Si crees que los archivos multimedia que recibes en apps de mensajería cifrada de extremo a extremo no pueden ser manipulados por terceros, estás equivocado.

Los investigadores de seguridad de Symantec demostraron ayer múltiples escenarios de ataque interesantes contra las aplicaciones de WhatsApp y Telegram para Android, lo que podría permitir a los hackers difundir noticias falsas o usuarios fraudulentos para enviar pagos a cuentas de terceros.

Apodado como *«Media File Jacking»*, el ataque aprovecha un hecho ya conocido de que cualquier aplicación instalada en un dispositivo puede acceder y reescribir archivos guardados en el almacenamiento externo, incluidos los archivos guardados por otras aplicaciones instaladas en el mismo dispositivo.

WhatsApp y Telegram permiten a los usuarios elegir si desean guardar todos los archivos multimedia entrantes en el almacenamiento interno o externo del dispositivo.

Sin embargo, WhatsApp para Android almacena de forma predeterminada los archivos multimedia en el almacenamiento externo, mientras que Telegram para Android utiliza el almacenamiento interno para almacenar los archivos de los usuarios que no son accesibles a ninguna otra app.

Aún así, muchos usuarios de Telegram cambian manualmente la configuración a almacenamiento externo, utilizando la opción *«guarda en la galería»,* cuando desean volver a compartir los archivos multimedia recibidos.

Cabe mencionar que el ataque no solo se limita a WhatsApp y Telegram, sino que también afecta la funcionalidad y la privacidad de muchas otras aplicaciones de Android.

Al igual que los ataques man-in-the-disk, una aplicación maliciosa instalada en el dispositivo de un destinatario puede interceptar y manipular archivos de medios, como fotos privadas, documentos o videos, enviados entre usuarios por medio del almacenamiento externo del dispositivo, todo sin el conocimiento del destinatario y en tiempo real.

> *«El hecho de que los archivos se almacenen y se carguen desde el almacenamiento externo sin los mecanismos de seguridad adecuados permite que otras aplicaciones con permiso de almacenamiento de escritura en externo corran el riesgo de la integridad de los archivos multimedia. Los atacantes podrían aprovechar las relaciones de confianza entre un remitente y un receptor al usar estas aplicaciones de mensajería instantánea para obtener beneficios personales o causar estragos»,* dijeron los investigadores.

Los investigadores ilustraron y demostraron cuatro escenarios de ataque, como se explica a continuación, donde una aplicación de malware puede analizar y manipular de forma instantánea los archivos entrantes:

1.- Manipulación de imagen

En este escenario de ataque, una aplicación inocente, pero que en realidad es maliciosa, descargada por un usuario, puede ejecutarse en segundo plano para realizar un ataque de Media File Jacking mientras la víctima usa WhatsApp y *«manipula fotos personales casi en tiempo real y sin el conocimiento de la víctima».*

2.- Manipulación de pago

En este escenario, que los investigadores denominan como *«uno de los ataques más dañinos de Media File Jacking»,* un actor malintencionado puede manipular una factura enviada por un proveedor a los clientes para engañarlos y hacer que realicen un pago en un cuenta del atacante.

3.- Suplantación de mensaje de audio

En este escenario de ataque, los hackers pueden explotar las relaciones de confianza entre los empleados de una organización. Pueden utilizar la reconstrucción de voz por medio de la tecnología de aprendizaje profundo para alterar un mensaje de audio original para su beneficio personal o para causar estragos.

4.- Propagación de noticias falsas

En Telegram, los administradores utilizan el concepto de «canales» para transmitir mensajes a un número ilimitado de suscriptores que consumen el contenido publicado. Al usar los ataques de Media File Jacking, un atacante puede cambiar los archivos multimedia que aparecen en un canal de confianza en tiempo real para difundir noticias falsas.

Cómo evitar el secuestro de tus archivos en Android

Symantec notificó a Telegram y Facebook sobre los ataques de Media File Jacking, pero cree que Google abordará el problema en su próxima actualización de Android Q.

Android Q incluye una nueva función de privacidad llamada Almacenamiento con Alcance, que cambia la forma en que las aplicaciones acceden a los archivos en el almacenamiento externo de un dispositivo.

El Almacenamiento con Alcance otorga a cada app un espacio aislado de almacenamiento en el almacenamiento externo del dispositivo, donde ninguna otra aplicación puede acceder directamente a los datos guardados por otras aplicaciones en el dispositivo.

Mientras tanto, es posible reducir el riesgo de estos ataques al deshabilitar la función responsable de almacenar los archivos multimedia en el almacenamiento externo del dispositivo.

En el caso de WhatsApp, es necesario acceder a la configuración > Chats > Desactivar el conmutador para *«visibilidad de medios»*.

Para Telegram, acceder a Configuraciones > Configuraciones de chat > Deshabilitar la opción para *«guardar en galería».*