Aplicaciones De Android Dejan Abiertas Graves Fallos SSL

Las **aplicaciones de Android** nos brindan un sin fin de posibilidades, ademas de permitir a los desarrolladores innovar, creando nuevas aplicaciones para ser usadas por otros usuarios. Pero, ¿Sabes que muchas de estas se prestan para que sufras un ataque de tipo **Man in the Middle**? Una nueva investigación revela que muchas de las **aplicaciones más populares de Android** tienen graves vulnerabilidades SSL, las cuales se prestan para realizar un ataque de hombre en el medio (MITM), dirigidos al robo de información personal. Preocupante, verdad?

Según el especialista en protección contra amenazas FireEye, un porcentaje significativo de las aplicaciones **permite a un atacante interceptar** los datos que se envían entre el **dispositivo Android** y un servidor remoto.

Un atacante puede simplemente «rastrear» los datos que se transmite, reemplazarlos ó modificarlos para inyectar contenido malicioso en una aplicación, o redirigir el tráfico a una nueva aplicación.

FireEye ha estudiado unas 1.000 **aplicaciones más descargadas en la Play Store** y encontró que alrededor del **68 por ciento** tiene una de las tres principales vulnerabilidades SSL, dejando expuestos a una gran cantidad de usuario a sufrir un ataque de este tipo.

De **614 aplicaciones que utilizan SSL/TLS** para comunicarse con un servidor remoto, el **73 por ciento** no verificó certificados. El ocho por ciento no pudo verificar los nombres de host de los servidores de la toma de redirección, y de 285 aplicaciones que usan WebKit, el 77 por ciento ha ignorado errores SSL lo que podría permitir el aprovechamiento de

vulnerabilidades de Javascript.

La empresa sugiere que los usuarios pueden ayudar a protegerse a sí mismos, «… no acceder a sitios web que requieren credenciales de inicio de sesión de usuario, haciendo uso de redes Wi-Fi públicas. Esto en sí mismo, con la vigilancia general, en la apertura de correos electrónicos de fuentes desconocidas, recorrer un largo camino en la protección de la información sensible para los ataques MITM «.

Puede leer más detalles de la investigación, que incluye estudios de caso de aplicaciones individuales, en el blog de FireEye. Usted también puede inscribirse para la prueba beta de la última solución de seguridad de Sophos para Android.