13/07/24

Detenido un hacker como presunto autor del ciberataque a una compañía eléctrica

Resumen

El detenido, que presumía tener la base de datos más grande de ciudadanos españoles, vendía los datos por Internet a cambio de criptomonedas

Contenido

Agentes de la Guardia Civil y los Mossos d'Esquadra han detenido en Madrid a un hacker especializado en ciberataques. Uno de estos ciberataques fue a una compañía de distribución eléctrica, donde robó datos de 37.000 de sus clientes.

La intrusión en los servidores de la compañía eléctrica, que se produjo en 2022, fue a través de la usurpación de credenciales autorizadas y la escalada de privilegios. El hacker, utilizando infraestructura ubicada en varios países, logró captar información sensible, tanto de la compañía como de sus clientes y usuarios.

El detenido transfería la información a terceros a cambio del pago en criptomonedas. Las criptomonedas son un sistema de monedas digitales descentralizado y pseudoanónimo que permite realizar transacciones financieras entre personas distantes y desconocidas. Las casas de cambio, llamadas exchanges, permiten el paso de criptomonedas a dinero fiduciario y viceversa.

Los técnicos informáticos de la compañía pudieron identificar las direcciones IP desde donde provenía el ataque. Detectaron el número de personas afectadas, el tipo de datos exfiltrados y la afectación a su servicio.

La empresa denunció los hechos, se puso en contacto con los usuarios afectados e informó del ataque a la Autoridad Catalana de Protección de Datos. Los investigadores, tras realizar diversas gestiones con los diferentes servicios que el hacker utilizó durante el ataque y gracias a la colaboración internacional, pudieron identificar al presunto autor de los hechos a través de la trazabilidad de las criptomonedas.

Una vez identificado, se estableció un equipo conjunto de investigación, ya que ambos cuerpos investigaban a la misma persona. En un operativo conjunto del Departamento contra el Cibercrimen de la UCO de la Guardia Civil y el Área Central de Cibercrimen de la DIC de los Mossos d'Esquadra, se practicó la detención y se realizaron dos registros en los que se recogieron evidencias de interés para la investigación.

Imágenes

mossos d'esquadra
GUARDIA CIVIL
Mº INTERIOR

mossos d'esquadra
GUARDIA CIVIL
Mº INTERIOR