

Apple y Google engañados por hackers que buscan datos de usuarios para extorsionar a mujeres

29/04/2022



Apple, Meta, Alphabet (matriz de Google), Snapchat, Twitter y Discord fueron engañados por un grupo de hackers para proporcionar información personal de sus consumidores que luego utilizaron para acosar y extorsionar a mujeres y menores.

Los ciberdelincuentes disponen de una nueva herramienta para obtener información personal que puede ser utilizada para el acoso y la extorsión, además de para sacar un beneficio económico por medio de la ingeniería social.

El método, que empezó a ser usado con mayor insistencia en los últimos meses, **engaña a las compañías y les envía una solicitud de datos de emergencia para acceder a la información personal de su base de usuarios suplantando a agencias**

policiales.

Una solicitud de datos de emergencia es un procedimiento utilizado por las fuerzas del orden en Estados Unidos para **recabar información de compañías que proveen servicios** alegando que se trata de una situación de emergencia, como la prevención de casos de suicidio, asesinato o secuestro, y **no disponen de tiempo para presentar una citación.**



Las empresas engañadas, entre las que están Apple, Meta, Alphabet, Snap, Twitter y Discord, **no suelen tener obligación legal de proporcionar los datos requeridos** ya que las solicitudes de emergencia no tienden a incluir una orden firmada por un juez. Sin embargo, suelen acceder a ello como **gesto de «buena fe».**

El método empleado por los ciberdelincuentes varía, pero suelen seguir un patrón que empieza con el hacker atacando el **sistema de correo electrónico** de una agencia de las fuerzas del orden extranjera. Posteriormente, el

atacante **falsifica** una solicitud de datos de emergencia que envía a la empresa tecnológica para pedir información personal sobre la cuenta de un usuario. Los datos proporcionados varían según cada empresa, pero -por norma general- suelen incluir **el nombre del usuario, su dirección IP, su correo electrónico y su domicilio**.

Los principales objetivos de los ciberdelincuentes son **las mujeres y los niños**. En algunos casos, el atacante llega a presionarles para crear y compartir **contenido sexual explícito** amenazándoles con sufrir **represalias** si no acceden a sus deseos.



El exdirector de Seguridad de Facebook y actualmente consultor, **Alex Stamos**, comentó a Bloomberg que «los departamentos policiales tendrán que centrarse en **prevenir** que se comprometan las cuentas de los usuarios». Para ello, propone una **autenticación multifactorial** y un «**mejor análisis del comportamiento del usuario**».

Las tecnologías deberían, por su parte, «**implementar una política de confirmación**» mediante llamadas telefónicas, además de pedir a las fuerzas del orden que usen sus portales

dedicados para **detectar mejor posibles suplantaciones de cuentas.**

Fuente: **Ámbito**