Se ha llevado a cabo la primera condena en Estados Unidos por *«Sim Swapping»* en febrero. El Departamento de Justicia de Estados Unidos anunció desde entonces, cargos contra distintas personas por participar en el plan para extraer millones de dólares en criptomonedas de las víctimas.

En el último incidente, las autoridades estadounidenses arrestaron el jueves a otros dos presuntos criminales cibernéticos de Massachusetts, acusándolos de robar 550 mil dólares en criptomonedas de al menos 10 víctimas que utilizan el intercambio de SIM entre noviembre de 2015 y mayo de 2018.

Sim Swapping, Intercambio de SIM o secuestro de SIM, es una técnica que generalmente involucra la ingeniería social del proveedor de telefonía móvil para convencer al empleado del operador.

Un atacante hace una llamada falsa haciéndose pasar por la víctima y convence al proveedor de telefonía móvil de que transfiera el número de teléfono del objetivo a una tarjeta SIM que pertenezca al atacante.

Una vez realizado esto exitosamente, el atacante puede obtener contraseñas de un solo uso, códigos de verificación y autenticación de dos factores recibidos en el teléfono del objetivo para restablecer contraseñas y obtener acceso a cuentas de cualquier tipo.

Los hackers apuntaron a ejecutivos de empresas de criptomonedas

Según la acusación, los acusados, Eric Meiggs de 20 años y Declan Harrington de 21 años, no solo se dirigieron a usuarios con cuentas de criptomonedas de alto valor, sino que también se dirigieron a ejecutivos de empresas de criptomonedas en un intento por obtener ganancias significativas.

Además, los dos acusados también fueron acusados por hacerse cargo de las cuentas de

redes sociales de sus víctimas, incluidos dos que *«tenían nombres de cuentas de redes sociales de alto valor o 'OG' (Gangster Original)».*

Ambos individuos fueron acusados de 11 cargos:

- Un cargo de conspiración para cometer fraude electrónico
- Ocho cargos de fraude electrónico
- Un cargo de fraude y abuso informático
- Un cargo de robo de identidad agravado

De declarar culpable a un individuo por fraude electrónico, podría enfrentar una pena máxima de 20 años en prisión. Mientras tanto, el cargo de robo de identidad agravado conlleva una pena máxima de 2 años de prisión.

Cómo protegerse del intercambio de SIM

Después de muchos incidentes relacionados con el SIM Swapping, la Comisión Federal de Comercio de Estados Unidos (FTC), emitió en octubre una lista adecuada de pautas que los usuarios pueden seguir para protegerse de este tipo de ataques.

- No responder llamadas, correos electrónicos o mensajes de texto que soliciten información personal
- Limitar la información personal que se comparte en línea
- Configurar un PIN o contraseña en la cuenta del celular
- Considerar el uso de una autenticación más fuerte en cuentas con información personal o financiera confidencial

En caso de ser víctima de esta estafa, se puede tomar alguna de las siguientes medidas:

- Ponerse en contacto con el proveedor de servicios telefónicos de inmediato para informar el fraude y tomar el control del número telefónico.
- Verificar los estados de cuenta en busca de cargos no reconocidos

- Cambiar las contraseñas de todas las cuentas en línea