Deloitte.

Cyber Notes

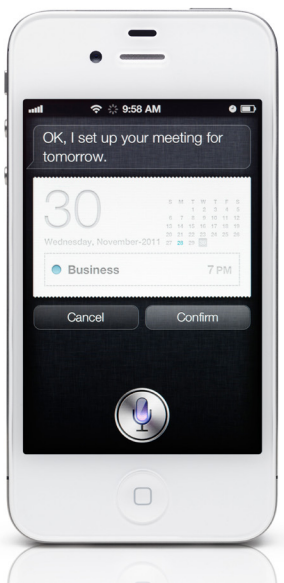
Seguridad en el Smartphone

Es por todos sabido que el uso de los teléfonos inteligentes ha aumentado exponencialmente en los últimos años, han pasado a formar parte de nuestras actividades diarias, pues lo utilizamos constantemente para tareas informativas, así como para incrementar nuestra productividad laboral y también para el entretenimiento.
Debido a esto, lógicamente ha crecido la cantidad de aplicaciones que se desarrollan para cubrir la necesidad. Esto también ha generado un incremento en el nivel de atención de personas que intentan aprovecharse de la ingenuidad de sus usuarios, generando aplicaciones con código malicioso con múltiples fines.

Dentro de los múltiples fines pueden ser tan simples como **spam**, **robo de contraseñas** hasta los más complejos como espiar, estafar, daño al dispositivo o robo de identidad. Las personas que buscan realizar este tipo de ataques informáticos dirigidos a los dispositivos móviles utilizan diferentes vectores de ingeniería social para logar su objetivo. La forma en que intentan que los usuarios instalen su malware dentro de los dispositivos pude ser muchas veces ingeniosa. Unas van desde difusión masiva de mensajes conteniendo una dirección para descargar directamente el software que viene disfrazado dentro de una aplicación o juego, hasta otras formas más ingeniosas como la suplantación de aplicaciones y otras pueden ser aprovechando alguna vulnerabilidad del software ya instalado en los dispositivos.

Las consecuencias de caer en la trampa e instalar software malicioso pueden ser múltiples, en el mejor de los casos se utilizará para obtener información personal o incluso información laboral si es que se encuentra sincronizado el dispositivo con información de la compañía, en el peor de los casos pueden llegar a obtener control total de nuestros dispositivos y utilizarlos para grabar conversaciones, mensajes, robo de contraseñas y estafas.

En los últimos meses han surgido múltiples aplicaciones que prometen brindar contenido para adultos a los usuarios que las descarguen, cuando su fin secundario es poder tomar fotografías mientras los usuarios utilizan las aplicaciones, para poder obtener una fotografía comprometedora y utilizarla para estafar pidiendo una cantidad de dinero para no hacer pública la imagen. Es por esto que cada día se incrementa la preocupación de los fabricantes de dispositivos móviles, desarrolladores de software, así como también los expertos en el área de seguridad informática enfocados los dispositivos móviles. Siempre se está en constante evolución, pensando nuevas formas de fortalecer los sistemas de aplicaciones móviles y creando filtros para evitar que lleguen a los markets de aplicaciones y los usuarios las puedan descargar confiando en que son legítimas.



Para ello se piensa en diferentes formas de proteger la información, como cifrar información importante, filtrar las aplicaciones por código en el market de aplicaciones, evitando así que aplicaciones con fines malicioso puedan ser publicadas. Pero cada vez se realizan formas ingeniosas de burlar este tipo de barreras. Y de nada sirven este tipo de filtros si el usuario no se educa y es quién al final descarga, instala y otorga permiso a estas aplicaciones con código malicioso.

Para evitar ser víctima de estas aplicaciones con código malicioso y comprometer información personal y laboral, o incluso introducir el malware dentro de la red de la corporativa es importante seguir medidas básicas para prevenir malware dentro de los móviles. El consejo principal es siempre mantener actualizado el sistema operativo del móvil.

Dentro de las actualizaciones, el fabricante puede agregar parches de seguridad que cubren vulnerabilidades que ya se han comprobado que pueden ser ejecutadas.

Evitar realizar modificaciones de las funciones del sistema operativo, como "jealibreak" o "rootear" debido a que esto altera los filtros nativos que realiza el sistema operativo y puede permitir que una aplicación aproveche esto y tome permisos privilegiados para realizar acciones.

Solo instalar aplicaciones o juegos desde los market de aplicaciones oficiales, debido a que antes de estar publicada la aplicación pasa por una serie de inspecciones y así se evita en medida ser víctima.

Otra alternativa es instalar una aplicación de seguridad que verifique en tiempo real el comportamiento del móvil y las aplicaciones instaladas dentro de él. Para esto hay aplicaciones de paga o gratuitas. Por último, nos tenemos que educar más como usuarios, leer bien los permisos que otorgamos a las aplicaciones e informarnos más sobre las últimas noticias de ataques a dispositivos para no ser víctimas.

Emilio Sandoval
Director ERS & Consulting