WizardofAus, usuario de Twitter y arquitecto de software, advirtió a los titulares de criptomonedas sobre una extensión para Chrome de billeteras de criptomonedas Ledger que supuestamente tiene malware.

> *«Alerta de extensión de Chrome de malware. Si tiene instalado «Ledger Secure», quítelo. El @ChromeExtension 'LedgerSecure' contiene malware que pasa a su espalda la frase seed al autor de la extensión. Este no es un * producto @Ledger. Utilizado con éxito contra @hackedzec»*, escribió en Twitter.

Al parecer, el identificador @hackedzec se creó únicamente para difundir el conocimiento luego de la experiencia con el malware, pues la cuneta se creó hace unos días.

Mientras tanto, la cuenta oficial de Twitter de Ledger Support, confirmó la detección de la extensión de malware este 2 de enero, con el encabezado *«PHISHING ALERT»*.

WizardofAus sufrió el robo de 600 Zcash, con un valor aproximado de 16 mi dólares, que fueron robados de su Ledger Nano por el creador de la extensión para Chrome.

Refiriéndose a las advertencias del fundador de Casa, Jeremy Welch, el año pasado contra el malware de extensión del navegador en el evento de Bitcoin, Baltic HoneyBadger, en Riga, WizardofAus describió los riesgos que representan estos productos y lo que los usuarios pueden hacer para protegerse de los ataques.

> *«En primer lugar, tenga mucho cuidado con las extensiones que instala. Si usa la misma computadora para su criptografía que usa generalmente, sea muy diligente. Es mejor tener una máquina mínima separada, o usar una máquina virtual que es el único lugar donde se realiza la actividad criptográfica»,* dijo.

Otra diligencia incluye el uso solo del software patentado del proveedor de billetera, Ledger

en este caso, y la doble verificación de que realmente proviene del sitio web del proveedor por medio de un enlace seguro.

Los usuarios también pueden verificar la suma de verificación del archivo descargado antes de ejecutar el software. Una suma de comprobación, también conocida como hash, es un número hexadecimal que es exclusivo del archivo .exe del instalador creado por el autor. El archivo descargado, suponiendo que no haya sido manipulado por un tercero, debe coincidir con la suma de verificación en el sitio del proveedor.

Hace unos días, Masterhacks informó sobre una extensión para Chrome de la billetera Ethereum conocida como *«Shitcoin Wallet»*, que según los informes, inyecta código JavaScript malicioso desde las ventanas abiertas del navegador para robar datos de sus usuarios.