El gobierno de Estados Unidos presentó hoy una demanda que busca tomar el control de 280 cuentas de Bitcoin y Ethereum que parecen tener fondos que los hackers norcoreanos robaron de dos plataformas de intercambio de criptomonedas.

Los documentos judiciales no identificaron los exchangers hackeados, pero los funcionarios afirmaron que los dos ataques ocurrieron el 1 de julio de 2019 y el 25 de septiembre de 2019.

En el primer incidente, los hackers de Corea del Norte robaron 272 mil dólares en criptomonedas y tokens alternos, incluidos Proton, PlayGame y tokens del protocolo IHT Real Estate. En el segundo incidente, los hackers robaron múltiples criptomonedas, con un valor total de más de 2.5 millones de dólares.

Los funcionarios estadounidenses dijeron que utilizaron el análisis de blockchain para rastrear los fondos robados de dos portales de intecambio pirateados.

Según los documentos judiciales, Estados Unidos afirma que los hackers norcoreanos utilizaron una técnica conocida como *«salto en cadena»* para lavar los fondos robados. La técnica, también conocida como *«salto de cadena de bloques»,* se refiere a tomar los fondos de algún tipo de criptomoneda e intercambiarlos por otra.

El Departamento de Justicia asegura que los piratas informáticos norcoreanos generalmente robaron fondos de un intercambio, transfirieron los fondos a otro intercambio donde se encadenaron varias veces y finalmente, reunieron todos los fondos en las 280 cuentas con BTC y ETH que se han rastreado.

También se lee en los documentos que las 280 direcciones están actualmente congeladas en los portales de criptomonedas donde se establecieron.

Las cuentas se congelaron inmediatamente luego de los ataques, ya que los portales de intercambio de criptomonedas cooperaron entre sí para rastrear fondos y congelar cuentas

antes de que los fondos se volvieran a convertir en moneda fiduciaria y todos los rastros se perdieran para siempre.

Ahora, el gobierno de Estados Unidos quiere tomar el control formal de esas cuentas para devolver el dinero a los exchangers o usuarios afectados.

El Departamento de Justicia de Estados Unidos dijo que los dos ataques cibernéticos están conectados con otros ataques norcoreanos y operaciones de lavado de dinero que expusieron en marzo de 2019, cuando acusaron a dos ciudadanos chinos por ayudar a los hackers norcoreanos a lavar sus ganancias a través de empresas chinas.

En septiembre de 2019, el Tesoro de Estados Unidos sancionó a tres grupos de hacking de Corea del Norte y tomó medidas para congelar los activos financieros asociados con sus empresas fantasma.