Investigadores en ciberseguridad han descubierto más de 40 extensiones maliciosas para el navegador Mozilla Firefox, diseñadas para robar secretos de billeteras de criptomonedas, poniendo en riesgo los activos digitales de los usuarios.

"Estas extensiones se hacen pasar por herramientas legítimas de billeteras de plataformas ampliamente utilizadas como Coinbase, MetaMask, Trust Wallet, Phantom, Exodus, OKX, Keplr, MyMonero, Bitget, Leap, Ethereum Wallet y Filfox", dijo Yuval Ronen, investigador de Koi Security.

Se afirma que esta campaña a gran escala ha estado activa al menos desde abril de 2025, y que se han subido nuevas extensiones a la tienda de complementos de Firefox tan recientemente como la semana pasada.

Se ha descubierto que las extensiones identificadas inflan artificialmente su popularidad, añadiendo cientos de reseñas de cinco estrellas que superan con creces el número real de instalaciones activas. Esta estrategia busca darles una apariencia de legitimidad, haciendo creer que son extensamente utilizadas y engañando a los usuarios para que las instalen.

Otra táctica empleada por el actor de amenazas consiste en hacer pasar estos complementos como herramientas auténticas de billeteras, utilizando los mismos nombres y logotipos.

El hecho de que algunas de las extensiones reales fueran de código abierto permitió a los atacantes clonar su código fuente e inyectar funcionalidades maliciosas para extraer claves de billeteras y frases semilla desde sitios web objetivo y enviarlas a un servidor remoto. También se ha encontrado que estas extensiones maliciosas transmiten las direcciones IP externas de las víctimas.

A diferencia de los fraudes de phishing convencionales, que dependen de sitios web o correos electrónicos falsos, estas extensiones operan dentro del navegador del usuario, lo que las hace mucho más difíciles de detectar o bloquear con herramientas tradicionales de seguridad en el dispositivo.

“Este enfoque de bajo esfuerzo y alto impacto permitió al atacante mantener una experiencia de usuario esperada mientras reducía las probabilidades de detección inmediata”, comentó Ronen.

La presencia de comentarios en ruso dentro del código fuente, así como metadatos obtenidos de un archivo PDF recuperado del servidor de comando y control (C2) utilizado en la operación, apuntan a un grupo de actores de amenazas de habla rusa.

Todos los complementos identificados, excepto MyMonero Wallet, han sido eliminados por Mozilla. El mes pasado, el desarrollador del navegador afirmó haber desarrollado un *“sistema de detección temprana”* para identificar y bloquear extensiones fraudulentas de billeteras cripto antes de que ganen popularidad y sean usadas para robar activos de los usuarios mediante engaños para que ingresen sus credenciales.

Para mitigar los riesgos que suponen estas amenazas, se recomienda instalar extensiones únicamente de editores verificados y revisar su comportamiento para asegurarse de que no cambien de forma silenciosa después de su instalación.

Reformulación con palabras distintas (respetando citas):

Expertos en seguridad informática han revelado la existencia de más de 40 extensiones maliciosas para el navegador Firefox que tienen como objetivo sustraer datos confidenciales de billeteras de criptomonedas, comprometiendo los fondos digitales de los usuarios.

«Estas extensiones simulan ser herramientas oficiales de billeteras reconocidas como Coinbase, MetaMask, Trust Wallet, Phantom, Exodus, OKX, Keplr, MyMonero, Bitget, Leap, Ethereum Wallet y Filfox», afirmó Yuval Ronen, investigador de la firma Koi Security.

Según se reporta, esta operación ha estado activa desde al menos abril de 2025, y continúan apareciendo nuevas versiones en la tienda de complementos de Firefox, incluso tan recientemente como la semana anterior.

Los complementos maliciosos descubiertos recurren a una técnica para aparentar ser populares, acumulando cientos de calificaciones con cinco estrellas, muchas más que las instalaciones reales. Con esto buscan generar una percepción falsa de fiabilidad, logrando que usuarios desprevenidos los instalen.

Otro método utilizado por los atacantes consiste en replicar los nombres e íconos de las billeteras legítimas para dar una apariencia auténtica a las extensiones.

Debido a que algunos de estos complementos originales son de código abierto, los atacantes pudieron copiar su base de código e introducir funciones dañinas que capturan frases semilla y claves privadas desde los sitios web que visita la víctima, enviándolas posteriormente a un servidor externo. Además, se ha comprobado que las extensiones maliciosas recolectan también la dirección IP pública del usuario afectado.

A diferencia de los ataques de phishing tradicionales que dependen de enlaces o correos falsos, estas extensiones operan desde dentro del propio navegador del usuario, lo que las vuelve más difíciles de identificar o neutralizar con soluciones comunes de protección.

“Este método de bajo costo y gran efectividad permitió al atacante ofrecer una experiencia normal al usuario mientras evitaba ser detectado rápidamente”, indicó Ronen.

El hallazgo de anotaciones en idioma ruso dentro del código y los metadatos extraídos de un archivo PDF localizado en el servidor C2 utilizado en la operación sugieren que se trata de un grupo de ciberdelincuentes de habla rusa.

Excepto por MyMonero Wallet, todos los complementos maliciosos han sido retirados por Mozilla. El mes pasado, la empresa anunció que ha implementado un *“sistema de detección anticipada”* capaz de reconocer y frenar extensiones de billeteras fraudulentas antes de que se popularicen y consigan engañar a los usuarios para que entreguen sus credenciales.

Para reducir la exposición ante estas amenazas, se aconseja descargar extensiones únicamente desde desarrolladores confiables y comprobar que su comportamiento no se

altere tras la instalación.