Un equipo de investigadores del Instituto Internacional de Ciencias de la Computación, en California, reveló que los desarrolladores de apps móviles están utilizando técnicas de sombra para recopilar datos de los usuarios, aún después de denegar los permisos.

En la conferencia *«50 formas de verter sus datos»* [Descargar], en PrivacyCon, organizada por la Comisión Federal de Comercio el pasado jueves, los investigadores presentaron sus hallazgos describiendo cómo más de 1,300 aplicaciones de Android están recolectando los datos precisos de geolocalización de los usuarios e identificadores de teléfono, incluso cuando los usuarios han denegado explícitamente los permisos requeridos para tales acciones.

> *«Las aplicaciones pueden eludir el modelo de permiso y obtener acceso a datos protegidos sin el consentimiento del usuario, mediante el uso de canales ocultos y laterales. Estos canales se producen cuando hay un medio alternativo para acceder al recurso protegido que no es auditado por el mecanismo de seguridad, dejando el recurso desprotegido»,* dijeron los investigadores.

Los investigadores han estudiado más de 88 mil aplicaciones de la tienda de Google, de las cuales, 1,325 violan los sistemas de permisos dentro del sistema operativo Android, utilizando soluciones ocultas que les permiten buscar datos personales de los usuarios de fuentes como metadatos almacenados en fotos y Wi-Fi.

Como ejemplo, encontraron una app de edición de fotos, llamada Shutterfly, que recopila los datos de ubicación de un dispositivo al extraer las coordenadas GPS de los metadatos de las fotos, como un canal lateral, incluso cuando los usuarios denegaron el permiso a la aplicación.

> *«Observamos que la app Shutterfly (com.shutterfly) envía datos precisos de geolocalización a su propio servidor (apcmobile.thislife.com) sin tener permisos de ubicación».*

Además, se debe tener en cuenta que si una app puede acceder a la ubicación del usuario, todos los servicios de terceros integrados en dicha aplicación también pueden acceder a ella.

Por otro lado, los investigadores encontraron otras 13 aplicaciones con más de 17 millones de instalaciones que acceden al IMEI del teléfono, un identificador de teléfono persistente, almacenado sin protección en la tarjeta SD de un teléfono por otras apps.

> *«Android protege el acceso al IMEI del teléfono con el permiso READ_PHONE_STATE. Identificamos dos servicios en línea de terceros que usan diferentes canales ocultos para acceder al IMEI cuando la app no tiene el permiso requerido para acceder al IMEI».*

Según los investigadores, las bibliotecas de terceros proporcionadas por dos compañías chinas, Baidu y Salmonads, también utilizan esta técnica como un canal encubierto para recopilar datos a los que de otra forma no tenían permiso para acceder.

Otras aplicaciones utilizan la dirección MAC del punto de acceso WiFi para determinar la ubicación del usuario. Se encontró que las apps que funcionan como controles remotos inteligentes, que de otra forma no necesitan información de ubicación para funcionar, recopilan datos de ubicación de esta forma.

> *«Descubrimos que las compañías obtuvieron las direcciones MAC de las estaciones base WiFi conectadas de la memoria caché ARP. Esto se puede utilizar como un sustituto de los datos de ubicación. Encontramos 5 apps que explotan esta vulnerabilidad y 5 con el código pertinente para hacerlo. Además, conocer la dirección MAC de un enrutador permite vincular diferentes dispositivos que comparten acceso a Internet, lo que puede revelar las relaciones personales de sus respectivos propietarios o habilitar el seguimiento entre dispositivos»,* dijeron los investigadores.

En su estudio, los investigadores probaron con éxito estas aplicaciones en versiones instrumentadas de Android Marshmallow y Android Pie.

Los investigadores informaron de sus hallazgos a Google en septiembre pasado, y la compañía pagó a su equipo una recompensa por divulgar los problemas de manera responsable, pero las correcciones serán lanzadas con el lanzamiento de Android Q, a finales del verano.

La actualización de Android Q solucionará los problemas ocultando los datos de ubicación en las fotos de apps de terceros, así como al obligar a las aplicaciones que acceden a WiFi a tener permiso para accedes a los datos de ubicación.

Hasta entonces, se recomienda a los usuarios no confiar en aplicaciones de terceros y que desactiven la configuración de permisos de ubicación e ID para las apps que realmente no las necesitan para funcionar.