Desmantelan a grupo de ciberdelincuentes "más dañino del mundo" que intentó hackear al estudio Guyer & Regules

El ataque al estudio uruguayo ocurrió en 2023 y comprometió información sensible de la compañía "incluyendo pasaportes, contratos y documentos bancarios y fiscales".

20/02/2024

En base a AFP

Una operación policial internacional desmanteló al grupo de ciberdelincuentes **Lockbit**, presentado como "**el más dañino**" **del mundo** por ataques que perjudicaron a miles de personas y causaron pérdidas millonarias a hospitales, alcaldías u otras instituciones.

En setiembre de 2023 este grupo intentó hackear al estudio **Guyer & Regules**, dedicado a asuntos legales, contables e impositivos complejos.

La detención del grupo fue dada a conocer el martes por las autoridades de varios países. "Después de infiltrarse en la red del grupo, la **NCA** (agencia de lucha contra la delincuencia británica) tomó el control de los servicios de LockBit, comprometiendo la totalidad de su empresa criminal", anunció la NCA en un comunicado.

Según la NCA, el grupo atacó a "miles de víctimas en todo el mundo" y causó pérdidas que ascienden a miles de millones de dólares, incluidos los rescates pagados y los costes para las víctimas.

"Hackeamos a los hackers", dijo Graeme Biggar, director general de la NCA, anunciando la neutralización de LockBit en una conferencia de prensa en **Londres**.

LockBit se centró en infraestructuras críticas y grandes grupos industriales, con demandas de rescate que oscilan entre 5,4 y 75,4 millones de dólares.

En 2023, el grupo atacó al operador postal británico, a un hospital canadiense para niños, y en **Francia** a los hospitales de Corbeil Essonnes y Versalles en la región parisina.

Los ciberdelincuentes ponían a disposición de sus "afiliados" herramientas e infraestructuras que les permitían realizar ataques. Estos consistían en infectar la red informática de las víctimas para robar sus datos y cifrar sus archivos.

Se exigía un rescate en criptomonedas para descifrar y recuperar la información, bajo amenaza de publicar los datos de las víctimas.

La empresa **Birmingham Cyber Arms**, dedicada al desarrollo de hardware de inteligencia de amenazas y seguridad ofensiva, informó que el estudio uruguayo fue víctima de un ataque en el que se vio comprometida "información sensible de la compañía y clientes incluyendo pasaportes, contratos y documentos bancarios y fiscales" y el rescate solicitado por dicha información ascendía a US$ 300.000.

LockBit recibió más de 120 millones de dólares en rescates en total, según **Estados Unidos**, donde cinco personas -entre ellas dos ciudadanos rusos-, están siendo procesadas.

Según el jefe de la NCA, las investigaciones no revelaron un "apoyo directo" del Estado ruso hacia LockBit, pero sí una "tolerancia" hacia la **ciberdelincuencia** en **Rusia**.

"Son **delincuentes cibernéticos**. Tienen su sede en todo el mundo. Hay una gran concentración de estos individuos en Rusia y a menudo hablan ruso", subrayó.

LockBit está considerado uno de los software maliciosos más activos del mundo, con más de 2.500 víctimas, "entre ellas hospitales, ayuntamientos y empresas de todos los tamaños", indicó en un comunicado la fiscalía de París.

La operación permitió, según la fiscalía de París, "tomar el control de una parte importante de la infraestructura del software LockBit, incluido el 'darknet'", y la "Wall of Shame" (**Muro de la Vergüenza**) "donde se publicaban los datos de quienes se negaban a pagar el rescate".

Según la NCA británica, más de 200 cuentas de **criptomonedas** relacionadas con el grupo fueron congeladas y los investigadores obtuvieron más de 1.000 claves necesarias para descifrar los datos con el fin de devolverlos a sus propietarios.

"Este sitio está ahora bajo control de las fuerzas del orden", indica un mensaje en un sitio de LockBit, precisando que la NCA británica tomó el control del sitio, en cooperación con el FBI estadounidense y las agencias de varios países.

En noviembre de 2022, el Departamento de Justicia de Estados Unidos (DoJ) calificó el programa malicioso LockBit como el "más activo y destructivo de las variantes en el mundo".