Un atacante técnicamente sofisticado conocido como SeaFlower, ha estado apuntando a los usuarios de Android e iOS, como parte de una extensa campaña que imita los sitios web oficiales de billeteras de criptomonedas con la intención de distribuir aplicaciones de puerta trasera que agotan los fondos de las víctimas.

Según los reportes, se descubrió por primera vez en marzo de 2022, el grupo de actividad *«indicia una relación sólida con una entidad de habla china aún por descubrir»*, según los nombres de usuario de macOS, los comentarios del código fuente en el código de la puerta trasera y su abuso de la red de entrega de contenido (CDN) de Alibaba.

> *«A partir de hoy, el principal objetivo actual de SeaFlower es modificar las billeteras Web3 con un código de backdoor que finalmente filtra la frase inicial»,* dijo Taha Karim de Confiant.

Las aplicaciones dirigidas incluyen versiones de Android e iOS de Coinbase Wallet, MetaMask, TokenPocket e imToken.

El modus operandi de SeaFlower implica la creación de sitios web clonados que actúan como un conducto para descargar versiones troyanizadas de las aplicaciones de billetera que prácticamente no han cambiado con respecto a sus contrapartes originales, excepto por la adición de un nuevo código diseñado para filtrar la frase inicial a un dominio remoto.

La actividad maliciosa también está diseñada para dirigirse a los usuarios de iOS por medio de perfiles de aprovisionamiento que permiten que las aplicaciones se transfieran a los dispositivos.

En cuanto a cómo los usuarios se topan con estos sitios web que ofrecen billeteras fraudulentas, el ataque aprovecha las técnicas de envenenamiento de SEO en los motores de búsqueda chinos como Baidu y Sogou, para que las búsquedas de términos como *«descargar MetaMask iOS»* estén manipuladas para mostrar las páginas de descarga oculta en la parte superior de la página de resultados de búsqueda.

En todo caso, la divulgación destaca una vez más cómo los actores de amenazas están poniendo cada vez más su mirada en las populares plataformas Web3 en un intento de saquear datos confidenciales y transferir engañosamente fondos virtuales.