Un ciudadano brasileño ha sido acusado en Estados Unidos por presuntamente amenazar con divulgar información obtenida tras hackear la red de una empresa en marzo de 2020.

Junior Barros De Oliveira, de 29 años y residente de Curitiba, Brasil, enfrenta cargos por cuatro casos de amenazas extorsivas relacionadas con datos extraídos de computadoras protegidas y cuatro cargos por comunicaciones amenazantes, según lo informado por el Departamento de Justicia de EE. UU. (DoJ) en una acusación formal divulgada esta semana.

El acusado habría vulnerado la seguridad de los sistemas de una filial brasileña de una compañía con sede en Nueva Jersey, accediendo de forma ilícita a la información confidencial de unos 300,000 clientes en al menos tres ocasiones distintas.

Se alega que, en septiembre de 2020, De Oliveira envió un correo electrónico al director ejecutivo (CEO) de la compañía, utilizando un nombre falso, en el que solicitaba un pago de 300 bitcoins (equivalente a unos 3.2 millones de dólares en ese momento) para no divulgar ni vender los datos robados.

En octubre del mismo año, el acusado habría reenviado dicho correo tanto al CEO como a un ejecutivo de la filial brasileña.

En mensajes posteriores dirigidos a un representante de la empresa, De Oliveira afirmó estar «*muy interesado en ayudarles a resolver esta vulnerabilidad de seguridad*», pero señaló que dicho servicio requeriría el pago de una tarifa de consultoría de 75 bitcoins (aproximadamente 800,000 dólares en ese momento). En dichos mensajes, también incluyó las instrucciones para transferir el monto a una billetera de Bitcoin.

Cada uno de los cargos de amenazas extorsivas podría conllevar una pena máxima de cinco años de prisión y una multa de hasta 250,000 dólares o el doble del valor de las ganancias o pérdidas derivadas, según cuál sea mayor.

Asimismo, los cargos de comunicaciones amenazantes conllevan penas máximas de dos años de prisión y multas similares, de hasta 250,000 dólares o el doble del valor de cualquier

beneficio o perjuicio ocasionado.