06/03/2025

Hackers realizan "el mayor robo en la historia de las criptomonedas" al sustraer US$1.500 millones de la empresa global Bybit

La empresa de criptomonedas Bybit ha sido víctima de lo que podría ser el mayor robo en la historia de los criptoactivos, según expertos y medios especializados.

Unos piratas informáticos lograron hacerse con 401.347 Ethereum valoradas en US$1.500 millones, informó Ben Zhou, fundador de la empresa con sede en Dubai (Emiratos Árabes Unidos).

Sin embargo, el directivo de Bybit pidió calma a sus clientes.

"Tengan la seguridad de que todas las demás billeteras frías están seguras", escribió Zhou en X.

"Todos los retiros son NORMALES", agregó, al tiempo que garantizó que la firma reparará a los afectados por el ciberrobo y que, para ello, recurrirá a fondos de la propia la empresa o a un préstamo de los socios.

Bybit tiene US$20.000 millones de dólares en activos.

En declaraciones a Bloomberg, Rob Behnke, cofundador y presidente ejecutivo de la empresa de seguridad blockchain Halborn, aseguró que el incidente probablemente sea del "mayor robo de la historia, no solo en el mercado cripto".

Sobre el golpe

Zhou informó que los piratas informáticos **vulneraron una de las billeteras digitales con Ethereum, la cual es la segunda criptomoneda de mayor valor tras Bitcoin**; y luego transfirieron las más de 400.000 monedas a direcciones no identificadas.

El robo se produjo el viernes 21 de febrero de 2025 durante una transferencia de rutina de Bybit, reportó Forbes.

De acuerdo con la revista especializada en economía, los atacantes emplearon un sofisticado método a través del cual manipularon la transacción enmascarando la interfaz de firma.

Un análisis forense posterior reveló que los piratas utilizaron técnicas avanzadas de "phishing" (suplantación de identidad) e ingeniería social para obtener acceso inicial a las credenciales internas, que luego se utilizaron para eludir los protocolos de seguridad, informó Forbes.

Una vez dentro del sistema, los delincuentes explotaron las vulnerabilidades en el proceso de autenticación de múltiples firmas de Bybit, creando aprobaciones fraudulentas que permitieron la transferencia de activos sin generar señales de alerta inmediatas.

Los fondos robados se transfirieron rápidamente a varias billeteras y se liquidaron a través de distintas plataformas, revelaron medios estadounidenses como CNBC.

Después del robo, el valor de Ethereum cayó alrededor de un 4% el viernes, dejándolo en US$2.641,41 por unidad.

La escala del incidente supera el récord anterior, que ascendió a US$620 millones de Ethereum y USD Coin de la red Ronin en 2022.

Sobre la firma atacada

Bybit se fundó en 2018 y el presidente estadounidense Donald Trump y el exjefe de Paypal, Peter Thiel, figuraban entre sus primeros inversores.

La empresa asegura que tiene más de 60 millones de usuarios en todo el mundo y ofrece acceso a varias criptomonedas.

"Bybit es solvente incluso si no se recupera esta pérdida por piratería, todos los activos de los clientes están respaldados 1 a 1, podemos cubrir la pérdida", aseveró Zhou.

La compañía dijo en una publicación en X que informó a las autoridades del robo y que estaba trabajando "rápida y extensamente" para identificar a los piratas informáticos.

Y aunque las investigaciones apenas se están iniciando, Forbes asegura que hay indicios que sugieren que piratas informáticos patrocinados por Corea del Norte, específicamente el Grupo Lazarus, podrían ser responsables del ataque.

Investigadores de ciberseguridad como ZachXBT han identificado patrones consistentes con operaciones anteriores del Grupo Lazarus, incluidas similitudes con el hackeo de la bolsa Phemex en enero de 2025.

Los llamados a la calma realizados por los directivos de Bybit a sus clientes parecen no haber dado resultados.

La prensa española asegura que en las últimas horas la firma ha experimentado una retirada masiva de fondos y una saturación de los números de soporte que atienden las peticiones de los clientes.

No obstante, por ahora la compañía no tiene previsto limitar las retiradas de fondo por parte de los usuarios y procesará todas las peticiones, reportó el diario económico CincoDías.

Un caso más para la lista

Este robo ha reavivado el debate sobre las criptomonedas, instrumentos que se han vuelto populares entre los inversores, pero que son criticadas por conomistas y otros expertos, que aluden que su valor se basa puramente en la especulación, lo que permite que su valor sea fácilmente manipulado y abre las puertas para estafas.

Desde hace días Argentina vive inmersa en un escándalo político debido el caso de $LIBRA, una criptomoneda que fue promocionada por el presidente de ese país, Javier Milei, y cuyo valor se desplomó horas después de haber sido lanzada, provocado pérdidas millonarias a cientos de personas.

El caso de $LIBRA ha sido presentado como un claro ejemplo de "rug pulling" (algo así como "tirar de la manta" o "tirar de la alfombra" en español), una estafa muy repetida y que consiste en promocionar un activo digital profusamente y así convencer a los inversores de que la compren e inviertan dinero en ella, para que luego sus creadores o promotores retiren su inversión con jugosas ganancias provocando una caída abrupta de su valor.

Antes de iniciar su segundo mandato, el propio Trump lanzó su propia moneda digital, aunque admitió que "no sabe mucho" sobre de ella.

La TRUMP apareció en sus cuentas de redes sociales antes de la vuelta del magnate inmobiliario neoyorquino a la Casa Blanca y rápidamente se convirtió en una de las criptomonedas más valiosas, pero desde entonces ha perdido significativamente valor.

El robo de Bybit también ha puesto de relieve las preocupaciones de seguridad dentro del mercado de divisas digitales, donde se esperaba una confianza renovada después de que Trump lanzara su moneda. Su asesor, el multimillonario de Tesla, Elon Musk, también ha hablado en el pasado sobre Bitcoin.

En 2014, la plataforma de intercambio de criptomonedas Mt Gox se declaró en quiebra después de que se robaran US$350 millones en monedas digitales debido a una falla de su seguridad.

Y antes, en 2019 otros piratas informáticos robaron US$41 millones en Bitcoin de la plataforma de intercambio Binance.

Fuente: https://www.bbc.com/

LINK DE LA NOTICIA