Tecnología

'APPS' ELIMINADAS POR FRAUDE

Un total de 46 *apps* fueron eliminadas de la tienda de Google Play tras ser acusadas de cometer fraude publicitario y recopilar datos privados de los usuarios.

Lista la 'autopista' de datos para Latinoamérica

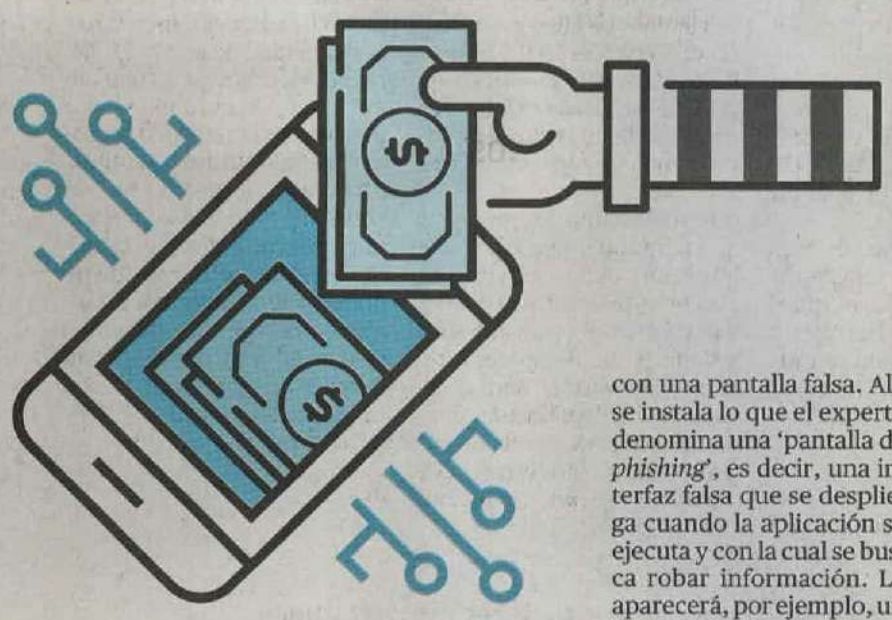
Fotonoticia

CURIE, EL CABLE SUBMARINO de Google en alianza con Equinix, que servirá de autopista de datos entre EE. UU. y Latinoamérica, ya está instalado en Valparaíso (Chile). La estructura tiene 9.000 kilómetros de extensión; se espera que facilite servicios en la nube y beneficie a proveedores de servicios de red. FOTO: EFE

Así pueden robarle dinero desde su teléfono

Un estudio de Eset revela que los troyanos bancarios y las *apps* falsas son dos de las tácticas más utilizadas por los cibercriminales.

ANA MARÍA VELÁSQUEZ DURÁN REDACCIÓN TECNOLOGÍA | @Anamariavd19



Obtener información sobre su dispositivo, ejecutar aplicaciones adicionales, interceptar, enviar mensajes y engañarlo para recolectar sus contraseñas. Estas son solo algunas de las artimañas que pueden usar los cibercriminales para robar dinero a sus víctimas desde sus dispositivos móviles. Muchos usuarios revisan sus cuentas en los teléfonos, hacen transferencias y pagan desde su celular. Tenga por seguro que los atacantes saben muy bien cómo aprovecharse de esto.

La compañía de seguridad Eset publicó un informe en el que revela dos de las estrategias más usadas: instalar troyanos bancarios (un tipo de *malware* para robar información financiera) y hacerlo descargar aplicaciones bancarias falsas. El reporte, realizado por el investigador Lukás Stefanko, detalla paso a paso el *modus operandi* en estos casos.

Troyanos

Los troyanos bancarios pueden ser instalados en su dispositivo mediante diferentes canales. La opción más común, según el reporte, es a través de aplicaciones fraudulentas descargadas tanto en tiendas oficiales como no oficiales. Sin embargo, otros métodos frecuentes de distribución incluyen sitios web y enlaces de descarga maliciosos difundidos a través de redes sociales, correos electrónicos o servicios de mensajería. MazarBot, BankBot, Anubis y Exobot son algunos de los tipos de *malware* más comunes. Una vez se instala el código malicioso, este es capaz de solicitar permisos necesarios para robar información. Incluso pueden obtener derechos de administrador para el sistema que incluyen "autorizaciones especialmente intrusivas, como cambiar la contraseña de la pantalla, bloquear el dispositivo o borrar todo su contenido". Al aplicar estas tácticas, los criminales pueden acceder fácilmente a información confidencial en su dispositivo, incluyendo datos bancarios. Para hacerlo, los troyanos suelen presentar a los usuarios mensajes de error falsos que afirman que una aplicación ha sido desinstalada o suelen hacerse pasar por servicios conocidos y legítimos del sistema.

