar datos como el teléfono del usuario y la actividad en Internet, similar a la aplicación Onavo Protect de Facebook, que Apple prohibió en junio y eliminó en agosto.

La red social esquiva a App Store y recompensa a los usuarios por descargar la app de investigación y dar acceso root, lo que podría ser una violación a la política de Apple para que la red social pueda descifrar y analizar su actividad telefónica, según investigaciones de TechCrunch.

Facebook admitió que estaba ejecutando dicho programa de investigación para recopilar datos acerca de los hábitos de uso, y que no tiene planes para detenerlo.

Desde 2016, Facebook ha pagado a los usuarios de 13 a 35 años de edad, hasta 20 dólares al mes más comisión por referencia para vender su privacidad mediante la instalación de la app «Facebook Research» para iOS o Android. Facebook pidió a los usuarios que capturen su página de historial de pedidos de Amazon.

El programa se administra por medio de los servicios de pruebas beta Applause, BetaBound y uTest para encubrir la participación de Facebook, y en un documento, se menciona el «Proyecto Atlas», un nombre apropiado para el esfuerzo de Facebook por mapear nuevas tendencias y rivales en todo el mundo.

TechCrunch pidió a Will Strafach, experto en seguridad de Guardian Mobile Firewall, que busque en la app de investigación de Facebook, a lo que Will respondió lo siguiente:

> *«Si Facebook utiliza completamente el nivel de acceso que reciben al pedirles a los usuarios que instalen el certificado, tendrán la posibilidad de recopilar continuamente los siguientes tipos de datos: mensajes privados en aplicaciones de redes sociales, chats desde aplicaciones de mensajería instantánea, incluyendo fotos / videos enviados a otros, correos electrónicos, búsquedas en la web,*

> *actividad de navegación web e incluso información de ubicación continua al acceder a las fuentes de cualquier aplicación de seguimiento de ubicación que pueda haber instalado»*.

Aún no está claro a qué datos se refiere Facebook, pero obtiene un acceso casi ilimitado al dispositivo de un usuario una vez que instala la aplicación.

Esta estrategia muestra qué tan lejos está dispuesto a llegar Facebook, además de cuánto está dispuesto a pagar para proteger su dominio, incluso corriendo el riesgo de romper las reglas de la tienda de Apple, ya que esta última compañía podría impedir que Facebook siga distribuyendo su app de investigación, o incluso, revocar su permiso para ofrecer apps solo para empleados, y la situación podría relajar aún más relaciones entre los gigantes tecnológicos.

Tim Cook, CEO de Apple, ha criticado repetidamente las prácticas de recopilación de datos de Facebook. La red social ha hecho caso omiso a las políticas de iOS para absorber más información, por lo que podría convertirse en un nuevo punto de discusión.

> *«El escalón bastante técnico de instalar nuestro certificado raíz es atroz. Esto proporciona a Facebook el acceso continuo a los datos más confidenciales sobre usted, y la mayoría de los usuarios no podrán dar su consentimiento de forma razonable a pesar de cualquier acuerdo que firmen, ya que no hay una buena manera de expresar cuánta potencia se entrega a Facebook cuando hagas esto»*, dijo Strafach.

Facebook entró por primera vez en el negocio de la detección de datos cuando adquirió Onavo, por unos 120 millones de dólares en 2014. La app VPN ayudó a los usuarios a rastrear y minimizar el uso de su plan de datos móviles, pero también le dio a Facebook análisis profundos sobre qué otras aplicaciones estaban utilizando.

Los documentos internos adquiridos por Charlie Warzel y Ryan Mac de BuzzFeed News, revelan que Facebook pudo aprovechar Onavo para saber que WhatsApp estaba enviando más del doble de mensajes por día que Facebook Messenger. Onavo le permitió a Facebook detectar el gran ascenso de WhatsApp y justificar el pago de 19 mil millones de dólares para comprar la startup en 2014. Desde entonces, WhatsApp ha triplicado su base de usuarios, lo que demuestra el poder de la previsión de Onavo.

A lo largo de los años, Onavo realizó seguimiento a Facebook sobre qué aplicaciones copiar, características para construir y fracasos para evitar. Para 2018, Facebook estaba promocionando la aplicación Onavo en un marcador de protección de la app principal de Facebook con la esperanza de que más usuarios pudieran espiar.

Facebook también lanzó la aplicación Onavo Bolt que le permite bloquear aplicaciones detrás de un código de acceso o huella digital mientras lo vigila, pero Facebook cerró la aplicación cuando se descubrió y ocasionó críticas relacionadas con privacidad. La aplicación principal de Onavo permanece disponible en Play Store de Google, y se ha instalado más de 10 millones de veces.

El problema se intensificó cuando el experto en seguridad Strafach explicó en marzo pasado cómo Onavo Protect informaba a Facebook cuando la pantalla de un usuario estaba encendida o apagada, y el uso de datos de WiFi y datos celulares, además de calcular el tiempo en que el VPN estaba apagado.

En junio, Apple actualizó sus políticas de desarrollador para prohibir la recopilación de datos acerca del uso de otras aplicaciones o datos que no son necesarios para que una app funcione. Apple informó a Facebook en agosto que Onavo Protect violó dichas políticas de recopilación de datos y que la red social necesitaba eliminarlo de la App Store, lo que hizo luego, según informó Deepa Seetharaman, del Wall Street Journal.

Proyecto Atlas

TechCrunch recibió hace poco una sugerencia que indica que aunque Onavo Protect fue eliminada por Apple, Facebook le estaba pagando a los usuarios por descargar una app VPN similar, bajo el nombre de Facebook Research fuera de la App Store. Al investigarlo, se encontró que Facebook estaba trabajando con tres servicios de prueba de aplicaciones beta para distribuir la aplicación de investigación de Facebook: BetaBound, uTest y Applause.

