Se ha descubierto un troyano bancario Android previamente desconocido, dirigido a los usuarios de la compañía española de servicios financieros BBVA.

Al parecer, el troyano se encuentra en sus primeras etapas de desarrollo, denominado Revive, por la compañía italiana de seguridad cibernética Cleafy, se observó por primera vez el 15 de junio de 2022 y se distribuyó mediante campañas de phishing.

> *«Se eligió el nombre Revive porque una de las funcionalidades del malware (llamada por los atacantes 'revive') se reinicia en caso de que el malware deje de funcionar»*, dijeron los investigadores de Cleafy, Federico Valentini y Francesco Lubatti.

Disponible para descargar desde páginas de phishing maliciosas como señuelo para engañar a los usuarios para que descarguen la aplicación, el malware se hace pasar por la autenticación de dos factores del banco (2FA) y se dice que está inspirado en el spyware de código abierto llamado Teardroid, y los autores modificaron el código fuente original para incorporar nuevas funciones.

A diferencia de otros programas maliciosos bancarios conocidos por atacar una amplia gama de aplicaciones financieras, Revive está diseñado para un objetivo específico, el banco BBVA. Sin embargo, no se diferencia de sus contrapartes en que aprovecha el API de servicios de accesibilidad de Android para cumplir con sus objetivos operativos.

Revive está diseñado principalmente para recopilar las credenciales de inicio de sesión del banco mediante el uso de páginas similares a las originales y facilitar de este modo los ataques de apropiación de cuentas.

También incorpora un módulo keylogger para capturar las pulsaciones de teclas y la capacidad de interceptar mensajes SMS recibidos en los dispositivos infectados, principalmente contraseñas de un solo uso y códigos 2FA enviados por el banco.

> *«Cuando la víctima abre la aplicación maliciosa por primera vez, Revive solicita dos permisos relacionados con los SMS y las llamadas telefónicas. Después de eso, aparece una página de clonación (del banco objetivo) para el usuario y, si se insertan las credenciales de inicio de sesión, se envían al servidor de comando y control de los TA».*

Los hallazgos subrayan una vez más la necesidad de tener cuidado cuando se trata de descargar aplicaciones de fuentes no confiables de terceros. El abuso de la carga lateral no ha pasado desapercibido para Google, que ha implementado una nueva función en Android 13, que impide que dichas aplicaciones utilicen API de accesibilidad.