El principal proveedor de software antivirus ESET, descubrió un navegador Tor falso con un troyano integrado, diseñado para robar Bitcoin de los compradores en la Deep Web.

Dirigido principalmente a usuarios en Rusia, el falso navegador Tor se distribuyó por medio de dos sitios web y ha estado robando criptomonedas de los compradores de la Web Profunda, intercambiando las direcciones de billeteras originales desde 2017, según informó la división editorial de ESET WeLiveSecurity este 18 de octubre.

Creados en 2014, los dos sitios web falsos de Tor (tor-browser punto org y torproect punto org), están imitando el sitio web real del navegador anónimo Torproject.org.

Según la firma de seguridad, estos sitios web muestran un mensaje de que los usuarios tienen una versión desactualizada del navegador Tor, aún teniendo la última versión del legítimo navegador, con el fin de que los usuarios descarguen la versión falsa con malware.

ESET asegura que el malware, recién descubierto, se distribuyó para Windows, aunque no existe evidencia de que los mismos sitios web hayan distribuido versiones para Linux, MacOS o móviles.

Después de la instalación, el navegador malicioso intercambia automáticamente las direcciones de cifrado de los usuarios por las direcciones controladas por los piratas informáticos.

Según ESET, la cantidad total de fondos recibidos para las tres billeteras que están involucradas en la campaña, representó 4.8 Bitcoin hasta ahora. Una de las billeteras reportadas cuenta con 2.66 BTC en este momento, con una última transacción fechada en septiembre de 2019.

Además de esto, la campaña maliciosa ha estado robando dinero alterando las billeteras QIWI.

A inicios de octubre, ESET advirtió sobre otra forma de malware que roba criptomonedas a

los usuarios, un troyano bancario llamado Casbaneiro o Metamorfo, que apunta a bancos y servicios de cifrado ubicados en Brasil y México.

Los usuarios de Tor ya han sido advertidos sobre posibles pérdidas de dinero debido a violaciones de seguridad. A mediados de septiembre, la plataforma LocalBitcoins advirtió a los usuarios de Tor acerca de los riesgos que conlleva el uso de dicho navegador, alegando que Tor Browser expone a muchos riesgos de robo de criptografía.