Grupo 5

Descubren Navegador Tor troyanizado utilizado para robar bitcoins en la darknet

¿Qué tipo de amenaza es? Es un troyano

¿Cómo comienza y cómo se propaga esta amenaza? Comienza en dos páginas web que afirman distribuir la versión oficial del navegador Tor en ruso. Cuando se hace click en actualizar el navegador Tor te redirige al segundo sitio web y se descarga el troyano.

¿Hay más de una amenaza aplicada?
Por un lado la versión troyanizada de Tor que no permite actualizar el navegador a una versión oficial. Por otro lado modifican el complemento HTTPS Everywhere para que ejecute un script de Java que redireccionaba el dinero de las billeteras virtuales a la cuenta de los delincuentes en la plataforma QIWI y otras billeteras de bitcoin de la darknet. También deshabilitaron la comprobación de firma digital para los complementos en Tor.

¿Qué solución o medida recomendarían?
Desinstalar la versión troyanizada y descargar la versión oficial. Como medida preventiva descargar siempre de fuentes oficiales.