Una billetera Ethereum conocida como «Shitcoin Wallet», está inyectando código JavaScript malicioso desde las ventanas abiertas del navegador Chrome para robar datos de los usuarios. El 30 de diciembre, el experto en seguridad cibernética y anti-phishing, Harry Denley, advirtió sobre la posible violación en Twitter.

Según Denley, el software de billetera criptográfica para el navegador web Chrome, Shitcoin Wallet, está dirigio a Binance, MyEtherWallet y otros sitios web conocidos que contienen contraseñas de los usuarios y claves privadas.

La extensión Shitcoin Wallet para Chrome, con ExtensionID: ckkgmcceffnbbalkmbbgebbojjogffn funciona descargando una cantidad de archivos JavaScript de un servidor remoto. Luego, el código busca ventanas de navegador abiertas que contengan páginas web de intercambios y herramientas de la red Ethereum.

El código intenta raspar la entrada de datos en esas ventanas. Una vez que lo logra, la información se envía a un servidor remoto identificado como *«erc20wallet.tk»,* que es una dirección de dominio de nivel superior que pertenece a Tokelau, un grupo de islas del Pacífico Sur que forman parte del territorio de Nueva Zelanda.

El incidente con Shitcoin Wallet es similar a otras amenazas, como cuando Apple amenazó con anular la lista del navegador móvil DApp de Coinbase de su tienda de aplicaciones y Google al eliminar la aplicación de billetera Ethereum MetaMask de Google Play Store la semana pasada. Sin embargo, ambos casos fueron objeto de controversias debido a la falta de evidencia de conducta maliciosa por parte de las aplicaciones.

En 2018, se encontraron varias extensiones de cryptojacking en la tienda web de Google Chrome. Según un informe reciente de McAfee Labs, el cryptojacking, que ocurre cuando el dispositivo informático de un usuario se utiliza en secreto para extraer criptomonedas, aumentó un 29 por ciento en el primer trimestre de 2019.

El nombre de la billetera ya es un indicio de una aplicación poco confiable, pero además, Shitcoin Wallet contiene algunas características adicionales que levantan sospechas.

Según una publicación de blog de la compañía, la billetera Ethereum, que se lanzó el 9 de diciembre y asegura tener más de 2 mil usuarios, es una billetera basada en la web que tiene varias extensiones para distintos navegadores.

> *«Es una billetera web que tiene varias extensiones para diferentes navegadores, que analizaré más adelante en el artículo»,* dice la compañía.

Sin embargo, esto tiene algunas discrepancias con lo que la compañía menciona al final de la misma publicación, que dice que Shitcoin Wallet actualmente solo es compatible con Chrome.

Unos días antes del ataque malicioso de JavaScript, Shitcoin Wallet anunció el lanzamiento de su nuevo aplicación de escritorio, regalando 0.05 ETH a los usuarios que descargan e instalan la aplicación de escritorio Shitcoin Wallet.

Aunque esos usuarios pudieron haber recibido algo de Ethereum gratis, ahora son vulnerables a que se eliminen sus datos y se comprometa su información personal.