28/11/25

Desmantelada una red de infraestructura tecnológica que recopilaban datos para ponerlos a disposición de ciberdelincuentes

Resumen

A través de un sistema informático exportaban miles de tarjetas SIM y enviaban millones de mensajes y llamadas simultáneamente

Se hacían pasar por agentes de la Policía Nacional y empleados del Banco de España y captaban, entre otras víctimas, a ciudadanos rusos y ucranianos residentes en España

Hay una persona detenida como encargada de crear y mantener activo el sistema

Contenido

La Guardia Civil, en la operación “Mosenik”, ha desmantelado una infraestructura tecnológica de gran capacidad, empleada para el envío masivo de mensajes y llamadas fraudulentas, que se ponía al servicio de grupos delictivos especializados en ciberestafas.

Se trata de un sistema informático industrial que permitía explotar miles de tarjetas SIM a la vez, enviando millones de mensajes y llamadas simultáneamente.

La investigación dio comienzo con varias denuncias en Alicante de perjudicados que estaban recibiendo llamadas en las que se hacían pasar por la Policía Nacional y por el Banco de España para presionarles y requerirles sus datos bancarios y transferencias de alto importe. Algunas de estas llamadas se realizaban en ruso o ucraniano para captar a residentes de estas nacionalidades en España.

En la operación ha sido detenido un hombre de 41 años al que se le imputan los delitos de estafa, usurpación de estado civil, falsedad documental, daños informáticos, blanqueo de capitales y pertenencia a grupo criminal.

Además, se han realizado tres registros en Barcelona, en una vivienda, un local comercial y un trastero donde se ha intervenido numeroso material informático y tecnológico valorado en 400.000 euros, entre el que destaca un maletín que albergaba una SIMBOX transportable, que permitía operar desde cualquier parte a través de una conexión a internet mediante WiFi o red móvil, dificultando ser localizado.

Se han incautado 35 SIMBOX industriales equipadas con 865 módems; 852 tarjetas SIM activas; más de 60.000 tarjetas SIM nacionales para su uso inmediato; 10.000 tarjetas SIM nuevas; una gran cantidad de dispositivos informáticos; dinero en efectivo y en criptomonedas.

El envío de mensajes y llamadas

El envío de mensajes y llamadas se realizaban desde una sofisticada infraestructura de SIMBOX industriales, en los que cada caja alberga cientos de módems GSM profesionales. Cada módem funciona individualmente como si fuera un teléfono móvil y es capaz de enviar entre 12 y 18 mensajes por minuto, es decir, 2,5 millones de mensajes al día. Esta red era controlada por una única persona mediante una decena de ordenadores.

Los números de teléfono remitentes eran cambiados frecuentemente, estando activos por un tiempo breve desde el alta para impedir que fueran rastreados.
Las tarjetas SIM eran compradas en grandes cantidades a diferentes proveedores y activadas con identidades falsas.

A pesar de la gran cantidad de contactos realizados a la vez, los investigadores han constatado que previamente estudiaban los perfiles de las potenciales víctimas y los mensajes o llamadas iban dirigidos hacia colectivos concretos.

Venta del sistema a ciberdelincuentes

El detenido tenía la función de crear y mantener activo el sistema, vendiendo este servicio a redes de ciberdelincuentes de todo el mundo.

La operación ha sido desarrollada por la Unidad Orgánica de Policía Judicial (UOPJ) de Alicante, el Equipo de Investigación Tecnológica de la UOPJ de Barcelona y la Unidad de Seguridad Ciudadana de Tarragona.

La investigación, dirigida por el Juzgado de Instrucción número 1 de Novelda, sigue abierta y la Guardia Civil continúa con el estudio del material intervenido y la localización de otros implicados y nuevas víctimas. Dado el valor del material intervenido y al tratarse de una red que daba infraestructura a múltiples grupos criminales, se estima que el montante estafado ascienda varios millones de euros.
Algunas ciberestafas, como los cargos fraudulentos con tarjetas bancarias y otros medios de pago electrónicos sin la autorización del titular, son algunos de los siete procedimientos que ya se pueden denunciar telemáticamente a través de la sede electrónica de la Guardia Civil https://guardiacivil.sede.gob.es

Para más información pueden contactar con la oficina de prensa de la Guardia Civil de Alicante, en el teléfono 96 514 56 60, extensión 0610011.

Imágenes


GUARDIA CIVIL
Mº INTERIOR


GUARDIA CIVIL
Mº INTERIOR


GUARDIA CIVIL
Mº INTERIOR


GUARDIA CIVIL
Mº INTERIOR