Expertos de la UMH alertan del aumento de aplicaciones que "hackean" los móviles - Información - 01/12/2017

Expertos de la UMH alertan del aumento de aplicaciones que «hackean» los móviles

▶Las app fraudulentas imitan los logotipos y nombres de las originales y se infiltran en las tiendas digitales para ser descargadas
▶La extracción de contraseñas y datos bancarios, el robo de bitcoins o el acoso digital en las redes, entre los principales peligros

BORJA CAMPOY

■ Cambiar la letra a una popular aplicación, por ejemplo, WhatsApp por WhotsApp, y publicarla en una de las tiendas digitales de los teléfonos móviles utilizando incluso el mismo logotipo. El anzuelo ya está puesto para que el usuario descargue el fraude en su terminal. A partir de ese escenario, toda la información que guarda el teléfono (desde los contactos hasta las contraseñas, pasando por los datos de las cuentas bancarias) queda a disposición de unos *hackers* que, incluso, pueden acceder libremente a la cámara de fotos.

Este tipo de prácticas están al alza, como explicaron ayer expertos del Parque Científico de la Universidad Miguel Hernández de Elche, en el marco del Día Internacional de la Seguridad Informática. Las aplicaciones que se ponen de moda o los juegos para pasar el tiempo más populares son el caladero perfecto para que los piratas digitales pongan en marcha sus redes. «Esto sobre todo se produce en las tiendas de Android, los filtros de iPhone son más restrictivos. Pueden pasar unos días hasta que Google detecta el fraude y lo retira», explica el arquitecto de *software* de la empresa Teralco, Rubén Villar.

¿Qué buscan los *hackers* que acceden a un teléfono o un ordenador? Principalmente robar datos a gran escala y hacerse con el control de información. Esto permite suplantar perfiles y realizar operaciones en nombre de otro. «Lo mejor para hacer frente a esto es utilizar contraseñas distintas. La principal que hay que proteger es la del correo electrónico, que no se debe repetir en ninguna otra cuenta», añade Villar.

Las criptomonedas también se han convertido en un botín muy deseado por parte de los *hackers*. «Hacerse con el dominio de las máquinas y mover grandes cantidades de bitcoins son operaciones muy golosas para los ciberdelincuentes», añade el jefe de desarrollo de Producto y Marketing de la firma ilicitana, Fran Zapata. «Aprovechan el desconocimiento que tiene la gente sobre el funcionamiento de los datos desagregados. La tecnología *blockchain* facilita el rastreo», matiza.

Las app fraudulentas están entre los grandes peligros que esconde la ciberdelincuencia. CRISTINA DE MIDDEL

Los profesionales recomiendan mantener al día las aplicaciones y los parches y no visitar páginas poco fiables

Otro de los anglicismos que surge en el mundo de la ciberdelincuencia es el de *stalking*, que se puede traducir como acoso a través de las redes sociales. En este sentido, los expertos ponen de manifiesto la ligereza con la que muchas personas, especialmente los adolescentes, ofrecen gran cantidad de datos sobre su rutina y actividades en plataformas como Facebook, Instagram o Snapchat. Uno de los ejemplos clarificadores en este sentido fue el de un joven que pidió a la red Tinder que le enviara los datos que tenía almacenados de él y recibió 800 páginas.

«En muchas ocasiones hacemos auténticas barbaridades en las redes sociales, y esto permite que se trace fácilmente un perfil de nuestra vida. El que nos espía puede saber dónde vivimos, por dónde nos movemos, si tenemos hijos o no o cuál es nuestro poder adquisitivo», advierte Zapata. «Damos demasiada información y esto se puede volver en nuestra cuenta, es un peligro para nosotros», completa Villar.

Ante el creciente aumento de estas amenazas, la Policía Local está recibiendo formación en inteligencia y escolta digital. Los agentes también advierten de los peligros que genera colgar fotos en las redes. «Cada vez que se publica una imagen en internet, se deja un rastro informático, una huella que es fácilmente localizable», advierte el inspector de la Policía Local, Aurelio Delicado.

En cuanto a la prevención de robos de datos en las empresas, los expertos afirman que se debe ser consciente de los riesgos que se asumen y concederle toda la importancia a la seguridad. Para ello, es preciso mantener al día las actualizaciones y los parches e inculcar a los empleados la consideración de no acceder a las páginas poco fiables y de no conectar USB externos.

Claves robustas y precaución ante las redes wifi públicas

▶ **En materia de seguridad digital, los expertos de la UMH ofrecen diferentes consejos para hacer frente a los ciberdelincuentes. Una de las principales recomendaciones es la de utilizar contraseñas o claves que sean robustas, es decir, que combinen de forma aleatoria cifras, números, mayúsculas, minúsculas y signos. Otro de los consejos de la firma Teralco es el de extremar la precaución con las redes wifi públicas para no dar datos personales.** B. CAMPOY