



[Electrum](#) anunció ayer que un sitio de Internet se está haciendo pasar por la página oficial de la compañía para defraudar a los usuarios y robar su dinero, esto por medio de una infección con malware en el código fuente de las descargas de la cartera Electrum para computadoras.

En [Twitter](#), Electrum anunció lo sucedido y afirmó que ha investigado a profundidad la proliferación de sitios web que se hacen pasar por el sitio oficial de la compañía, con lo que ha descubierto un esquema de fraude que con dominios similares al de Electrum (electrum.org), inyecta por medio de las descargas un malware en la computadora que extrae las palabras iniciales y claves privadas del monedero Bitcoin para enviarlas a un servidor remoto.

«Recientemente, un sitio web alojado en 'electrum dot com' ha intentado defraudar a los usuarios de Electrum, por medio de la distribución de binarios de Electrum falsos que extraen las palabras iniciales y claves privadas del usuario para enviarlas a un servidor remoto», escribió Electrum.

Electrum.com es el sitio con mayor proliferación del intento de estafa, ya que el dominio atrae demasiadas visitas por su ubicación en la red.

Electrum informó en [GitHub](#) que los estafadores habrían afirmado que se trata de una bifurcación del proyecto Electrum en pleno desarrollo, siendo un fork que supuestamente trata de mejorar la experiencia de los servicios financieros del usuario.

«El esquema 'electrum dot com' está llevando el ataque mucho más lejos: los estafadores lograron tomar el control del dominio punto com y desarrollaron un sitio web con un diseño y logotipo ligeramente diferente. Los autores afirmaron que están desarrollando una bifurcación legítima del proyecto Electrum y están tratando de mejorar la experiencia del usuario», añadió Electrum.



Electrum alerta sobre caso de fraude por medio de portales falsos

Los especialistas de Electrum decidieron investigar el asunto y descubrieron que la página web ofertaba la descarga de códigos fuentes falsos para monederos para PC, cuya constitución fue alterada de tal forma que permitiera el robo de [criptomonedas](#).

Los archivos de descarga de la billetera para Windows y Mac se encuentran modificados con el malware del sitio web, lo que será comprobado por medio de una copia de seguridad.

Electrum afirmó que lanzará paquetes oficiales por medio de la tienda MacOS para que los usuarios puedan identificar la autenticidad de los productos originales. Además, está desarrollando las firmas GPC para verificar si los monederos son en realidad originales.