

8 apps peligrosas que hay que eliminar de todo celular Android

Como parte de un proceso de depuración de contenido en la tienda digital de Google, Play Store ha anunciado que ha encontrado una serie de programas que podrían estar poniendo en peligro los dispositivos de todas las personas que hayan alcanzado a descargarlos cuando estuvieron disponibles en la plataforma.

A pesar de los controles tradicionales de seguridad con los que cuenta la tienda Play Store, cada temporada se hacen revisiones para confirmar que las aplicaciones disponibles cumplan con los requisitos de seguridad y no incluyan virus ni algún tipo de malware. Sin embargo, hay ciertas ocasiones en las que apps se saltan los controles y quedan abiertas al público por un tiempo.

En la última revisión hecha por la tienda de Google se encontraron **8 aplicaciones** en específico que estarían transmitiendo un peligroso virus de ransomware llamado '**Joker**', el cual estaría tomando control de los celulares de forma silenciosa para adquirir acceso a información personal de los usuarios y tomar control parcial de las tarjetas SIM.

Este virus en específico estaría registrando a los usuarios a diversos **servicios de pago mediante SMS como esquema de robo a largo plazo** por el cual estaría estafando a varias personas sin que se den cuenta. Un detalle notable de tales casos se puede ver en el registro de mensajes del dispositivo o, para mayor seguridad, en las facturas de pagos para los servicios telefónicos pues se encontrarán pagos a suscripciones no reconocidas.

Las aplicaciones reconocidas como potencialmente peligrosas que cuentan con el ransomware mencionado serían las siguientes:

- Auxiliary Message
- Element Scanner
- Fast Magic SMS
- Free CamScanner
- Go Messages
- Super Message

- Super SMS
- Travel Wallpapers

Para los usuarios que hayan descargado alguna de las aplicaciones en la lista es recomendado **eliminar de inmediato el software en cuestión** y todos los datos del mismo que estén presentes en el teléfono. Es necesario asegurarse de que tanto el programa ejecutable como el **archivo APK** queden completamente eliminados para que el dispositivo no se encuentre en peligro de estafa.

Por otra parte, la empresa de ciberseguridad *Zscaler* también ha mencionado que ese mismo virus podría estar presente en otras apps que aún se pueden encontrar en la tienda, las cuales serían:

- Free Affluent Message
- PDF Photo Scanner
- Delux Keyboard
- Comply QR Scanner
- PDF Converter Scanner
- Font Style Keyboard
- Translate Free
- Saying Message
- Private Message
- Read Scanner
- Print Scanner

Como medida preventiva lo más pertinente en caso de contar con tales aplicaciones en el teléfono es realizar el mismo proceso de eliminación completa de datos relacionados. Además, en caso de querer asegurarse de eliminar el virus por completo del dispositivo también es aconsejable instalar y usar antivirus tales como **Avast Mobile Security**, **Kaspersky** o **Esetnod32** que también están disponibles para el sistema operativo Android.

Finalmente, se aconseja como costumbre de seguridad digital siempre revisar que el origen de una aplicación sea confiable antes de descargarla, además de revisar reseñas y comentarios para asegurarse de que el número de descargas sean de personas

reales y no de bots usados para posicionarla en la tienda. Existen muchos tipos de software malicioso que no son notables a simple vista entonces lo mejor es no poner en riesgo información importante por descargar programas de poco fiar.

Con información de Infobae