25/11/2025

Ciberseguridad en el mundo cripto: avances, riesgos y aprendizajes de 2025

Durante 2025, pérdidas multimillonarias y ataques sofisticados pusieron a prueba la confianza en el futuro de las criptomonedas



El año 2025 estuvo marcado por pérdidas récord en ataques y fraudes en el universo de las criptomonedas. Solo en la primera mitad del año, los robos ya totalizaron 2,17 mil millones de dólares, superando el valor total registrado en 2024, según Chainalysis. Y las proyecciones indican que 2025 podría terminar con más de 4 mil millones de dólares en activos desviados, un máximo histórico.

Este escenario de vulnerabilidad contrasta con la creciente institucionalización del sector. Si bien los ETF de criptomonedas registraron entradas récord de 5.95 mil millones de dólares e inversores corporativos como Strategy (anteriormente MicroStrategy) anunciaron nuevas compras de Bitcoin, el mercado expuso sus debilidades de seguridad.

La BBC señaló que el ataque de 1.500 millones de dólares al exchange Bybit, atribuido a hackers vinculados a Corea del Norte, fue el más grande de la historia, simbolizando así esta contradicción: incluso con avances regulatorios y técnicos, se siguen explotando fallas conocidas.

A continuación, veremos algunos de los principales casos ocurridos en 2025 y cómo vulnerabilidades aparentemente simples resultaron en robos millonarios que sacudieron el mercado de criptomonedas.

Panorama general: los números y el tamaño del problema

El año 2025 se ha consolidado como un período de pérdidas históricas para el mercado de criptoactivos. Según CertiK,La industria perdió casi 2.5 mil millones de dólares por ataques y estafas solo en los primeros seis meses del año. Chainalysis, por otro lado,eñaló que el volumen de criptoactivos robados en el mismo período superó la marca de 2.17 mil millones de dólares registrada en todo 2024. Manteniendo este ritmo, las pérdidas podrían superar los 4 mil millones de dólares para fin de año, lo que haría de 2025 el año con la mayor cantidad de activos desviados en la historia de las criptomonedas.

Aunque el número total de incidentes es alto, las pérdidas se concentraron en algunos eventos de alto impacto: los ataques contra el exchange Bybit y el protocolo Cetus, que en conjunto totalizaron 1.780 millones de dólares.

Principales tipos de incidentes

Incluso con la creciente madurez técnica y regulatoria del ecosistema, los ciberdelincuentes han demostrado que siguen un paso por delante en 2025, mejorando los métodos, explotando las lagunas conocidas y diversificando los objetivos. Los incidentes más significativos del año ilustran cómo las vulnerabilidades de diferente naturaleza pueden resultar en pérdidas multimillonarias.

1. Ataques a exchanges y plataformas centralizadas (CEX)

Entre los episodios más emblemáticos se encuentra el ataque a Bybit, que resultó en el robo de aproximadamente 1.500 millones de dólares en Ethereum, el más grande jamás registrado en la historia de las criptomonedas.

En este caso, los atacantes no violaron directamente los servidores del exchange, sino que comprometieron a un proveedor externo de la plataforma, cambiando la dirección de la billetera donde se transfirieron los fondos. ByBit pensó que estaba transfiriendo los fondos a su propia billetera digital, pero lo envió todo a los piratas informáticos. La sofisticación de la operación reveló cómo las cadenas de confianza y las integraciones externas pueden convertirse en puntos de entrada para delincuentes altamente especializados.

Otro caso de alto impacto fue el de Cetus, un exchange descentralizado (DEX), que perdió >al menos USD 250 millones debido a una vulnerabilidad en su sistema de liquidez. La falla permitió a los atacantes manipular transacciones internas y desviar activos, lo que destaca la dificultad de asegurar contratos inteligentes complejos, incluso en plataformas no centralizadas.

2. Exploits en protocolos DeFi

El ataque a Balancer, que causó pérdidas de más de 100 millones de dólares, destacó una de las debilidades recurrentes en el espacio DeFi: errores en el código. Un error en el contrato inteligente permitió retiros no autorizados, exponiendo cómo se pueden explotar pequeñas fallas lógicas para comprometer un protocolo completo. El impacto se extendió a proyectos derivados, como Beets Finance, que también reportó pérdidas millonarias. Estos incidentes refuerzan la importancia de las auditorías continuas e independientes, un desafío para los protocolos que priorizan la innovación y la velocidad de lanzamiento.

