Si utilizas la versión gratuita de la aplicación CamScanner, que crea archivos PDF en el teléfono, debes tener cuidado porque los hackers pueden secuestrar de forma remota tu dispositivo Android y robar tu información. La aplicación cuenta con más de 100 millones de descargas en Play Store.

Google ya ha eliminado la app de su tienda oficial, para evitar problemas, deberías desinstalar la aplicación inmediatamente.

Desafortunadamente, CamScanner se ha vuelto deshonesta recientemente cuando los investigadores de seguridad encontraron un módulo troyano oculto dentro de la aplicación, que permite a los hackers remotos descargar e instalar secretamente apps maliciosas en los dispositivos Android de los usuarios sin su conocimiento.

Sin embargo, el módulo malicioso en realidad no reside en el código de la aplicación CamScanner para Android, en cambio, forma parte de una biblioteca de publicidad de terceros que se introdujo recientemente en la aplicación de creación de PDF.

Descubierto por los investigadores de seguridad de Kaspersky, el problema salió a la luz después de que muchos usuarios de CamScanner detectaron un comportamiento sospechoso y publicaron críticas negativas en Google Play Store en los últimos meses, lo que indica la presencia de una función no deseada.

> *«Se puede suponer que la razón por la que se agregó el malware fue la asociación de los desarrolladores de la app con un anunciante sin escrúpulos»*, dijeron los investigadores.

El análisis del módulo troyano Dropper malicioso reveló que el mismo componente también se observó anteriormente en algunas aplicaciones preinstaladas en teléfonos inteligentes chinos.

> *«El módulo extrae y ejecuta otro módulo malicioso de un archivo cifrado incluido en los recursos de la aplicación. Como resultado, los propietarios del módulo pueden usar un dispositivo infectado para su beneficio de la forma que mejor les parezca, desde mostrar a la víctima publicidad intrusiva hasta robar dinero de su cuenta móvil mediante el cobro de suscripciones»,* dijeron los investigadores.

Los investigadores de Kaspersky informaron sus hallazgos a Google, quien rápidamente eliminó la aplicación CamScanner de su Play Store, pero afirman que *«parece que los desarrolladores de aplicaciones eliminaron el código malicioso con la última actualización de CamScanner».*

Aún así, los investigadores aconsejaron a los usuarios que solo tengan en cuenta *«que las versiones de la aplicación varían para diferentes dispositivos, y algunas de ellas aún pueden contener código malicioso»*.

Además, dado que la versión paga de la app CamScanner no incluye la biblioteca de publicidad de terceros, y por lo tanto, el módulo malicioso, no se ve afectada y todavía está disponible en Google Play Store.

Google ha intensificado sus esfuerzos para eliminar aplicaciones potencialmente dañinas en Play Store en los últimos años y ha agregado controles de malware más estrictos para nuevas aplicaciones, pero aún así, las apps legítimas pueden volverse deshonestas y apuntar a sus millones de usuarios.

> *«Lo que podemos aprender de esta historia es que cualquier aplicación, incluso de tienda oficial, aún con buena reputación e incluso con millones de críticas positivas y una gran base de usuarios leales, puede convertirse en malware de la noche a la mañana»*, advirtieron los investigadores.

Debido a esto, se recomienda mantener siempre una buena aplicación antivirus en tu

dispositivo Android que pueda detectar y bloquear dichas actividades maliciosas antes de que puedan infectar tu dispositivo.

Además, siempre se debe verificar las revisiones de la aplicación dejadas por otros usuarios que la hayan descargado, y también verificar los permisos de la aplicación antes de instalar cualquier app y otorgar solo los permisos relevantes para el propósito de la aplicación.

Para obtener más detalles técnicos sobre el malware Trojan Dropper que se encuentra en CamScanner y una lista completa de sus indicadores de compromiso (IOC), incluyendo los hash MD5 y sus dominios de servidor de comando y control, puedes dirigirte al informe de Kaspersky.