El Departamento de Justicia de Estados Unidos anunció hoy cargos contra nueve individuos, de los cuales, seis son miembros de un grupo de piratería llamado *«The Community»* y otros tres son ex empleados de proveedores de telefonía móvil que supuestamente los ayudaron a robar cerca de 2.5 millones de dólares en criptomonedas utilizando el método conocido como «SIM Swapping».

De acuerdo con la acusación de 15 cargos que se presentó hoy, cinco estadounidenses y un irlandés relacionados con el grupo de piratería de The Community están acusados por conspiración para cometer fraude electrónico, además de robo de identidad con agravantes.

Otros tres estadounidenses, que supuestamente son ex empleados de proveedores de telefonía móvil, son acusados de una denuncia penal por fraude bancario.

SIM Swapping o SIM Hijacking, es un tipo de robo de identidad que generalmente implica trasladar de forma fraudulenta el mismo número a una nueva tarjeta SIM que pertenece al hacker.

En el intercambio de SIM, los hackers tratan socialmente al proveedor de telefonía móvil de una víctima al convencerlo de que son los propietarios reales del número de teléfono que desean intercambiar al proporcionar la información personal requerida sobre el objetivo y finalmente, engañar a las operadoras para que transfieran el número de teléfono del objetivo a una tarjeta SIM perteneciente a los atacantes.

Los acusados ejecutaron los ataques con éxito, gracias a los tres ex empleados del proveedor de servicios de telefonía móvil acusados, que según informes, ayudaron a The Community a *«robar las identidades de los suscriptores a los servicios de sus empleadores a cambio de sobornos».*

La siguiente es la lista de los acusados:

- Conor Freeman, 20, de Dublín, Irlanda
- Ricky Handschumacher, 25, del condado de Pasco, Florida

- Colton Jurisic, 20, de Dubuque, Iowa
- Reyad Gafar Abbas, 19, de Rochester, Nueva York
- Garrett Endicott, 21, de Warrensburg, Missouri
- Ryan Stevenson, 26, de West Haven, Connecticut
- Jarrat White, 22, de Tucson, Arizona (ex empleado del proveedor de telefonía móvil)
- Robert Jack, 22, de Tucson, Arizona (ex empleado del proveedor de telefonía móvil)
- Fendley Joseph, 28, de Murrietta, California (ex empleado del proveedor de telefonía móvil)

Al intercambiar la tarjeta SIM con éxito, los atacantes de The Community utilizaron los números de teléfono de sus víctimas para restablecer las contraseñas y obtener acceso a sus cuentas en línea, incluidos el correo electrónico, el almacenamiento en la nube y las cuentas y billeteras de intercambio de criptomonedas, utilizando códigos de verificación y códigos de autenticación de dos factores recibidos en dichos números.

En total, los acusados ejecutaron siete ataques de intercambio de SIM para robar los fondos de las víctimas de sus billeteras criptomonedas, transfiriendo aproximadamente 2.5 millones de dólares en criptomonedas a billeteras controladas por el grupo de hackers.

> *«Los teléfonos móviles de hoy no son solo un medio de comunicación, sino también un medio de identificación. Este caso debe servir como un recordatorio para todos nosotros para proteger nuestra información personal y financiera de aquellos que buscan robarla»,* dijo el abogado Matthew Schneider.

Si son condenados por el cargo de conspiración para cometer fraude electrónico, cada acusado enfrenta una pena máxima de 20 años de prisión. Mientras tanto, un cargo por robo de identidad agravado conlleva una sentencia máxima de 2 años de prisión.

A inicios del año, un estudiante universitario de 20 años, en Nueva York, fue condenado a 10 años de prisión en lo que constituyó la primera acusación de intercambio de SIM de la jurisdicción. Robó más de 5 millones de dólares en criptomonedas de unas 40 víctimas al

secuestrar su número telefónico.