Más de 4000 aplicaciones de Android que utilizan las bases de datos Firebase alojadas en la nube de Google, están filtrando *«sin saberlo»*, información confidencial de sus usuarios, incluyendo direcciones de correo electrónico, nombres de usuario, contraseñas, números de teléfono, nombres completos, mensajes de chat y datos de ubicación.

La investigación, dirigida por Bob Diachenko de Security Discovery en asociación con Comparitech, es el resultado del análisis de 15,735 aplicaciones de Android, que forman aproximadamente el 18 por ciento de todas las apps en la Google Play Store.

> *«El 4.8 por ciento de las aplicaciones móviles que usan Google Firebase para almacenar datos de los usuarios no están protegidas adecuadamente, lo que permite a cualquiera acceder a bases de datos que contienen información personal de los usuarios, tokens de acceso y otros datos sin una contraseña o cualquier otro método de autenticación»*, dijo Comparitech.

Adquirido por Google en 2014, Firebase es una popular plataforma de desarrollo de aplicaciones móviles que ofrece una variedad de herramientas para ayudar a los desarrolladores de aplicaciones de terceros a crear aplicaciones, almacenar gratuitamente datos y archivos de aplicaciones, solucionar problemas e incluso, interactuar con los usuarios por medio de mensajes de texto.

Las aplicaciones vulnerables, que abarcan principalmente categorías de juegos, educación, entretenimiento y negocios, han sido instaladas 4.22 mil millones de veces por usuarios de Android. Comparitech asegura que *«hay muchas posibilidades de que la privacidad de un usuario de Android se haya visto comprometida por al menos una aplicación».*

Debido a que Firebase es una herramienta multiplataforma, los investigadores también advirtieron que es probable que las configuraciones incorrectas también afecten a las aplicaciones web y iOS.

El contenido completo de la base de datos, que abarca 4,282 aplicaciones, incluye:

- Direcciones de correo electrónico: más de 7,000,000
- Nombres de usuario: más de 4,400,000
- Contraseñas: más de 1,000,000
- Números de teléfono: más de 5,300,000
- Nombres completos: más de 18,300,000
- Mensajes de chat: más de 6,800,000
- Datos GPS: más de 6,200,000
- Direcciones IP: más de 156,000
- Direcciones: más de 560,000

Diachenko encontró las bases de datos expuestas utilizando la API REST de Firebase conocida que se utiliza para acceder a los datos almacenados en instancias desprotegidas, recuperados en formato JSON, con el sufijo «.jason» a una URL de la base de datos.

Además de 155,066 aplicaciones que tienen bases de datos expuestas públicamente, los investigadores encontraron 9014 aplicaciones con permisos de escritura, lo que potencialmente permite a un atacante inyectar datos maliciosos y corromper la base de datos, e incluso propagar malware.

Además, la indexación de URL de bases de datos de Firebase por motores de búsqueda como Bing, expone los puntos finales vulnerables para cualquier persona en Internet.

Después de notificar a Google sobre esto el 22 de abril, la compañía dijo que se está comunicando con los desarrolladores afectados para solucionar el problema.

Esta no es la primera vez que las bases de datos expuestas de Firebase filtran información personal. Investigadores de la compañía de seguridad móvil Appthority encontraron un caso parecido hace dos años, lo que resultó en la exposición de 100 millones de registros de datos.

Dejar una base de datos expuesta sin autenticación es una invitación abierta para los

hackers. Por lo tanto, es recomendable que los desarrolladores de apps se adhieran a las reglas de la base de datos de Firebase para proteger los datos y evitar acceso no autorizado.