El exchange de criptomonedas Bybit anunció el viernes que un ataque altamente sofisticado resultó en el robo de más de $1.5 mil millones en activos digitales desde una de sus billeteras frías (desconectadas) de Ethereum, convirtiéndose en el mayor robo de criptomonedas registrado hasta la fecha.

> *«El incidente tuvo lugar cuando nuestra billetera fría multisig de ETH realizó una transferencia hacia nuestra billetera caliente. Desafortunadamente, esta operación fue intervenida mediante un ataque avanzado que alteró la interfaz de firma, mostrando la dirección correcta mientras modificaba la lógica interna del contrato inteligente»,* explicó Bybit en una publicación en X.
>
> *«Como consecuencia, el atacante logró tomar control de la billetera fría de ETH comprometida y desviar los fondos hacia una dirección desconocida».*

En un comunicado adicional en la misma plataforma, el CEO de Bybit, Ben Zhou, aseguró que el resto de las billeteras frías permanecen protegidas. La empresa también informó que ha presentado el caso ante las autoridades competentes.

Aunque Bybit aún no ha emitido una confirmación oficial sobre la identidad del atacante, las firmas de análisis blockchain Elliptic y Arkham Intelligence señalaron que el robo fue llevado a cabo por el notorio Grupo Lazarus. Este suceso marca el mayor asalto a criptomonedas jamás registrado, superando incidentes anteriores como los de Ronin Network ($624 millones), Poly Network ($611 millones) y BNB Bridge ($586 millones).

El analista independiente ZachXBT afirmó haber *«rastreado el hackeo de Bybit en la cadena hasta el ataque a Phemex»,* el cual ocurrió a finales del mes pasado.

El Grupo Lazarus, un colectivo de hackers vinculado a Corea del Norte, es uno de los más activos en este tipo de delitos, perpetrando múltiples robos de criptomonedas para financiar al país, que enfrenta fuertes sanciones. El año pasado, Google describió a Corea del Norte

como *«posiblemente la organización criminal cibernética más grande del mundo».*

Durante 2024, se estima que este grupo ha sustraído aproximadamente $1.34 mil millones en 47 ataques relacionados con criptomonedas, lo que representa el 61% de todos los fondos robados en el ecosistema cripto durante ese período, según datos de la firma de inteligencia blockchain Chainalysis.

> *«El número de robos de criptomonedas sigue en aumento debido a la alta rentabilidad de estos delitos, la dificultad para rastrear a los responsables y la falta de experiencia con tecnologías blockchain y Web3 en muchas compañías»*, señaló el equipo de Mandiant, una empresa de ciberseguridad propiedad de Google, en un informe reciente.

Actualización

En una declaración posterior, Bybit informó que identificó actividad sospechosa en una de sus billeteras frías de Ethereum (ETH) durante un procedimiento rutinario de transferencia el 21 de febrero de 2025, alrededor de las 12:30 p.m. UTC.

> *«La operación formaba parte de un movimiento planificado de ETH desde nuestra billetera fría multisig de ETH hacia nuestra billetera caliente»*, explicó la empresa en su comunicado.
>
> *«Lamentablemente, la transacción fue comprometida mediante un ataque altamente elaborado que modificó la lógica del contrato inteligente y alteró la interfaz de firma, lo que permitió al atacante tomar el control de la billetera fría de ETH. Como resultado, más de 400,000 ETH y stETH, valorados en más de $1.5 mil millones, fueron enviados a una dirección desconocida».*

TRM Labs ha identificado con un alto grado de certeza al Grupo Lazarus como responsable del ataque, basándose en *«coincidencias significativas entre las direcciones utilizadas por los hackers de Bybit y aquellas asociadas con robos previos vinculados a Corea del Norte».*

«El reciente ataque a Bybit representa una evolución en las tácticas empleadas, incorporando métodos avanzados de manipulación de interfaces de usuario. En vez de limitarse a explotar vulnerabilidades en los protocolos, los atacantes recurrieron a sofisticadas técnicas de ingeniería social mediante interfaces alteradas, lo que les permitió comprometer un sistema institucional de firmas múltiples a gran escala», destacó Check Point Research.

La firma de ciberseguridad también señaló que este ataque evidencia cómo los ciberdelincuentes pueden intervenir en transacciones legítimas utilizando la función `execTransaction` del protocolo Gnosis Safe. *«Las billeteras frías multisig no garantizan seguridad si los firmantes pueden ser engañados o infiltrados, lo que resalta el creciente nivel de sofisticación en los ataques dirigidos a la cadena de suministro y la manipulación de interfaces de usuario»,* advirtió.

En un informe detallado publicado durante el fin de semana, Elliptic explicó que el proceso de lavado de activos del Grupo Lazarus sigue un patrón recurrente: convertir los tokens sustraídos en un activo nativo de blockchain, como Ether, con el fin de evitar que los fondos sean congelados.

«Esto fue exactamente lo que sucedió momentos después del robo en Bybit, cuando cientos de millones de dólares en tokens, incluidos stETH y cmETH, fueron convertidos en Ether», señaló la compañía. Además, indicó que los fondos fueron distribuidos en 50 billeteras diferentes en un lapso de dos horas para dificultar su rastreo, antes de ser transferidos a intercambios de criptomonedas como eXch para su conversión en Bitcoin.

> *«El Grupo Lazarus de Corea del Norte es la organización más avanzada y con mayores recursos para el lavado de criptoactivos, mejorando constantemente sus*

> *estrategias para evitar ser detectados y perder el control de los fondos robados»*, afirmó Elliptic.