Se recuperaron más de 30 millones de dólares en criptomonedas robadas por Lazarus Group, vinculado a Corea del Norte, del videojuego en línea Axie Infinity, lo que marca la primera vez que se incautan activos digitales robados por el grupo de hackers.

> *«Las incautaciones representan aproximadamente el 10% del total de los fondos robados de Axie Infinity (teniendo en cuenta las diferencias de precio entre el tiempo robado y el tiempo incautado), y demuestran que cada vez es más difícil para los atacantes cobrar con éxito sus ganancias criptográficas malhabidas»*, dijo Erin Plante, directora senior de investigaciones de Chainlysis.

El desarrollo llega más de cinco meses después de que se robaron 620 millones de dólares de la plataforma de finanzas descentralizadas (DeFi) Ronin Network, y los atacantes lograron lavar la mayoría de los activos, siendo alrededor de 455 millones de dólares, por medio de la criptomoneda basada en Ethereum Tornado Cash.

El robo de criptomonedas de marzo de 2022 resultó en pérdidas de un total de 173,600 ETH con un valor aproximado de 594 millones de dólares en ese momento, y 25.5 millones de dólares en monedas estables USDC, lo que lo convierte en el mayor robo de criptomonedas hasta ahora.

Aunque Tornado Cash surgió como una herramienta popular para anonimizar las transacciones de criptomonedas, su abuso por parte de hackers como Lazarus Group para cobrar los activos obtenidos ilegalmente lo ha puesto en la mira del gobierno de Estados Unidos, que impuso sanciones contra el servicio el mes pasado.

La compañía de análisis de blockchain dijo que la lista de bloqueo obligó al adversario a alejarse del mezclador a favor de los servicios de DeFi, como los puentes criptográficos, para saltar en cadena y mover activos digitales entre cadenas en un intento por ocultar el rastro de los fondos.

> *«El hacker unió ETH desde la cadena de bloques Ethereum a la cadena BNB y después cambió ese ETH por USDD, que luego se unió a la cadena BitTorrent»,* dijo Plante, detallando el cambio entre varios tipos distintos de criptomonedas en una sola transacción.

Lazarus Group es una Amenaza Persistente Avanzada (APT) que está impulsada por los esfuerzos para apoyar los objetivos operativos de Corea del Norte, que incluyen el espionaje y la generación de ingresos para la nación afectada por las sanciones al golpear las instituciones financieras. La mayoría de las operaciones cibernéticas son realizadas por elementos dentro de la Oficina General de Reconocimiento.

La incautación también se produce cuando seis usuarios de Tornado Cash, incluyendo los empleados de Coinbase, presentaron una demanda esta semana contra el Departamento del Tesoro de Estados Unidos, la Secretaria del Tesoro, Janet Yellen, y otros funcionarios por su decisión de imponer sanciones a la plataforma.

La recuperación de criptomonedas también es indicativa del avance que han logrado las autoridades estadounidenses en su capacidad para rastrear e incautar fondos robados en criptomonedas de varios delitos cibernéticos.

A fines de julio, el Departamento de Justicia anunció la incautación de 500,000 dólares en Bitcoin de un equipo de hackers de Corea del Norte, que extorsionó los pagos digitales de los centros de atención médica mediante el uso de una nueva variedad de ransomware conocida como Maui.