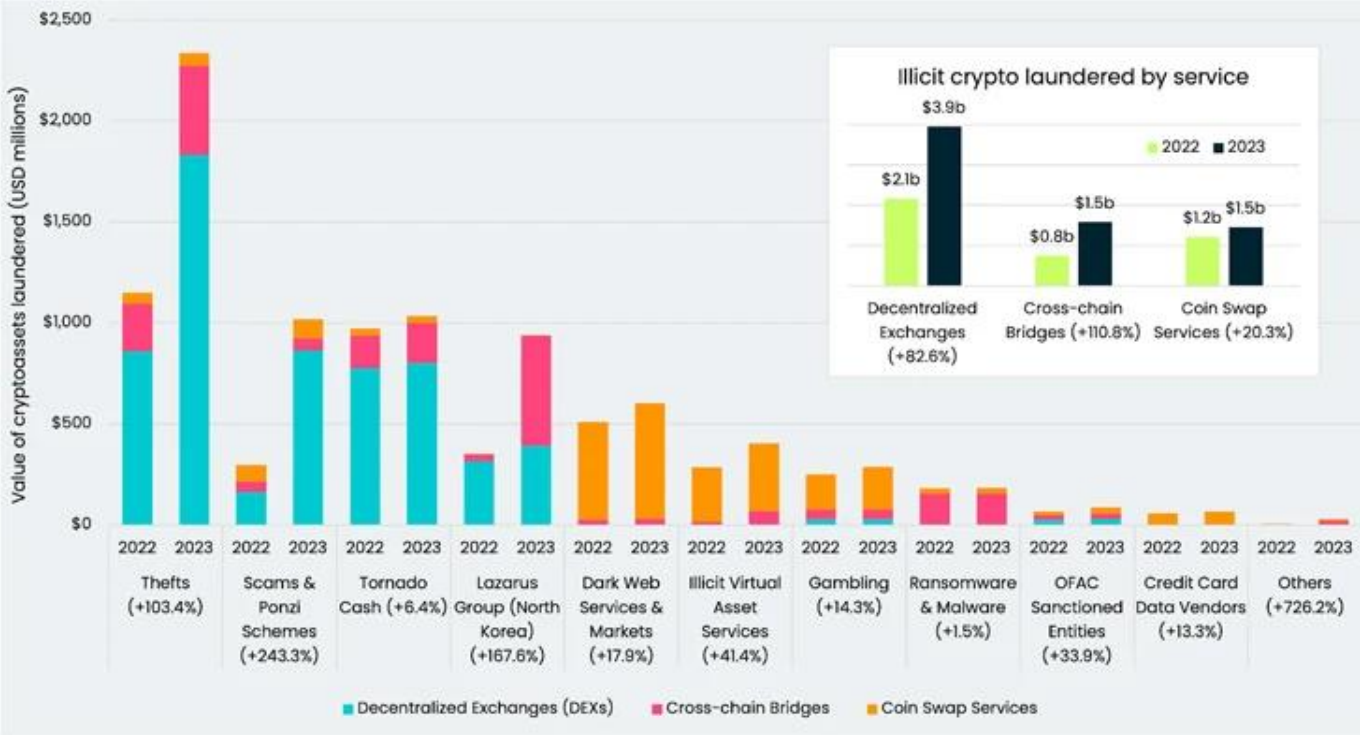
Hasta un total de $7 mil millones en criptomonedas han sido ilegalmente blanqueados mediante actividades transfronterizas, y el grupo Lazarus, vinculado a Corea del Norte, está asociado al robo de aproximadamente $900 millones de esos fondos entre julio de 2022 y julio de este año.

> *«Según un informe recién publicado esta semana por la empresa de análisis de blockchain Elliptic, a medida que las entidades tradicionales como los mezcladores continúan siendo objeto de confiscaciones y escrutinio por parte de las autoridades, la tendencia a cometer crímenes criptográficos mediante cambios o movimientos de activos entre cadenas también está en aumento»*, afirmó Elliptic en su informe.

La actividad de crimen transfronterizo hace referencia a la conversión de activos criptográficos de un token o cadena de bloques a otra, a menudo de manera rápida y consecutiva, con el objetivo de ocultar su origen. Esto se ha convertido en un método lucrativo para el lavado de dinero en casos de robos de criptomonedas y representa una alternativa a enfoques como el uso de mezcladores.

De acuerdo con los datos recopilados por Elliptic, el grupo Lazarus ha utilizado puentes transfronterizos para la mayoría de los fondos enviados a través de estos servicios, contribuyendo al aumento del 111% en la proporción de fondos transferidos de esta manera.

Se estima que el grupo de hackers norcoreanos ha sustraído casi $240 millones en criptomonedas desde junio de 2023, tras una serie de ataques dirigidos hacia Atomic Wallet ($100 millones), CoinsPaid ($37.3 millones), Alphapo ($60 millones), Stake.com ($41 millones) y CoinEx ($31 millones).




> *«La empresa de seguridad cibernética ESET describió el mes pasado al grupo de amenazas señalando su diversidad, cantidad y originalidad en la ejecución de sus campañas, así como su participación en los tres pilares de actividades cibercriminales: ciberespionaje, cibersabotaje y búsqueda de ganancias financieras».*

Este actor de amenazas también ha sido relacionado con el uso de Avalanche Bridge para depositar más de 9,500 bitcoins, mientras que simultáneamente utiliza soluciones transfronterizas para trasladar parte de los activos obtenidos ilegalmente.

> *«Como lo evidencia la repetición de transacciones en la misma cadena de bloques en numerosas ocasiones, estas operaciones no tienen ningún propósito comercial legítimo más allá de ocultar su procedencia. El proceso de realizar transferencias*

> *hacia adelante y hacia atrás con el único fin de ocultar su origen, es decir, el 'salto entre cadenas', es ahora una tipología ampliamente reconocida de lavado de dinero»,* declaró Elliptic.

Esto se da a conocer mientras que el Servicio de Inteligencia Nacional de Corea del Sur (NIS) ha emitido una advertencia sobre los ataques de Corea del Norte contra su sector de construcción naval desde el comienzo del año.

> *«Los métodos de piratería utilizados principalmente por las organizaciones de hackers norcoreanas consisten en tomar el control y evadir los sistemas informáticos de empresas de mantenimiento de TI, y posteriormente instalar código malicioso tras distribuir correos electrónicos de phishing entre los empleados internos»*, comunicó la agencia.