Facebook comenzó a distribuir la aplicación Research VPN en 2016, a la que se conoce como Proyecto Atlas, desde mediados de 2018, aproximadamente cuando se magnificó la reacción de Onavo Protect y Apple instituyó nuevas reglas para prohibir Onavo.

La red social no quiso dejar de recopilar datos sobre el uso del teléfono por parte de las personas, por lo que el programa de investigación siguió sin tomar en cuenta que Apple prohibió Onavo Protect.

Los anuncios, (como el que se muestra en la siguiente imagen), del programa administrado por uTest en Instagram y Snapchat buscaron a adolescentes de 13 a 17 años de edad para un *«estudio de investigación de medios sociales pagado».* La página de registro para el programa de investigación de Facebook administrada por Applause no menciona a Facebook, pero busca usuarios con edad de 13 a 35 años, requiriendo el consentimiento de los padres para edades entre 13 y 17.

Anuncio del Proyecto Atlas pidiendo acceso a la ubicación

Si los menores intentan registrarse, se les pide que obtengan el permiso de sus padres por medio de un formulario que revele la participación de Facebook y dice que *«no hay riesgos conocidos asociados con el proyecto, sin embargo, usted reconoce que la naturaleza inherente del proyecto implica el seguimiento de la información personal a través del uso de las aplicaciones por parte de su hijo. Applause lo compensará por la participación de su hijo».*

Para los niños con poco dinero, los pagos podrían obligarlos a vender su privacidad a Facebook. El sitio web de Applause explica qué datos podrían recopilarse con la app de investigación de Facebook.

> *«Al instalar el software, le está dando permiso a nuestro cliente para recopilar datos de su teléfono que les ayudará a entender cómo navega por Internet y cómo utiliza las funciones de las aplicaciones que ha instalado... Esto significa que le está permitiendo a nuestro cliente recopilar información como qué aplicaciones están en su teléfono, cómo y cuándo las usa, datos sobre sus actividades y contenido dentro de esas aplicaciones, y cómo otras personas interactúan con usted o su contenido dentro de ellas. También le está permitiendo a nuestro cliente recopilar información sobre su actividad de navegación en Internet (incluidos los sitios web que visita y los datos que se intercambian entre su dispositivo y esos sitios web) y su uso de otros servicios en línea. Hay algunos casos en los que nuestro cliente recopilará esta información, incluso cuando la aplicación utilice el cifrado, o desde sesiones de navegador seguro».*

Mientras tanto, la página de registro de BetaBound, con una URL que temrina en «Atlas», explica que *«por 20 dólares al mes (por medio de tarjetas de regalo electrónicas), instalará una aplicación en su teléfono y la dejará en segundo plano».* Lo que significa que ofrece 20 dólares por amigo que se recomiende. El sitio tampoco menciona a Facebook en un inicio, pero el manual de instrucciones para instalar Facebook Research revela la participación de la compañía.

Al parecer, Facebook ha evitado a propósito TestFlight, el sistema de prueba beta oficial de Apple, que requiere que Apple revise las aplicaciones y además, está limitado a 10 mil participantes. En su lugar, el manual de instrucciones revela que los usuarios descargan la aplicación desde r.facebook-program.com y se les dice que instalen un Certificado de Desarrollador Empresarial y una VPN con un Facebook «confiable» con acceso root al teléfono, además de gran parte de los datos que transmite.

Apple requiere que los desarrolladores acepten utilizar solo este sistema de certificado para distribuir aplicaciones corporativas internas a sus propios empleados. El reclutamiento aleatorio de evaluadores y el pago de una tarifa mensual parece violar el espíritu de dicha regla.

Una vez instalado, los usuarios solo tenían que mantener la VPN funcionando y enviar datos a Facebook para poder recibir el pago. El programa administrado por Applause solicitó que los usuarios capturaran su página de pedidos de Amazon. Estos datos podrían ayudar a Facebook a relacionar los hábitos de navegación y el uso de otras aplicaciones con preferencias y comportamientos de compra. Esa información podría aprovecharse para identificar la orientación de anuncios y comprender qué tipos de usuarios compran qué tipos de productos.

TechCrunch pidió a Strafach analizar la aplicación de investigación de Facebook y descubrió dónde estaba enviando los datos. Confirmó que los datos se enrutan a «vpn-sjc1.v.facebook-program.com» que está asociado con la dirección IP de Onavo, y que el dominio facebook-program.com está registrado en Facebook, según MarkMonitor.

La aplicación se puede actualizar a sí misma sin tener que interactuar con la App Store, y está vinculada a la dirección de correo electrónico PeopleJourney@fb.com. También descubrió que el Certificado de Empresa indica que Facebook lo renovó el 27 de junio de 2018, semanas después de que Apple anunciara sus nuevas reglas que prohibían la app similar de Onavo Protect.

Aún es difícil saber qué datos está guardando realmente Facebook. La única información que se puede conocer aquí es qué acceso a Facebook puede basarse en el código de la aplicación. Strafach explica que se trata de algo muy preocupante.

> *«Podrían responder y afirmar que solo retienen/guardan datos limitados muy específicos, y eso podría ser cierto, realmente se reduce a cuánto confías en la palabra de Facebook. La narrativa más caritativa de esta situación sería que*

> *Facebook no pensó demasiado en el nivel de acceso que se otorgaban a sí mismos... el que es un nivel sorprendente de descuido en sí mismo si ese es el caso».*