El Departamento del Tesoro de Estados Unidos implicó al Grupo Lazarus (también conocido como Hidden Cobra), respaldado por Corea del Norte, en el robo de 540 millones de dólares del Ronin Network, del videojuego Axie Infinity el mes pasado.

El jueves, el Tesoro vinculó la dirección de la billetera Ethereum que recibió la moneda digital robada al actor de amenazas y sancionó los fondos agregando la dirección a la Lista de Nacionales Especialmente Designados (SDN) de la Oficina de Control de Activos Extranjeros (OFAC).

> *«El FBI, en coordinación con el Tesoro y otros socios del gobierno de Estados Unidos, seguirá exponiendo y combatiendo el uso de actividades ilícitas por parte de la RPDC, incluidos los delitos cibernéticos y el robo de criptomonedas, para generar ingresos para el régimen»,* dijo la agencia de inteligencia y aplicación de la ley en un comunicado.

El robo de criptomonedas, el segundo robo cibernético más grande hasta ahora, involucró el desvío de 173,600 ETH y 25.5 millones de monedas de USD del puente de cadena cruzada Ronin, que permite a los usuarios transferir sus activos digitales de una red criptográfica a otra, el 23 de marzo de 2022.

«El atacante usó claves privadas hackeadas para falsificar retiros», explicó Ronin Network en su informe de divulgación una semana después de que saliera a la luz el incidente.

Al sancionar la dirección de la billetera, la medida prohíbe que las personas y entidades estadounidenses realicen transacciones con ella para garantizar que el grupo patrocinado por el estado no pueda retirar más fondos. Un análisis de Elliptic encontró que el atacante ya logró lavar el 18% de los fondos digitales desviados (alrededor de 97 millones de dólares) a partir del 14 de abril.

> *«Primero, el USDC robado se cambió por ETH a través de intercambios*

> *descentralizados (DEX) para evitar que sea incautado. Al convertir los tokens en DEX, el hacker evitó las comprobaciones contra el lavado de dinero (AML) y 'conozca a su cliente' (KYC) realizadas en los intercambios centralizados»,* dijo Elliptic.

Casi 80.3 millones de dólares de los fondos lavados involucraron el uso de Tornado Cash, un servicio de mezcla en la cadena de bloques Ethereum diseñado para ocultar el rastro de los fondos, con otros 9.7 millones de dólares en Ethereum que probablemente se laven de la misma forma.

Lazarus Group, un nombre general asignado a prolíficos actores patrocinados por el estado que operan en nombre de los intereses estratégicos de Corea del Norte, tiene un historial de robos de criptomonedas desde al menos 2017 para eludir las sanciones y financiar los programas nucleares y de armamento del país.

> *«Se cree que las operaciones de espionaje del país reflejan las preocupaciones y prioridades inmediatas del régimen, que probablemente se centren actualmente en adquirir recursos financieros a través de criptoatracos, apuntando a medios, noticias y entidades políticas, e información sobre relaciones exteriores»,* dijo Mandiant.

La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), describió a los actores cibernéticos como un colectivo cada vez más sofisticado que ha desarrollado e implementado una amplia gama de herramientas de malware en todo el mundo para facilitar estas actividades.

Se sabe que el grupo robó un valor estimado de 400 millones de dólares en activos digitales de plataformas criptográficas en 2021, lo que marca un salto del 40% desde 2020, según Chainalysis, con solo el 20% de esos fondos robados asociados con Bitcoin y Ethereum representando un 58% mayoría. Los tokens ERC-20 y otras monedas alternativas constituyen

el 22% restante.

A pesar de las sanciones impuestas por el gobierno de Estados Unidos al colectivo de hackers, las campañas recientes emprendidas por el grupo capitalizaron las aplicaciones de billetera de finanzas descentralizadas (DeFi) con troyanos para sistemas Windows de puerta trasera y malversación de fondos de usuarios desprevenidos.

Además, en otra ofensiva cibernética revelada por Broadcom Symantec esta semana, se observó al actor apuntando a organizaciones de Corea del Sur que operan dentro del sector químico en lo que parece ser una continuación de una campaña de malware denominada *«Operation Deam Job»,* lo que corrobora los hallazgos del Grupo de Análisis de Amenazas de Google en marzo de 2022.

Las intrusiones, detectdas a inicios de enero, comenzaron con un archivo HTM sospechoso recibido como enlace en un correo electrónico de phishing o descargado de Internet, que al abrirse, desencadena una secuencia de infección, lo que finalmente conduce a la recuperación de una carga útil de segunda etapa de un servidor remoto para facilitar futuras incursiones.

El objetivo de los ataques, evaluó Symantec, es *«obtener propiedad intelectual para promover los propios objetivos de Corea del Norte en esta área».*

La avalancha continua de actividades ilícitas perpetradas por el Lazarus Group también ha llevado al Departamento de Estado de Estados Unidos a anunciar una recompensa de 5 millones de dólares por *«información que conduzca a la interrupción de los mecanismos financieros de personas involucradas en ciertas actividades que apoyan a Corea del Norte».*

El desarrollo se produce días después de que un tribunal estadounidense en Nueva York sentenciara a Virgil Griffith, un ex desarrollador de Ethereum de 39 años, a cinco años y tres meses de prisión por ayudar a Corea del Norte a usar monedas virtuales para evadir las sanciones.

> *«Casi el 97% de todas las criptomonedas robadas en los primeros tres meses de 2022 se tomaron de los protocolos DeFi, frente al 72% en 2021 y solo el 30% en 2020»,* dijo Chainalysis en un informe.

> *«Sin embargo, para los protocolos DeFi en particular, los robos más grandes generalmente se deben a un código defectuoso. Los exploits de código y los ataques de préstamo flash, un tipo de exploit de código que involucra la manipulación de los precios de las criptomonedas, han representado gran parte del valor robado fuera del ataque de Ronin»*, agregó la compañía de análisis de blockchain.