11 millones de usuarios afectados por apps que espían sus datos

Un estudio señala que diferentes aplicaciones recopilan el historial de navegación. Aun no se conoce con quién se comparte la información.

¿Cómo protegerse?

Varias aplicaciones de la compañía Big Star Labs espían la información de más de 11 millones de usuarios. Lo afirma un estudio del bloqueador de publicidad de AdGuard, que revela cómo recopilan el historial de navegación de sus usuarios. Se trata de una nueva campaña de spyware.

Son aplicaciones catalogadas como maliciosas. Pueden monitorear comunicaciones, robar información, y utilizar el dispositivo infectado de la víctima como si fuera propio.

En este caso, AdGuard descubrió varias extensiones, a través de Google Chrome y Mozilla Firefox para Android e iOS, y apps móviles que recopilan, de manera invisible, el historial de navegación de los usuarios. Se desconoce aún con quién se comparte la información.

La lista completa de las apps y extensiones sospechosas:

- Block Site
- AdblockPrime
- Speed Booster
- Battery Saver
- AppLock
- Clean Droid
- Poper Blocker
- CrxMouse

Todas estas apps sirven para optimizar el rendimiento del smartphone o brindar capas de protección a las apps, entre otras funciones. Por ejemplo, AppLock sirve para que las aplicaciones tengan contraseña o patrón de acceso.

Estas herramientas dicen recopilar datos no personales o anónimos. Pero, según AdGuard, existen muchas formas de descubrir fácilmente la identidad real de un usuario al observar su historial de navegación.

Según un estudio de investigadores de las universidades de Princeton y Stanford, el comportamiento en línea de un usuario determinado se puede identificar al vincularlo con historias de navegación web anónimas y con perfiles de redes sociales.

Además, el problema no solo es que una compañía sepa quién y cómo es el usuario que descarga una app. Esos datos se pueden compartir, vender y combinar con datos de otras fuentes. En definitiva, según indica AdGuard, el producto final es el perfil completo de una persona.

Otros casos

A fines de 2017, varias empresas debieron remover una cantidad importante de aplicaciones de sus tiendas. "Todas tenían en común el hecho de tener integrado un software de publicidad malicioso llamado IGEXIN, que incluía un código para el robo de información", explica a Infobae Martín Fuentes, gerente de seguridad de negocios de CenturyLink LATAM.

"Las aplicaciones afectadas eran de los más diversos tipos y fueron descargadas millones de veces. Debido a su riesgo, debieron ser eliminadas de inmediato del store o reemplazadas por versiones no afectadas", señala.

Ese mismo año, se descubrió una nueva variante de spyware que era capaz de robar una enorme cantidad de información de los usuarios, incluyendo mensajes de texto, correos, fotografías, datos de ubicación y demás. "Si bien el impacto fue muy bajo, este spyware de nombre Lipizzan podría haber tenido gran impacto de no haberse detectado oportunamente", asegura.

Continúa: "Otro caso fue el de SonicSpy que, enmascarado como una aplicación de mensajería, realizaba varias actividades maliciosas, incluyendo la grabación de llamadas y audio del micrófono, el uso no autorizado de la cámara del dispositivo y el envío de mensaje de textos a números elegidos por el atacante. Robaba además información asociada a logs de llamadas, contactos y Access Point empleados, lo que fácilmente podría haber sido usado para ubicar al usuario".

Cómo protegerse

En principio, Santiago Pontiroli, analista de seguridad para Kaspersky Lab., dice a Infobae: "Si bien descargar la aplicación de una tienda oficial siempre es lo más recomendable, no siempre garantiza que la misma no posea ningún código malicioso".

Y agrega: "Podemos leer las reseñas escritas por los usuarios, cantidad de descargas, si el desarrollador tiene otras aplicaciones publicadas, etc. Sin embargo, hoy en día todo esto puede ser falsificado y creado de forma automática por los cibercriminales por lo que, en última instancia, la mejor forma de evaluar aquello que instalaremos en nuestro dispositivo es a través de los permisos que requiere".

Según Pontiroli, teniendo en cuenta los permisos y el tipo de aplicación, el usuario podría evaluar entonces si algo no está bien. "Pocas aplicaciones deberían tener acceso a toda nuestra lista de contactos, o a monitorear llamadas y mensajes, por lo que es una forma básica de poder dar cuenta que algo está mal", manifiesta.

¿Qué ajustes debemos hacer?

Entre las medidas que podemos implementar, el experto sugiere:

- Descargar aplicaciones solo de las tiendas oficiales y no habilitar la opción de instalación de aplicaciones de sitios de terceros.
- Elegir aplicaciones publicadas por desarrolladores con buena reputación.
- Verificar las reseñas y cantidad de descargas de los usuarios.
- Poner especial atención a los permisos requeridos por la aplicación.
- Utilizar una solución de seguridad para dispositivos móviles. El malware no solo afecta a equipos de escritorio y debemos proteger todos los frentes.

Fuente:https://www.infobae.com/america/tecno/2018/08/05/11-millones-de-usuarios-afectados-por-apps-que-espian-sus-datos/