07/05/24

Detenidas 30 personas por estafar más de un millón de euros mediante el método “Man in the middle”

Resumen

Han sido localizados más de 100 perjudicados en España, Alemania, Andorra, Bélgica, Bulgaria, Ecuador, Eslovenia, Finlandia, Holanda, Hungría, Irlanda, Italia, Lituania, Polonia, Portugal, Reino Unido, República Checa y Rumanía

Suplantaban las conversaciones entre proveedores de empresas y sus clientes y modificaban los datos bancarios para estafar el dinero de pagos pendientes

Creaban cuentas bancarias con datos personales usurpados a personas a las que captaban mediante falsas ofertas de empleo

Contenido

La Guardia Civil, en el marco de la operación “Osgiliath”, ha detenido a 30 personas en diversas localidades de Andalucía, Cataluña, Madrid, Murcia y Toledo, a las que se les atribuye la estafa de más de un millón de euros a víctimas de diferentes países. Dos de los cabecillas del grupo han sido detenidos en Getafe y Barcelona.

Se ha identificado además a otros 40 presuntos autores, la mayoría residentes en España, y también en Croacia, Hungría, Inglaterra, Marruecos, Nigeria, Pakistán y Rumanía, de cuyas identidades se ha dado cuenta al Juzgado que entiende de la causa, y a las autoridades de esos países.

Han sido localizados más de 100 perjudicados en España, Alemania, Andorra, Bélgica, Bulgaria, Ecuador, Eslovenia, Finlandia, Holanda, Hungría, Irlanda, Italia, Lituania, Polonia, Portugal, Reino Unido, República Checa y Rumanía a los que la organización criminal ha estafado en apenas un año.

La investigación se inició en mayo del pasado año tras recibir la denuncia de una empresa de construcción a la que le habían estafado más de 10.000 euros empleando el método conocido como “Man in the middle”.

En este tipo de ciberataque, conocido también como Fraude del CEO o del BEC (Business E-mail Compromise), los autores se cuelan en las conversaciones entre dos o más dispositivos, normalmente un proveedor y sus clientes. El estafador accede a las conversaciones entre ambos e intercepta las referidas a pagos, en las que suplantan la identidad, y haciéndose pasar por el proveedor, modifica la información logrando que la víctima realice las transferencias a un número de cuenta del delincuente. De otro lado, haciéndose pasar por el cliente, negocia con el proveedor prórrogas para realizar los pagos, consiguiendo así ganar tiempo. Una vez que se logra que la víctima realice la transferencia, el estafador deja de intervenir en las conversaciones y, es entonces cuando se destapa que se trata de una estafa.

Creación de páginas web falsas

Los agentes comprobaron que los mismos autores empleaban otras metodologías de ciber estafa: haciéndose pasar por empresas reales, anunciaban vehículos a motor, maquinaria agrícola y viviendas de alquiler vacacional. Para esto, crean páginas web falsas en las que ofertan uno de estos productos, que realmente no poseen, a un precio competitivo y bajo el nombre de una marca solvente, empleando incluso el CIF real de la empresa a la que suplantan, pero aportando como contacto un email creado por los estafadores.

Captada la atención de los interesados en adquirir alguno de los productos, inician una conversación por correo electrónico en la que solicitan a la víctima, entre otras cosas, una copia de su documento de identidad que posteriormente emplean para contratar productos financieros (alta de cuentas bancarias o préstamos) utilizando una identidad usurpada. La cantidad estafada en estos casos es la reclamada en concepto de reserva del vehículo, la máquina o la vivienda.

Falsas ofertas de empleo

Otra forma de hacerse con datos de personas a las que usurpan la identidad es mediante falsas ofertas de empleo que difunden de forma masiva. Cuando un perjudicado pica, le solicitan la documentación y datos personales con la excusa de dar de alta el contrato, pero que realmente son utilizados para llevar a cabo la actividad criminal.

Para transferir el dinero procedente de las estafas, la organización contaba con una red de mulas a las que abonaba comisiones que iban desde los 50 hasta los 1.500 euros. Una vez que este dinero estaba en poder de las cuentas de los criminales, lo sacaban en cajeros automáticos, lo invertían en monedas virtuales o lo transferían a cuentas de la República de Malta y la República de Lituania. La Guardia Civil continúa estudiando el rastro de estas transferencias.

La explotación de la operación se ha llevado a cabo en dos fases, la primera en el mes de diciembre de 2023, en la que se detuvo a cinco personas en las localidades de Getafe (Madrid), Talavera de la Reina (Toledo), Moratalla (Murcia) y Pegalajar (Jaén).

Durante la segunda fase, que finalizó el pasado 12 de marzo, se ha detenido a otras 25 personas en las localidades de Lloret de Mar (Girona) y Barcelona.

En total, han sido detenidas 30 personas, 19 hombres y 11 mujeres, con edades comprendidas entre los 19 y los 56 años, a los que se les imputan los delitos de estafa tecnológica, usurpación de identidad, falsificación de documentos, descubrimiento y revelación de secretos, blanqueo de capitales y pertenencia a organización criminal.

Han sido identificadas 40 personas, 29 hombres y 11 mujeres, de entre 20 y 45 años de edad, como presuntos autores, cuyas identidades han sido facilitadas a la autoridad judicial. Las diligencias han sido puestas a disposición del Juzgado de Instrucción número 4 de Alicante.

Se han intervenido 153 cuentas bancarias logrando recuperar 114.366 euros, procedentes de las estafas cometidas por el grupo.

La operación ha sido desarrollada por el Puesto Principal de la Guardia Civil de San Juan de Alicante, que ha contado con la colaboración de la Fiscalía de Criminalidad Informática de Alicante, EUROPOL y las Policías de 22 países.

Imágenes


GUARDIA CIVIL
Mº INTERIOR
GUARDIA CIVIL


GUARDIA CIVIL
Mº INTERIOR
CIVIL