05/02/26

Investigadas doce personas por hacer de “mulas bancarias” de una organización criminal internacional

Resumen

Los autores usaban aplicaciones de control remoto para vaciar las cuentas bancarias de la víctima y solicitar préstamos a su nombre

El total de dinero estafado a la víctima asciende a 442.650 euros

Contenido

La Guardia Civil, en el marco de la operación “Vicentius”, ha investigado a doce personas como presuntos autores de delitos de estafa, blanqueo de capitales y acceso ilícito a sistemas informáticos. Se trata de ocho hombres y cuatro mujeres de entre 20 y 75 años, residentes en diferentes puntos del territorio nacional.

La persona perjudicada por este entramado criminal sufrió un perjuicio económico de 432.000 euros en criptoactivos.

Además, los agentes identificaron a dos residentes chinos, como presuntos integrantes de la organización criminal, y constataron que los datos personales y bancarios de la afectada también fueron utilizados para solicitar a su nombre dos préstamos bancarios por un importe de 10.450 euros. Esto elevó la estafa inicial a un total de 442.650 euros.

Una denuncia, el comienzo de la investigación
Esta operación se inició cuando la víctima presentó una denuncia ante la Guardia Civil en La Rioja. El motivo fue la detección de movimientos bancarios que no reconocía y la imposibilidad de recuperar las supuestas inversiones que había realizado en una plataforma de criptomonedas.

En su denuncia explicó que había sido contactada meses atrás por unos supuestos asesores financieros a través de plataformas digitales. Le convencieron para realizar una pequeña inversión inicial con la promesa de obtener beneficios extraordinarios.

Aplicaciones de control remoto
Los criminales facilitaron a la víctima el acceso a una plataforma web falsa. En ella podía visualizar gráficos y datos manipulados que mostraban cómo su capital crecía supuestamente de forma exponencial y en tiempo real. Esto llevó a la perjudicada a realizar sucesivas transferencias de dinero cada vez mayores con el fin de maximizar sus ingresos.

Una vez ganada su confianza, los estafadores la convencieron para instalar en sus dispositivos electrónicos un software de acceso remoto denominado “AnyDesk” con el pretexto de prestarle asistencia técnica para gestionar operaciones más complejas. Sin embargo, esta aplicación permitió a los ciberdelincuentes tomar el control total de su ordenador y de su teléfono móvil, accediendo directamente a sus credenciales bancarias y a toda su información personal.

Con el control de los equipos y de las claves bancarias, los responsables de la trama vaciaron totalmente las cuentas personales de la víctima, así como de otras que gestionaba desde sus dispositivos informáticos, pertenecientes a la empresa en la que trabajaba.

Además del capital sustraído, utilizaron su identidad para suscribir préstamos de concesión inmediata, incrementando el perjuicio económico. Este sofisticado entramado técnico y psicológico permitió rastrear la red internacional de blanqueo asociada a la estafa.

Los investigados eran las “mulas bancarias”

Los investigados en esta operación desempeñaban el papel de “mulas bancarias”. Estas personas actúan como intermediarios, cediendo sus cuentas o abriendo otras nuevas para recibir el dinero estafado a las víctimas.

Su función principal consiste en extraer, mover, fragmentar y redistribuir los fondos que reciben de los responsables de la organización. Para ello, realizan transferencias sucesivas a otras cuentas, tanto nacionales como extranjeras, o convierten el dinero en criptomonedas. Con estas operaciones encadenadas logran dificultar la trazabilidad del dinero, proteger la identidad de los verdaderos criminales y ocultar el origen ilícito de los fondos.

La investigación permitió rastrear hasta 42 transferencias dirigidas a cuentas ubicadas en Dinamarca, Lituania, Reino Unido y China, lo que facilitó seguir el recorrido del dinero y destapar una red criminal de carácter internacional con ramificaciones en Europa y Asia.

La investigación continúa abierta y centrada en determinar el destino final de los fondos para su posible recuperación.

Denuncia telemática

La Guardia Civil recuerda a los perjudicados por este tipo de delito la posibilidad de poder presentar denuncia telemática sin tener que acudir a una instalación oficial.

Puede acceder a la Sede Electrónica de la Guardia Civil, bien de forma directa, o bien desde la web corporativa de Guardia Civil o por medio del siguiente enlace https://web.guardiacivil.es/es/tramites/denuncias/denuncia-electronica/.

Además, en esta plataforma se pueden realizar otros cuatro procedimientos penales –daños, hurtos, sustracción de vehículos y sustracción en interior de vehículos- y dos procedimientos administrativos –pérdida o extravío de documentación y localización de documentación-.

Para acceder a los formularios específicos, se deberá realizar a través del sistema Cl@ve que permite identificar de forma inequívoca al denunciante que interpone la denuncia e informarle de los derechos que le asisten como denunciante.

Una vez completado el formulario, la denuncia no resultará válida hasta ser revisada y confirmada formalmente a través de la Sede Electrónica.

Para más información relacionada con esta nota, pueden contactar con la oficina de prensa de la Guardia Civil en La Rioja en el teléfono 941229900.

Imágenes