05/02/25

Detenido un peligroso hacker responsable de más de 40 ciberataques a organismos estratégicos

Resumen

El investigado, que reivindicaba las intrusiones en foros de la darkweb, logró acceder a los servicios informáticos de entidades públicas y privadas entre las que se encontrarían la Guardia Civil, el Ministerio de Defensa, la Fábrica Nacional de Moneda y Timbre, el Ministerio de Educación, Formación Profesional y Deportes, la Generalitat Valenciana, diferentes Universidades españolas, bases de datos de la OTAN y del Ejército de EEUU, así como otras empresas y entidades internacionales

Durante el registro, los agentes han intervenido criptomonedas y diverso material informático el cual está siendo analizado por los especialistas, que no descartan el esclarecimiento de otros hechos delictivos

Contenido

La Guardia Civil y la Policía Nacional, en el marco de la operación “Abbadon-Theatre”, han detenido el pasado martes en la localidad de Calpe (Alicante) a una persona por su presunta participación en los delitos de descubrimiento y revelación de secretos, acceso ilícito a sistemas informáticos, daños informáticos y blanqueo de capitales.

El detenido realizó múltiples ataques a los servicios informáticos de empresas y entidades nacionales e internacionales, entre los que se encontraban servicios públicos y organismos de tipo gubernamental. Además, reivindicaba los ataques en foros de la darkweb bajo diferentes pseudónimos para evitar ser identificado y relacionado con los hechos delictivos.

En el registro de su domicilio se ha intervenido múltiple material informático que está siendo analizado por los especialistas y no se descarta esclarecer otros hechos similares. Además, el detenido disponía de más de 50 cuentas de criptomonedas con diferentes tipos de criptoactivos, hecho significativo del amplio conocimiento que el arrestado dispone del mundo blockchain.

Cambiaba de pseudónimo frecuentemente para evitar ser detectado

Tras estos hechos, y durante el año 2024, se sucedieron diversos ciberataques contra otras entidades, organismos públicos e incluso universidades españolas. Posteriormente, y utilizando hasta tres pseudónimos distintos, atacó a organismos internacionales y organizaciones de tipo gubernamental accediendo a bases de datos con información personal de empleados y clientes, así como documentos internos que posteriormente eran vendidos o publicados libremente en foros.

Ciberataques realizados contra importantes instituciones

La investigación sobre este objetivo fue iniciada por la Policía Nacional en febrero del pasado año, tras la denuncia de una asociación empresarial madrileña al detectar una publicación en un foro especializado de filtración de datos, donde alegaban estar en posesión de información procedente de su web. Realizadas las primeras gestiones, los agentes comprobaron que, no solo había extraído datos, sino que había dejado el portal desfigurado, mostrando un mensaje en el que se podía leer que habían hackeado el sistema.

Tras estos hechos y a lo largo del año 2024, esta persona fue realizando numerosos ciberataques, entre los que destaca el ataque a la Fábrica Nacional de Moneda y Timbre, el Servicio Público de Empleo Estatal, el Ministerio de Educación, Formación Profesional y Deportes, diferentes universidades españolas, así como a bases de datos de la OTAN, Ejercito de los Estados Unidos, la Dirección General de Tráfico, la Generalitat Valenciana, Naciones Unidas, la Organización Internacional de Aviación Civil, al Ministerio de Defensa y su último ataque reivindicado, a la Guardia Civil.

Este último ataque, ejecutado a finales de diciembre de 2024, propicia que por parte de la Unidad Central Operativa de la Guardia Civil se desarrolle la investigación del mismo y se identifique al mismo objetivo como autor, llevándose a cabo la explotación operativa de forma conjunta por ambos cuerpos policiales.

Medidas para ocultar el rastro de navegación durante sus ataques

El detenido, con profundos conocimientos de informática, había conseguido configurar un complejo entramado tecnológico mediante el uso de aplicaciones anónimas de mensajería y de navegación mediante las cuales habría conseguido ocultar su rastro y dificultar así su identificación.

La operación, que ha sido realizada de manera conjunta por agentes de la Guardia Civil y de la Policía Nacional, ha contado con la colaboración del Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

En el ámbito internacional se ha contado con la colaboración de Europol y Homeland Security Investigations (HSI) de los EE. UU.

El detenido ha sido puesto a disposición del Juzgado de Instrucción de Guardia de Denia.

Imágenes


GUARDIA CIVIL
Mº INTERIOR
POLICÍA NACIONAL


GUARDIA CIVIL
Mº INTERIOR
POLICÍA NACIONAL
GUARDIA CIVIL
UCO


GUARDIA CIVIL
Mº INTERIOR
UCO
POLICÍA NACIONAL