Europol, en coordinación con la policía nacional española y rumana, arrestó a 26 personas en relación con el robo de más de 3.9 millones de dólares al secuestrar los números de teléfono de usuarios por medio de ataques de intercambio de SIM.

Los organismos encargados de hacer cumplir la ley arrestaron a 12 y 14 personas en España y Rumania, respectivamente, como parte de una operación conjunta contra dos grupos diferentes de intercambiadores de SIM, según confirmó la Europol.

Este desarrollo se produce cuando los ataques de intercambio de SIM se convirtieron en una de las mayores amenazas para los operadores de telecomunicaciones y usuarios móviles. El truco es cada vez más popular y dañino, promovido mediante ingeniería social y utilizado por los piratas informáticos para persuadir a los operadores telefónicos de transferir los servicios celulares de sus víctimas a una tarjeta SIM bajo su control.

El SIM Swapping otorga a los atacantes acceso a las llamadas telefónicas entrantes, mensajes de texto y código de verificación únicos, que distintos sitios web envían por medio de mensajes SMS como parte del proceso de autenticación de dos factores (2FA).

Como resultado de esto, un estafador puede hacerse pasar por una víctima con un proveedor de cuenta en línea y solicitar que el servicio envíe enlaces de restablecimiento de contraseña de la cuenta o código de autenticación al dispositivo de intercambio de SIM controlado por los hackers, mediante el cual, el atacante puede restablecer la cuenta de la víctima.

Este tipo de ataques tienen éxito aún si las cuentas están protegidas por 2FA basado en SMS, lo que permite a los piratas informáticos llevar a cabo datos y robos financieros simplemente al robar los códigos OTP enviados por el sitio web al número de teléfono del individuo.

Se cree que el grupo de hackers en España, que forma parte de una red de piratería grande, ha realizado más de 100 ataques de este tipo, robando entre 6,700 y 153,518 dólares de cuentas bancarias de víctimas desprevenidas por cada ataque.

Además de aprovechar troyanos maliciosos para robar las credenciales bancarias de las

víctimas, los intercambiadores de SIM solicitaron una tarjeta SIM duplicada comunicándose con sus proveedores de servicios móviles y proporcionando documentos falsos.

Luego de la activación de las tarjetas SIM duplicadas, los delincuentes presuntamente hicieron transferencias fraudulentas desde las cuentas de las víctimas utilizando los códigos de autenticación que los bancos enviaron a los teléfonos para su confirmación.

El grupo criminal detenido en Rumania, que logró robar más de 500 mil euros (560,285 dólares) de víctimas inocentes en Austria, utilizó técnicas similares para apoderarse de sus teléfonos y retirar el dinero en cajeros automáticos sin tarjeta.