Lazarus Group, vinculado a Corea del Norte, ha sustraído cerca de 240 millones de dólares en criptomonedas desde junio de 2023, marcando un aumento notable en sus ataques cibernéticos.

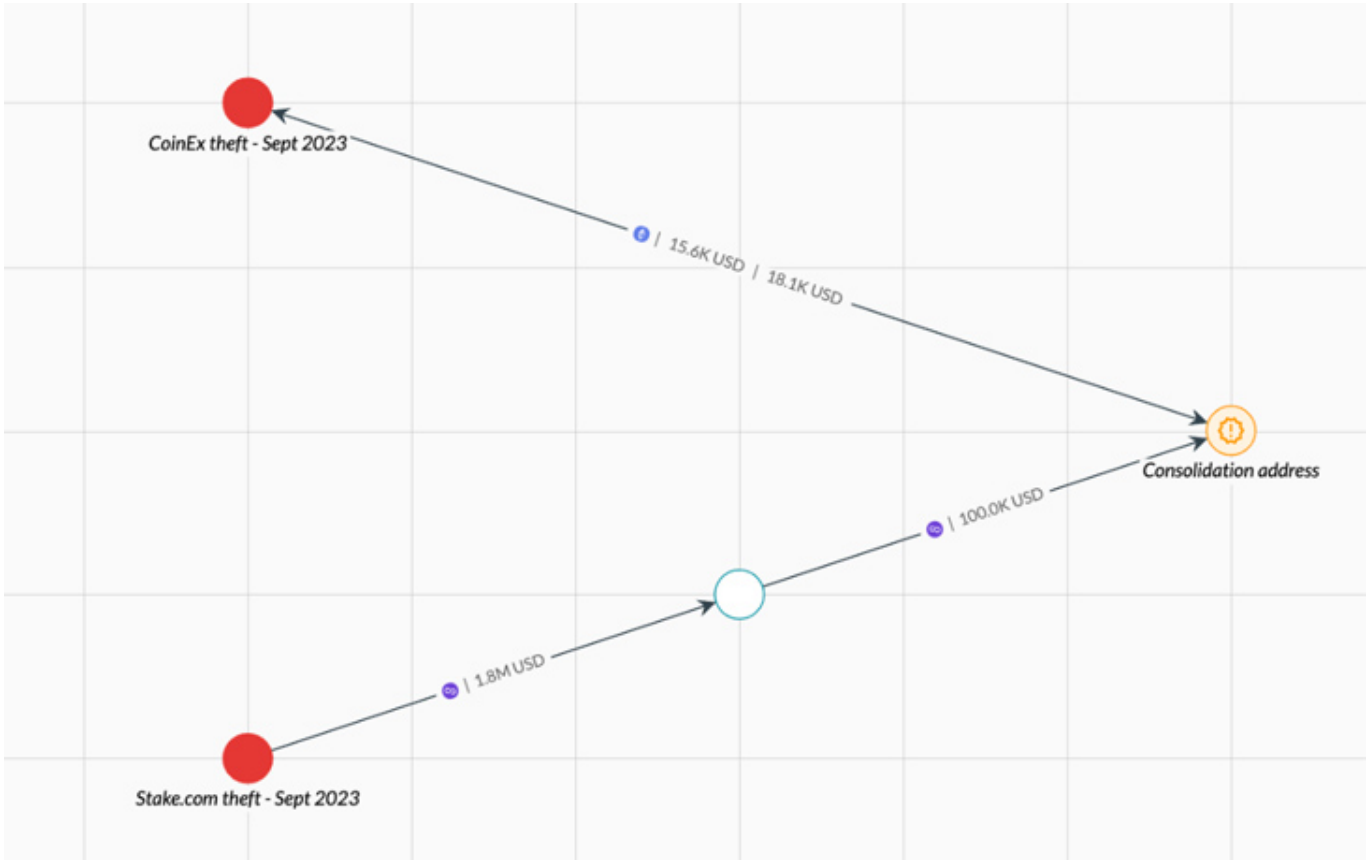
Según informes de diversas fuentes, como Certik, Elliptic y ZachXBT, se sospecha que este infame grupo de piratería estuvo detrás del robo de 31 millones de dólares en activos digitales de la plataforma CoinEx el 12 de septiembre de 2023.

Este robo de criptomonedas en CoinEx se suma a una serie de ataques recientes contra Atomic Wallet (100 millones de dólares), CoinsPaid (37,3 millones de dólares), Alphapo (60 millones de dólares) y Stake.com (41 millones de dólares).

> *«Algunos de los fondos sustraídos de CoinEx se enviaron a una dirección previamente utilizada por el grupo Lazarus para ocultar fondos robados a Stake.com, aunque en una cadena de bloques diferente. Luego, estos fondos se movieron a la plataforma Ethereum a través de un puente previamente empleado por Lazarus, y después se reenviaron a una dirección conocida como controlada por el ciberdelincuente de CoinEx»,* declaró Elliptic.

La firma de análisis de blockchain señaló que estos recientes ataques indican que el colectivo adversario está cambiando su enfoque desde servicios descentralizados hacia servicios centralizados, que eran sus objetivos antes de 2020.

Este cambio de estrategia probablemente esté motivado por mejoras en la auditoría de contratos inteligentes y en los estándares de desarrollo en el espacio de Finanzas Descentralizadas (DeFi), así como por el mayor acceso proporcionado por los intercambios centralizados mediante ataques de ingeniería social.



Este desarrollo coincide con la visita del líder de la nación sancionada, Kim Jong Un, a Rusia en lo que se cree que fue un acuerdo relacionado con armamento, a pesar de que, a principios de semana, se lanzaron dos misiles balísticos de corto alcance hacia sus aguas orientales.

Corea del Norte ha utilizado los robos de criptomonedas como una forma de eludir las sanciones internacionales y financiar sus programas de armamento. Otra fuente de ingresos es la utilización de trabajadores independientes de tecnología de la información en el extranjero que emplean documentos de identidad falsos para ocultar su nacionalidad real.

> *«En los últimos años, hemos observado un marcado aumento en el tamaño y alcance de los ciberataques contra empresas relacionadas con criptomonedas por*

> *parte de Corea del Norte. Esto ha coincidido con un aparente avance en los programas nucleares y de misiles balísticos del país»*, indicó TRM Labs en junio de 2023.

El grupo Lazarus y sus subdivisiones, junto con otros grupos de piratería vinculados a Corea del Norte, han estado llevando a cabo una serie de operaciones maliciosas en los últimos meses, que incluyen ataques a la cadena de suministro de software dirigidos a empresas como 3CX y JumpCloud, así como a repositorios de código abierto de JavaScript y Python.

En un análisis posterior al ataque, CoinsPaid reveló que falsos reclutadores de empresas de criptomonedas contactaron a sus empleados a través de LinkedIn y diversas aplicaciones de mensajería con ofertas de empleo atractivas, con el fin de engañarlos para que *«instalaran el agente JumpCloud o un programa especial para llevar a cabo una tarea técnica»*, en una campaña conocida como Operación Trabajo de Ensueño.