



## 16 Extensiones maliciosas para Firefox se hacen pasar por las billeteras Rabby y OKX para robar frases de recuperación

Los investigadores de ciberseguridad han identificado un conjunto de 16 extensiones maliciosas para Mozilla Firefox capaces de robar frases de recuperación (seed phrases) y claves privadas de billeteras de criptomonedas.

*«Las extensiones se hacen pasar por portales de billeteras, utilidades de escritorio y herramientas para navegadores. Sin embargo, su código intercepta las frases de recuperación y las claves privadas durante el proceso de importación de billeteras, e intenta transmitir estos datos confidenciales a servicios Cloudflare Workers controlados por los atacantes», [afirmó](#) el investigador de Socket, Joseph Edwards, en un análisis.*

Los nombres de las extensiones son los siguientes:

1. view-focus-bright@webtools.co@6.12.2
2. quick-track-nest@tabtools.co@8.1.18
3. vibe-kit-tool@fasttools.co@9.21.9
4. edge-hub-snap@protools.net@4.12.24
5. core-hub-peak@neattools.example@8.24.21
6. sipoo-grozza@browserweb.com@2.1
7. mozart-seo@webtools.com@1.4
8. clean-file-bar@neattools.com@4.21.8
9. clean-net-timer@plugify.example@4.17.1
10. manager-square@webtools.com@1.4
11. manager-course@webtools.com@1.4
12. val-andrew@browserweb.com@1.4
13. manager-team@browserweb.com@1.4
14. valory-andrew@browserweb.com@1.4
15. franklin-uk@browserweb.com@1.4
16. franklin-uro@browserweb.com@1.4

Cuatro de estas extensiones corresponden a copias fraudulentas de Rabby Wallet, mientras que las demás imitan específicamente a OKX Wallet. Con excepción de una de ellas, todas fueron observadas comunicándose con el dominio «\*.icy-star-f45c.workers[.]dev». El



## 16 Extensiones maliciosas para Firefox se hacen pasar por las billeteras Rabby y OKX para robar frases de recuperación

propósito final de esta operación es recopilar frases mnemónicas y claves privadas para posteriormente enviarlas a una infraestructura basada en Cloudflare Workers controlada por los atacantes.

Los expertos consideran que esta campaña es una continuación de una «oleada previa» documentada por la empresa de seguridad de aplicaciones en agosto de 2026. Los hallazgos indican que los actores de la amenaza modifican continuamente nombres de paquetes, versiones, identificadores de extensiones, descripciones y elementos visuales, mientras reutilizan las mismas interfaces de billeteras, la lógica de manejo de credenciales y la infraestructura de red.

Al 5 de octubre de 2026, todas estas extensiones habían sido eliminadas de la plataforma. Los usuarios que instalaron cualquiera de ellas y proporcionaron una frase de recuperación o una clave privada auténtica deben asumir que sus activos están comprometidos, crear una nueva billetera desde un sistema limpio y transferir inmediatamente sus fondos.

Estos descubrimientos coinciden con la detección reciente de otras extensiones sospechosas o maliciosas para Firefox, Google Chrome y Microsoft Edge:

1. Una extensión de Firefox denominada «[ID-Pay](#)» ([pdf-para-texto@extensao.local](mailto:pdf-para-texto@extensao.local)), presentada como una herramienta de verificación de identidad para abrir documentos PDF protegidos. En realidad, incorporaba funciones para descargar código malicioso desde infraestructura remota controlada por atacantes e inyectar JavaScript en el dominio legítimo «[accounts.google\[.\]com](https://accounts.google.com)» con el objetivo de robar cookies de sesión.
2. Un [conjunto de 32 extensiones maliciosas](#) distribuidas a través de Chrome Web Store y Microsoft Edge Add-ons Store, que aparentaban ser herramientas de productividad inofensivas. No obstante, recopilaban información de los usuarios, supervisaban sus hábitos de navegación y reemplazaban discretamente la pestaña activa por direcciones URL definidas en configuraciones remotas. Esta campaña se encuentra activa desde marzo de 2025 y ha sido atribuida a un actor de amenazas de habla coreana.
3. Un [grupo de aproximadamente 30 extensiones maliciosas](#) que simulaban ser



## 16 Extensiones maliciosas para Firefox se hacen pasar por las billeteras Rabby y OKX para robar frases de recuperación

herramientas de productividad, utilidades de privacidad y servicios relacionados con criptomonedas. Estas extensiones utilizaban la identidad de figuras reconocidas del sector financiero para redirigir a las víctimas hacia páginas fraudulentas de billeteras de criptomonedas diseñadas para robar frases de recuperación, evitando al mismo tiempo a usuarios angloparlantes y entornos de análisis.

4. Un [conjunto de 31 extensiones de Chrome](#) en idioma ruso promocionadas como VPN para acceder a servicios restringidos en ese país, tales como Anthropic Claude, Facebook, Google Gemini, LinkedIn, Netflix, Notion, OpenAI ChatGPT, Spotify, Telegram, Threads, Wikipedia, X y YouTube. Sin embargo, tras su instalación, el tráfico del navegador era redirigido mediante servidores proxy obtenidos desde páginas de GitHub Pages, así como desde Blogger, Google Docs y Telegram como mecanismos alternativos.
5. Una extensión de Chrome Web Store llamada [Stylish](#), capaz de [interceptar](#) conversaciones mantenidas con ChatGPT, Gemini, Claude, Perplexity, Character.AI y GitHub Copilot, reenviando el contenido completo de las respuestas a sus operadores.
6. Una extensión denominada Urban VPN, que incorporaba una supuesta función de «*protección antiphishing*» destinada a advertir sobre sitios maliciosos. Sin embargo, nunca generaba alertas de phishing y transmitía silenciosamente las URL visitadas a servidores administrados por BIScience. La extensión ya había sido objeto de acusaciones relacionadas con la captura de conversaciones mantenidas con chatbots de IA. Posteriormente, sus desarrolladores aclararon que el procesamiento vinculado a IA solo se activaba cuando la función «*AI Protection*» era habilitada expresamente por el usuario. Además, meses antes corrigieron una vulnerabilidad crítica que permitía a cualquier sitio web enviar comandos arbitrarios a la extensión sin verificar el origen de la solicitud.
7. Una extensión de Chrome Web Store denominada «Pop up blocker for Chrome™ – Poper Blocker», promocionada como bloqueador de anuncios. Sin embargo, integraba un intérprete que descargaba e interpretaba instrucciones procedentes de un servidor de comando y control (C2), eludiendo las restricciones de Manifest V3 de Google. Gracias a este mecanismo, podía recopilar huellas digitales del navegador, historial de navegación, información de perfiles en redes sociales e interacciones con asistentes de inteligencia artificial.



## 16 Extensiones maliciosas para Firefox se hacen pasar por las billeteras Rabby y OKX para robar frases de recuperación

Para reducir los riesgos asociados a extensiones maliciosas, se recomienda revisar periódicamente las extensiones instaladas en el navegador y eliminar aquellas que ya no sean necesarias. Asimismo, las organizaciones deberían realizar auditorías de extensiones en entornos administrados, implementar mecanismos de monitoreo en tiempo de ejecución y desplegar soluciones de supervisión basadas en comportamiento para detectar actividades sospechosas de manera más efectiva.