La brecha de seguridad de la extensión para Chrome de Trust Wallet provocó una pérdida de 7 mdd en criptomonedas a través de un código malicioso

Trust Wallet está instando a sus usuarios a actualizar la extensión de Google Chrome a la versión más reciente tras lo que describió como un *"incidente de seguridad"* que provocó la pérdida de aproximadamente 7 millones de dólares.

El problema, según explicó el servicio de billetera de criptomonedas multicadena y no custodial, afecta a la versión 2.68. De acuerdo con la ficha en Chrome Web Store, la extensión cuenta con alrededor de un millón de usuarios. Se recomienda actualizar a la versión 2.69 lo antes posible.

"Hemos confirmado que aproximadamente 7 millones de dólares se han visto afectados y nos aseguraremos de que todos los usuarios impactados reciban un reembolso", señaló Trust Wallet en una publicación en X. *"Apoyar a los usuarios afectados es nuestra máxima prioridad y estamos finalizando activamente el proceso para reembolsarlos"*.

Trust Wallet también exhortó a los usuarios a no interactuar con mensajes que no provengan de sus canales oficiales. Los usuarios exclusivamente móviles y las demás versiones de extensiones para navegadores no se han visto afectadas.

Según la información compartida por SlowMist, la versión 2.68 incorporó código malicioso diseñado para recorrer todas las billeteras almacenadas en la extensión y solicitar la frase mnemónica de cada una de ellas.

"La mnemónica cifrada se descifra posteriormente utilizando la contraseña o la passkeyPassword introducida durante el desbloqueo de la billetera", indicó la firma de seguridad blockchain. *"Una vez descifrada, la frase mnemónica se envía al servidor del atacante api.metrics-trustwallet[.]com"*.

El dominio *"metrics-trustwallet[.]com"* fue registrado el 8 de diciembre de 2025, y la primera solicitud a *"api.metrics-trustwallet[.]com"* comenzó el 21 de diciembre de 2025.

Análisis adicionales revelaron que el atacante utilizó una biblioteca de análisis de cadena completa de código abierto llamada posthog-js para recopilar información de los usuarios de

las billeteras.

Los activos digitales drenados hasta el momento incluyen cerca de 3 millones de dólares en Bitcoin, 431 dólares en Solana y más de 3 millones de dólares en Ethereum. Los fondos robados fueron canalizados a través de intercambios centralizados y puentes entre cadenas para su lavado y conversión. De acuerdo con una actualización compartida por el investigador blockchain ZachXBT, el incidente ha afectado a cientos de víctimas.

"Aunque aproximadamente 2.8 millones de dólares de los fondos robados permanecen en las billeteras del hacker (Bitcoin/EVM/Solana), la mayor parte —más de 4 millones en criptomonedas— ha sido enviada a CEX [intercambios centralizados]: unos 3.3 millones a ChangeNOW, cerca de 340,000 a FixedFloat y alrededor de 447,000 a KuCoin", indicó PeckShield.

"Este incidente de puerta trasera se originó a partir de una modificación maliciosa del código fuente dentro de la base interna de la extensión de Trust Wallet (lógica de analítica), y no por la inyección de una dependencia de terceros comprometida (por ejemplo, un paquete npm malicioso)", explicó SlowMist.

"El atacante manipuló directamente el código propio de la aplicación y luego utilizó la biblioteca legítima de analítica PostHog como canal de exfiltración de datos, redirigiendo el tráfico analítico a un servidor controlado por el atacante".

La compañía indicó que existe la posibilidad de que se trate de la obra de un actor patrocinado por un Estado, y añadió que los atacantes podrían haber tomado control de dispositivos de desarrolladores vinculados a Trust Wallet u obtenido permisos de despliegue antes del 8 de diciembre de 2025.

Changpeng Zhao, cofundador del intercambio de criptomonedas Binance —propietario de la herramienta—, insinuó que la explotación fue *"muy probablemente"* realizada por un insider, aunque no se presentaron pruebas adicionales que respalden esta hipótesis.