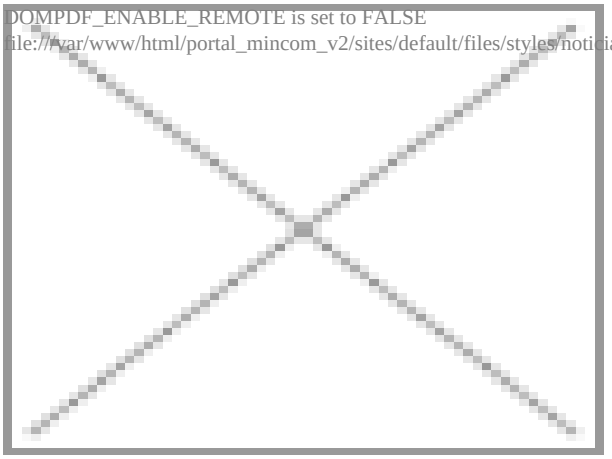

Source:
Computer World

Según el informe ?McAfee Labs Threats Report: June 2016? una nueva amenaza debería preocupar a los usuarios: el uso de las diferentes aplicaciones del smartphone para orquestar un ataque contra su dueño.

En el informe de Intel se señala este comportamiento en más de 5.056 versiones. Las aplicaciones varían desde transmisión de vídeo, control del estado de salud y planificación de viajes.

El origen de esta manipulación de las apps para dirigir un ataque (en el que en algunos casos solo requiere dos aplicaciones) puede estar relacionado con no actualizar periódicamente las versiones de las mismas, dejándolas expuestas a los hackers.

Así, sus sistemas operativos aíslan aplicaciones en sandboxes, a la vez que restringen sus capacidades y controlan a un nivel qué permisos gozan. El problema se halla en que las plataformas móviles también permiten a las aplicaciones comunicarse entre sí, a través de entornos aislados. El resultado es ya conocido: exposición de información privada o confidencial, transacciones financieras indeseadas o el control de un servicio en el móvil.

Para que esta “intercomunicación” entre aplicaciones móviles tenga lugar, es necesario que al menos una de las aplicaciones que intervienen en el proceso cuente con el permiso para acceder a la información o servicios restringidos, que una aplicación sin este permiso cuente con acceso al exterior del dispositivo y que tengan la capacidad de comunicarse entre ellas; pueden utilizar un espacio compartido (archivos accesibles e inteligibles para todos) para intercambiar información acerca de privilegios concedidos y determinar cuál de ellas está localizada de forma óptima para servir como punto de entrada a comandos remotos.

Según explica el informe, hay varias medidas que pueden tomar los usuarios para minimizar los efectos de estas conexiones ilegítima: se deben descargar aplicaciones sólo desde fuentes de confianza, evitar aplicaciones con publicidad integrada, no eliminar restricciones software o "jailbreaking" en dispositivos móviles, y lo más importante, el mantenimiento y la actualización constante del sistema operativo y de aplicaciones.

Troyanos que vuelven
Tampoco se quedan a un lado las amenazas más “tradicionales”; ha vuelto a atacar el troyano W32 / Pinkslipbot (también conocido como Qakbot, Qbot, Qbot). El cibercriminal, que comenzó a actuar en el 2007, roba datos bancarios, contraseñas de correo electrónico y certificados digitales mediante el uso del malware.

A finales del año pasado ha resurgido con características mejoradas (anti-análisis o encriptación multi-capa por ejemplo). El informe ofrece también detalles acerca de la auto-actualización que el troyano es capaz de llevar a cabo así como del mecanismo de exfiltración de datos, e insta a las organizaciones a mantener sus sistemas actualizados con los estándares “hash” más nuevos y más fuertes.

Las amenazas más crecientes
Las nuevas formas de ramsomware han crecido un 24% este trimestre debido a la continua entrada de delincuentes poco expertos en la comunidad del cybercrimen y el ranswomware (utilizan kits para desplegar el malware); en cuanto a móviles, las nuevas muestras de malware también han crecido un 17% respecto al trimestre anterior, y un 113% en los últimos cuatro trimestres.

Más enfocado a marcas, el malware Mac OS ha crecido también rápidamente durante el trimestre debido a un aumento en adware VSearch (se ha incrementado un 68% respecto al trimestre anterior y un 559% durante los últimos cuatro trimestres).

El malware Macro tampoco se queda atrás con un incremento del 42% por trimestre en muestras nuevas de malware macro; la nueva generación de macro malware se centra en atacar redes corporativas.

El botnet Gamut se ha convertido en el spam botnet más productivo aumentando su volumen casi un 50%. Las campañas de spam que todavía perduran ofrecen esquemas del tipo hazte rico rápidamente y suministros farmacéuticos con grandes descuentos. Po otro lado no todos prosperan: Kelihos, el botnet de envío de correo basura más prolífico durante el Q4 del 2015 y un distribuidor de software malicioso generalizado, ha descendido hasta situarse en el cuarto lugar.

Disponible en:

http://cso.computerworld.es/tendencias/un-informe-de-mcafee-labs-revela-nuevas-amenazas-derivadas-de-la-intercomunicacion-entre-aplicaciones-moviles#cxrecs_s [1]

Links
[1] http://cso.computerworld.es/tendencias/un-informe-de-mcafee-labs-revela-nuevas-amenazas-derivadas-de-la-intercomunicacion-entre-aplicaciones-moviles#cxrecs_s