14/02/2025

Detenido un hacker de 18 años responsable de 40 ciberataques al Ejército de EEUU, la OTAN o la Guardia Civil

Detenido en Calpe (Alicante) un hacker, español de 18 años, por acceder a los servicios informáticos de 40 entidades, entre las que se encuentra la Guardia Civil, el Ministerio de Defensa, la OTAN o el Ejército de EEUU.



Según informa el Ministerio del Interior, el detenido está acusado por **delitos de descubrimiento y revelación de secretos**, acceso ilícito a los sistemas informáticos y dañar éstos, además de blanqueo de capital.

Recién estrenada la mayoría de edad, el joven español accedió a las bases de datos de empresas y entidades nacionales e internacionales, entre los que se encontraban servicios públicos y organismos de tipo gubernamental, para, posteriormente, **vender la información por la darkweb**. Los agentes han intervenido 50 cuentas de criptomonedas.

La investigación tiene su origen en 2024 con una primera denuncia de una asociación empresarial madrileña. Se denunció el hackeo y la extracción de datos, sin embargo, lo más sorprendente fue que **el autor firmó su ciberataque**: dejó el portal desfigurado, donde se podía leer que habían hackeado el sistema. Además, reivindicaba los ataques en foros bajo diferentes pseudónimos para evitar ser identificado y relacionado con los hechos delictivos.

A lo largo de 2024 realizó numerosos ataques informáticos, destacando la **Fábrica de Moneda y Timbre, la OTAN, el Ejército de los Estados Unidos, la DGT, la ONU, el Ministerio de Defensa o, su último ataque, la Guardia Civil.** Accedía a las bases de datos con información personal y documentos internos de empleados y clientes, que posteriormente eran vendidos o publicados libremente en foros.

Sin embargo, **fue este último acceso ilícito al sistema informático de la Guardia Civil lo que propició su detención** . Ocurrido a finales de diciembre de ese mismo año, provocó que la Unidad Central Operativa (UCO) se sumara a la investigación. Ambos cuerpos policiales llevaron a cabo una explotación cooperativa que dio con el autor de los hechos.

"El detenido tiene profundos conocimientos de informática", así lo declaran las fuerzas del orden. Había conseguido configurar un complejo entramado tecnológico de aplicaciones anónimas de mensajería y navegación, mediante las cuales ocultaba su rastro e imposibilitaba su identificación.

Presumía de los ataques en la 'dark web'

El cibercriminal operaba bajo **tres pseudónimos en la 'dark web'** y utilizaba estos alias para presumir de sus ataques y vender información sensible extraída de las bases de datos infiltradas.

Durante el registro de su vivienda, los agentes hallaron múltiples dispositivos electrónicos, que están siendo analizados por expertos en delitos tecnológicos. Además, el detenido disponía de más de **50 cuentas de criptomonedas con distintos activos digitales**, lo que demuestra su profundo conocimiento del ecosistema blockchain y su posible implicación en operaciones de blanqueo de capitales.

Un modus operandi perfeccionado

La investigación arrancó en febrero de 2024, cuando una **asociación empresarial madrileña** denunció la publicación de datos sustraídos de su portal en un foro especializado en filtraciones.

Los agentes descubrieron que no solo se había robado información confidencial, sino que el atacante había modificado la web dejando un mensaje que evidenciaba su autoría. Desde ese momento, los investigadores comenzaron a seguir su rastro y recopilaron pruebas de múltiples ataques que se fueron intensificando a lo largo del año.

Cargos y posible condena

El hacker enfrenta cargos por descubrimiento y revelación de secretos, acceso ilícito a sistemas informáticos, daños informativos y blanqueo de capitales. Las autoridades no descartan que puedan vincularlo a otros delitos similares y continúan analizando la magnitud de su actividad delictiva.

Fuente: https://www.antena3.com/

LINK DE LA NOTICIA