La agencia de policía noruega Økokrim anunció la incautación de 60 millones de coronas noruegas (alrededor de 5.84 millones de dólares) en criptomonedas robadas por Lazarus Group en marzo de 2022, después del hackeo del puente Axie Infinity Ronin.

> *«Este caso demuestra que también tenemos una gran capacidad para seguir el dinero en la cadena de bloques, incluso si los delincuentes usan métodos avanzados»*, dijo la agencia en un comunicado.

El desarrollo se produce más de 10 meses después de que el Departamento del Tesoro de Estados Unidos implicara al grupo de hacking respaldado por Corea del Norte por el robo de 620 millones de dólares del puente de cadena cruzada Ronin.

Después, en septiembre de 2022, el gobierno de Estados Unidos anunció la recuperación de más de 30 millones de dólares en criptomonedas, lo que representa el 10% de los fondos robados.

Økokrim dijo que trabajó con socios internacionales encargados de hacer cumplir la ley para seguir y reconstruir el rastro del dinero, lo que dificulta que los hackers lleven a cabo actividades de lavado de dinero.

> *«Este es dinero que puede apoyar a Corea del Norte y su programa de armas nucleares. Por lo tanto, ha sido importante rastrear al criptomoneda y tratar de detener el dinero cuando intentan retirarlo en activos físicos»*, agregó.

El desarrollo se produce cuando los intercambios de criptomonedas Binance y Huobi congelaron cuentas que contenían aproximadamente 1.4 millones de dólares en criptomonedas que se originaron a partir del hackeo de junio de 2022 de Harmony´s Horizon Bridge.

El ataque, también atribuido a Lazarus Group, permitió a los hackers lavar parte de las ganancias a través de Tornado Cash, que fue sancionado por el gobierno de Estados Unidos en agosto de 2022.

> *«Los fondos robados permanecieron inactivos hasta hace poco, cuando los investigadores comenzaron a verlos canalizados por medio de complejas cadenas de transacciones hacia los intercambios»,* dijo la semana pasada la compañía de análisis de blockchain, Elliptic.

Además, hay indicios de que Blender, otro mezclador de criptomonedas que fue sancionado en mayo de 2022, puede haber resucitado como Sinbad, lavando casi 100 millones de dólares en Bitcoin de hackeos atribuidos a Lazarus Group, según Tom Robinson de Elliptic.

Según la compañía, los fondos desviados a raíz del robo de Horizon Bridge fueron *«lavados por medio de una serie compleja de transacciones que involucran intercambios, puentes entre cadenas y mezcladores»*.

> *«Se usó Tornado Cash una vez más, pero en lugar de Blender, se usó otro mezclador de Bitcoin: Sinbad».*

Aunque el servicio se lanzó solo a principios de octubre de 2022, se estima que facilitó decenas de millones de dólares de Horizon y otros hacks vinculados a Corea del Norte.

En el período de dos meses que va desde diciembre de 2022 hasta enero de 2023, el grupo de estado-nación ha enviado un total de 1429.6 Bitcoin por un valor aproximado de 24.2 millones de dólares al mezclador, según reveló Chainalysis a inicios del mes.

La evidencia de que Sinbad es *«muy probablemente»* un cambio de marca de Blender, se deriva de las superposiciones en la dirección de la billetera utilizada, su nexo con Rusia y los

puntos en común en la forma en que ambos mezcladores funcionan.

> *«El análisis de las transacciones de blockchain muestra que una billetera de Bitcoin usada para pagar a las personas que promovían Sinbad, recibió Bitcoin de la billetera del operador de Blender sospechoso»,* dijo Elliptic.

> *«El análisis de las transacciones de blockchain muestra que casi todas las primeras transacciones entrantes a Sinbad (alrededor de $22 millones) se originaron en la billetera del operador de Blender».*

El creador de Sinbad, que usa el alias «*Mehdi*«, dijo a WIRED que el servicio se lanzó en respuesta a la «creciente centralización de las criptomonedas» y que es un proyecto legítimo de preservación de la privacidad similar a monero, Zcash, Wasabi y Tor.

Los hallazgos también llegan cuando las entidades de atención médica están en el punto de mira de una nueva ola de ataques de ransomware orquestados por los hackers de Lazarus para generar ingresos ilícitos para la nación afectada por las sanciones.

Las ganancias obtenidas de estos ataques con motivación financiera se usan para financiar otras actividades cibernéticas que incluyen el espionaje del sector de defensa y las organizaciones de base industrial de defensa en Corea del Sur y Estados Unidos, según un aviso conjunto emitido por los dos países.

Pero las acciones de aplicación de la ley aún no frenan la prolífica ola de ataques del actor de amenazas, que ha seguido evolucionando con nuevos comportamientos.

Esto comprende una amplia gama de técnicas antiforenses que están diseñadas para borrar los rastros de las intrusiones, así como para obstruir el análisis, reveló AhnLab Security Emergency Response Center (ASEC) en un informe.

> *«El grupo Lazarus realizó un total de tres técnicas: ocultación de datos, eliminación de artefactos y ofuscación de rastros»,* dijeron los investigadores de ASEC.