Alertan sobre nueva táctica de ciberdelincuentes en iPhone

Una nueva campaña de phishing parece estar dirigida a los usuarios de dispositivos iPhone de Apple, según revela una investigación realizada por el experto en ciberseguridad Brian Krebs. Los atacantes están aprovechando un fallo presente en la función de restablecimiento de contraseña del ID de Apple para intentar engañar a los usuarios y tomar el control de sus cuentas.

Krebs explica que los atacantes pueden bombardear a los usuarios con una serie de notificaciones que instan a la víctima a permitir el cambio de contraseña. Esto se logra al enviar una larga cadena de solicitudes de restablecimiento de contraseña a todos los dispositivos asociados a la cuenta de Apple del usuario. Aunque lo habitual es que el usuario rechace estas solicitudes, los atacantes abusan del sistema para enviar numerosas peticiones, informó Andro4All.

El problema surge cuando, por error o desconocimiento, el usuario pulsa «Permitir». En ese momento, los atacantes pasan a la siguiente fase del ataque: realizar una llamada telefónica a la víctima haciéndose pasar por Apple y solicitando el código de acceso de un solo uso que se envía al dispositivo. Si la víctima comparte este código, los atacantes pueden cambiar la contraseña del ID de Apple y acceder a toda la información almacenada en la cuenta del usuario.

Para llevar a cabo estos ataques, los ciberdelincuentes necesitan acceder a la dirección de correo electrónico o al número de teléfono del usuario. En muchos casos, han utilizado datos obtenidos de filtraciones de bases de datos que contienen información de usuarios de todo el mundo.

Krebs recomienda a los usuarios nunca pulsar «Aceptar» si reciben una solicitud de restablecimiento de contraseña en un dispositivo de Apple, a menos que ellos mismos hayan solicitado el cambio. Además, nunca se debe compartir un código de verificación de un solo uso a través de una llamada telefónica o un mensaje de texto.

Con información de Versión Final