El gobierno estadounidense acusó a un experto en seguridad informática de haber hackeado un intercambio de criptomonedas y haber robado alrededor de $9 millones en criptomonedas. Parece ser un caso en el que un hacker ético se convierte en un hacker malintencionado y luego intenta aparentar ser ético nuevamente.

En un comunicado de prensa el martes, la Oficina del Fiscal de los Estados Unidos para el Distrito Sur de Nueva York anunció la acusación de Shakeeb Ahmed, de 34 años, a quien describió como *«un ingeniero de seguridad de alto nivel de una compañía tecnológica internacional, cuyo currículum muestra habilidades en, entre otras cosas, el análisis inverso de contratos inteligentes y las auditorías de blockchain. Estas son algunas de las habilidades especializadas que Ahmed utilizó para llevar a cabo el ataque».*

No se mencionó específicamente dónde trabajaba Ahmed. Su perfil de LinkedIn indica que es un ingeniero de seguridad principal en Amazon. August Aldebot-Green, portavoz de Amazon, dijo a TechCrunch que ya no trabaja en la empresa.

Si bien los fiscales no especificaron quién fue la víctima, el sitio web de noticias sobre criptomonedas CoinDesk informó que la descripción y la fecha del hackeo coinciden con el ataque a Crema Finance, un intercambio basado en Solana, que ocurrió a principios de julio de 2022, alrededor de las mismas fechas (2 y 3 de julio) en las que se acusa a Ahmed de haber pirateado un intercambio no revelado.

En ese caso, el hacker terminó devolviendo aproximadamente $8 millones en criptomonedas y se quedó con el resto, según se informó en ese momento. En su comunicado de prensa, los fiscales del Departamento de Justicia (DOJ) dijeron que Ahmed *«mantuvo comunicaciones con el intercambio de criptomonedas en las que decidió devolver todos los fondos robados, excepto $1.5 millones, si el intercambio de criptomonedas aceptaba no informar del ataque a las autoridades».*

Esta es una práctica muy común en el mundo de las criptomonedas y web3. En el pasado, los hackers que robaban criptomonedas y ofrecían devolver parte de ellas mediante negociaciones directas con las víctimas a veces se hacían llamar *«sombreros blancos»,*

término utilizado en el argot de la seguridad informática para referirse a los hackers con buenas intenciones. Estos hackers han tomado una palabra con un significado claro y establecido y la han adaptado para una práctica que se encuentra en un área gris, por decir lo menos.

Y, como se muestra en este caso, devolver parte del botín de criptomonedas no significa que no se pueda enfrentar un proceso legal.

Las autoridades destacaron el hecho de que Ahmed, acusado de fraude electrónico y lavado de dinero, utilizó las habilidades que adquirió en sus trabajos anteriores para llevar a cabo el robo.

> *«Ahmed utilizó sus habilidades como ingeniero de seguridad informática para robar millones de dólares. Luego, supuestamente intentó ocultar los fondos robados, pero sus habilidades no fueron suficientes para el Equipo de Cibercrimen de Investigación Criminal del IRS»,* declaró el Agente Especial a Cargo Tyler Hatcher, quien trabaja para IRC-CI, la división de investigación criminal del IRS, según se cita en un comunicado de prensa.

Según la acusación contra Ahmed, este aprovechó una vulnerabilidad en el intercambio e introdujo *«datos de precios falsos para generar fraudulentamente millones de dólares en comisiones infladas, que en realidad no había ganado pero aún así pudo retirar».*

Luego, según las autoridades, Ahmed supuestamente blanqueó las criptomonedas robadas *«a través de una serie de transacciones»,* como el intercambio de tokens y la transferencia de los fondos de la cadena de bloques Solana a la cadena de bloques Ethereum, entre otras.

Más tarde, Ahmed también supuestamente buscó en línea información sobre el hackeo, *«su propia responsabilidad penal»,* abogados especializados en casos similares, si las fuerzas del orden podrían investigar dicho ataque y *«huir de Estados Unidos para evitar cargos penales»*.