Un nuevo ataque en Android combina phishing, malware y robo de datos

Los atacantes combinan la **suplantación de credenciales, el robo de datos de tarjetas de crédito y el malware** en una sola campaña que apunta a la obtención de información bancaria.

La campaña utiliza el **phishing con la distribución del troyano Marcher Android**, un malware bancario que se ha mantenido activo al menos desde finales de 2013 y que ha utilizado como señuelos una actualización falsa de software, una actualización de seguridad falsa y un popular juego móvil.

Marcher se originó inicialmente en foros clandestinos rusos, pero desde entonces se ha convertido en una amenaza global, con troyanos dirigidos a bancos de todo el mundo.

La última campaña de Marcher ha estado en curso desde enero y utiliza el esquema de **varios pasos para infectar a los clientes de los bancos austriacos.**

Los ataques comienzan con correos electrónicos de phishing que contienen un enlace abreviado de **bit.ly que es una versión falsa de la página de inicio de sesión de Bank Austria,** que ha sido registrada en varios dominios diferentes que contienen 'bankaustria' en el asunto para engañar al usuario haciéndole creer que está visitando el sitio oficial.

A aquellos que visitan la página falsa de Bank Austria **se les pide la información de sus clientes, dirección de correo electrónico y número de teléfono.** Estos detalles proporcionan a los atacantes todo lo que necesitan para pasar a utilizar la ingeniería social y llevar a cabo la siguiente etapa de la campaña.

A continuación se solicita que el usuario se instale la **"Aplicación de Seguridad Bank Austria" (falsa) en su smartphone** y posteriormente se le redirige a una URL acortada y con la afirmación de que seguir el enlace permitirá instalar la aplicación. Los usuarios que hacen clic reciben **instrucciones adicionales sobre cómo descargar la aplicación,** que exige modificar la configuración de seguridad para permitir la descarga de aplicaciones de fuentes desconocidas, una parte del ecosistema Android que los atacantes **explotan regularmente para instalar malware** (en este caso permite la instalación de Marcher).

De acuerdo con los investigadores de seguridad que han descubierto la nueva campaña, **casi 20.000 personas han sido ya víctimas**, entregando potencialmente sus datos bancarios e información personal a los piratas informáticos.