3. Estafas de phishing

Si bien las grandes plataformas sufrieron ataques coordinados, los usuarios individuales siguieron siendo los objetivos preferidos. Las estafas de phishing, en las que se engaña a las víctimas para que renuncien voluntariamente a sus credenciales, generaron 410 millones de dólares en pérdidas, según Certik. Se estima que los ataques dirigidos a individuos representaron el 23,35% de todos los fondos robados en el período, una señal de que la ingeniería social sigue siendo tan eficiente como las intrusiones técnicas.

4. Ataques históricos y vulnerabilidades de puentes

Aunque en 2025 no se produjeron incidentes importantes relacionados con puentes, este tipo de ataque sigue siendo uno de los más destructivos. El recuerdo del caso del puente Ronin, en 2022, cuando se robaron 600 millones de dólares, sigue siendo una alerta permanente. Estas fallas muestran cómo la interconectividad entre redes, esencial para la escalabilidad del ecosistema criptográfico, también amplía la superficie de ataque y puede convertir un solo error de código en un colapso sistémico.

La profesionalización de los ataques y el papel de los Estados

Los ataques recientes también revelan el creciente nivel de profesionalización de la ciberdelincuencia relacionada con las criptomonedas. Los grupos patrocinados por el Estado, en particular el Grupo Lazarus, vinculado al gobierno de Corea del Norte, siguen operando de forma muy organizada.

Los ataques a Bybit en 2025 y al puente Ronin en 2022 se atribuyen correctamente a Lazarus, según una auditoría deTRM Labs, que identificó similitudes en el modus operandi de otras invasiones. Funcionarios estadounidenses y aliados dicen que los ataques de Lazarus tienen como objetivo financiar los programas militares y nucleares del régimen norcoreano.

Durante los últimos cinco años, Lazarus ha centrado sus esfuerzos en las empresas de criptomonedas, que se consideran menos protegidas y tienen menos barreras para el lavado de dinero que las instituciones financieras tradicionales. Esta especialización

muestra que, incluso en un mercado cada vez más regulado, las vulnerabilidades operativas siguen siendo el eslabón más débil de la cadena.

Lo que estos ataques revelan sobre el futuro del mercado de criptomonedas

Los acontecimientos de 2025 refuerzan un mensaje que el mercado todavía parece reacio a aceptar: la tecnología por sí sola no garantiza la seguridad. Si bien la industria ha madurado en regulación, transparencia e infraestructura, muchos de los ataques explotaron errores humanos, integraciones mal administradas y código no auditado, puntos que la innovación por sí sola no elimina.

Además, el crecimiento de la inversión institucional y el avance de los productos financieros, como los ETF de Bitcoin y Ethereum, han aumentado la exposición al mercado y han llamado aún más la atención de los grupos criminales y los actores estatales. La paradoja es evidente: cuanto más busca profesionalizarse el ecosistema, más se convierte en un target de alto valor.

La maduración de la ciberseguridad en el sector de las criptomonedas depende menos de las nuevas cadenas de bloques y más de los cambios en la cultura y la gobernanza, las auditorías independientes, la gestión de proveedores y la educación de los usuarios son pilares que aún están evolucionando lentamente.

Al final, las pérdidas récord de 2025 no solo expusieron vulnerabilidades técnicas, sino que cuestionaron el principio mismo de autonomía digital que sustenta el mundo de las criptomonedas.

Para muchos inversores y usuarios, los ataques han reavivado el debate sobre la autocustodia y la protección de activos, lo que ha llevado a un mayor uso de billeteras frías, que se consideran una de las formas más seguras de almacenar criptoactivos fuera del alcance de los ataques directos.

Aun así, incluso la mejor tecnología depende de las buenas prácticas. El fortalecimiento de la seguridad, ya sea institucional, regulatoria o personal, también implica reconocer que, en el universo cripto, la confianza no es un dato técnico, sino una construcción continua.

Fuente: https://www.welivesecurity.com/

LINK DE LA NOTICIA