Una vez completado este paso se ejecuta la táctica principal. Según Stefanko, el ciberdelincuente aplica una estrategia especial que consiste en superponer el *malware* en la aplicación con una pantalla falsa. Allí se instala lo que el experto denomina una 'pantalla de *phishing*', es decir, una interfaz falsa que se despliega cuando la aplicación se ejecuta y con la cual se busca robar información. Le aparecerá, por ejemplo, un formulario falso en el que se le pide ingresar los datos de su tarjeta de crédito. Al obtener esa información, el atacante puede realizar transacciones fraudulentas utilizando la cuenta bancaria de la víctima o vender las contraseñas en el mercado negro.

"La presencia de *malware* en el dispositivo y su conexión a aplicaciones bancarias está destinada a permanecer oculta durante el mayor tiempo posible", resalta el estudio.

'Apps' falsas

La otra posibilidad que tiene un criminal para engañarlo es a través de aplicaciones falsas de los bancos. Los ciberdelincuentes trabajan para hacerlas parecer lo más reales posibles y mostrarlas como si fueran las plataformas oficiales de las entidades. Por eso se fijan en detalles que van desde el nombre y la descripción, hasta el ícono y la opción de previsualización de imágenes.

Sin embargo, Stefanko resalta que lo que a veces puede servir como indicador de sospecha es que la *app* es clasificada en una categoría incorrecta. Por ejemplo, la pueden ubicar en la sección de 'Libros y referencias'. Además, otro de los aspectos más importantes para tener en cuenta es que el nombre del desarrollador normalmente es desconocido y no se relaciona con la institución financiera.

Al instalar estas *apps*, verá también pantallas de inicio de sesión falsas a través de las cuales le robarán sus contraseñas. Después de que sus datos son hurtados no le aparecerá ninguna funcionalidad real, por lo que "algunas aplicaciones muestran mensajes genéricos con la promesa de volver para acceder al servicio".

Durante el proceso de instalación, estas aplicaciones también solicitan permisos como acceso a los mensajes de texto. En ese sentido, las aplicaciones falsas pueden interceptar y redirigir los mensajes con el fin de evitar la autenticación de dos factores, un método de seguridad que le permite añadir otro requisito, a parte de su contraseña, para acceder a un servicio. Normalmente son códigos de autenticación que llegan por mensajes de texto, así que al interceptar esta herramienta, dicha información también es robada.

Cómo protegerse

Para evitar ser víctima es importante que antes de instalar una aplicación, compruebe siempre sus valoraciones, el contenido de las reseñas, el número de instalaciones y el nombre del desarrollador. Preste especial atención a los permisos solicitados y verifique si son realmente necesarios. Es importante que mantenga sus dispositivos y aplicaciones actualizados y que, además, utilice una solución de seguridad en su celular. Según Stefanko, la forma más fiable de detectar troyanos bancarios en su dispositivo es ejecutar un escaneo utilizando un antivirus de confianza.

En caso de ser engañado, cambie las contraseñas de sus tarjetas y de los servicios de internet y verifique su cuenta lo más pronto posible para detectar transacciones sospechosas. Recuerde que lo mejor es que siempre consulte el sitio web oficial del banco para realizar transacciones.

Apple elimina 'apps' de control parental

Apple eliminó 11 de las 17 aplicaciones de control parental más utilizadas de su tienda App Store argumentando "razones de seguridad y privacidad".

Según un informe de *The New York Times*, Apple tomó las medidas después de introducir su propia función 'Screen Time', el año pasado, que permite a los usuarios establecer limites en ciertas funciones de iPhone y iPad y hacer un seguimiento de los movimientos de los menores en los dispositivos.

La decisión suscitó críticas e, incluso, dos fabricantes de aplicaciones presentaron quejas ante la Unión Europea, según las informaciones. Sin embargo, Apple argumentó que las aplicaciones que había prohibido utilizaban una tecnología llamada 'gestión de dispositivos móviles', diseñada para empresas que administran grupos de dispositivos para empleados y "proporciona a un tercero control y acceso a un dispositivo e información confidencial, como la ubicación del usuario, uso de la aplicación, cuentas de correo electrónico, permisos de cámara e historial de navegación". Esto supone una "clara violación de las políticas de la App Store".

Así mismo, la compañía dijo que dio a los desarrolladores 30 días para modificar sus aplicaciones, motivo por el cual aquellas que no introdujeron los cambios necesarios fueron eliminadas.

Esta no es la primera vez que acusan a Apple de competencia "injusta". En marzo, el fundador de Spotify, Daniel Ek, presentó una queja ante la Comisión Europea con motivo del impuesto del 30 por ciento que impuso el gigante de la manzana a las compras realizadas con su sistema de pago, que cubriría la suscripción al servicio prémium.