El peligro de los troyanos bancarios en nuestros móviles

Con el creciente uso de los dispositivos móviles, y con ello la gestión de nuestras finanzas personales a través de diferentes aplicaciones, cada vez son más los ataques a estos dispositivos con el fin de obtener información confidencial relativa a entidades bancarias.

Los usuarios ya no se preocupan sólo por la seguridad de sus propios aparatos electrónicos, sino también por su dinero. Es evidente que las aplicaciones de servicios bancarios o las que manejan información financiera se han convertido en un punto de interés para los ciberdelincuentes, que se esfuerzan cada día por cruzar las barreras de seguridad que les ponen las entidades financieras. Dada la importancia de los datos que se pueden extraer de estas aplicaciones, es fundamental mantener un exhaustivo análisis y control de las posibles amenazas.

Los expertos en seguridad informática han detectado un crecimiento exponencial de los “troyanos bancarios”, dedicados a espiar, manipular e intermediar en los datos transferidos por los usuarios, y si lo consideran posible, a sustraer el dinero de las cuentas a las que han podido acceder.

A pesar de que las entidades financieras que más amenazas han sufrido hayan pertenecido a USA y Reino Unido (por ejemplo, el banco estadounidense Wells Fargo ha sufrido el 35% del total de amenazas de troyanos en el sector), bancos españoles como BBVA y Santander también han sido víctimas de intentos de ataques a la información de sus clientes.

En los últimos años, cada vez son más las personas que utilizan su móvil, tablet o smartwatch, no solo para consultar la situación de sus cuentas bancarias, sino también para realizar pagos móviles a través de ellos. Aunque a simple vista parece que nuestro móvil es únicamente un teléfono, y que se puede obtener información más valiosa de nuestros ordenadores, estamos equivocados. Los móviles son potentes aparatos que guardan información sobre nuestras cuentas bancarias, sobre nuestros movimientos y sobre nuestra actividad en general, por lo que es en ellos donde se están empezando a centrar los esfuerzos de los hackers.

¿Cómo atraen los hackers al usuario para intentar acceder a su información?

Por ejemplo, muchos bancos utilizan los números de móvil de los clientes para autorizar las operaciones, enviándoles claves de un solo uso que luego tienen que introducir en la aplicación para poder validar la operación. Dado que los cibercriminales conocen el funcionamiento de estos sistemas, tratan de utilizar estos canales de comunicación para poder realizar pagos y transferencias desde las cuentas bancarias de los usuarios, sin su consentimiento.

Además de este ejemplo, existen varios métodos que utilizan los troyanos bancarios para obtener la información confidencial que buscan. A continuación analizamos tres de los métodos más utilizados:

- Sustraer la información a través de los SMS: el malware en dispositivos móviles funciona con una técnica similar al “man in the middle”, recogiendo los SMS que llegan de los bancos, con claves para realizar operaciones, y enviándolos a los hackers, que los utilizarán para intentar transferir dinero de la cuenta de la víctima.
- Pequeños movimientos bancarios: es muy frecuente también transferir pequeñas cantidades de dinero desde la cuenta

del usuario que está sufriendo el ataque, a cuentas fraudulentas que crean los propios hackers.

- Efecto espejo en las apps: esta técnica es similar al “phishing”, con la que el malware imita las aplicaciones móviles de las entidades financieras que los usuarios manejan frecuentemente, para que éstos introduzcan sus credenciales (usuario, contraseña etc.), y así los hackers puedan acceder a la aplicación real de la entidad con los datos que el propio usuario, sin ser consciente de ello, les ha facilitado.

Analizando las potenciales amenazas que podemos sufrir en nuestros teléfonos móviles, nos damos cuenta de la importancia que tiene estar siempre atentos a posibles irregularidades que detectemos en el uso diario de nuestro móvil, o incluso de movimientos en nuestra cuenta que, a pesar de ser cantidades pequeñas de dinero, no hayamos ordenado nosotros. Sin embargo, parece que los bancos y entidades financieras están cada vez más concienciados de este creciente problema, y están trabajando en ofrecer servicios cada vez más seguros, para que los usuarios puedan realizar pagos móviles con total confianza.