La amenaza es un troyano.

A través de mensajes de Spam en diferentes foros rusos, los ciberdelicuentes comenzaron a hacer llegar diferentes enlaces de sitios web para la descarga de un archivo para actualizar un navegador (Tor en este caso) y de esta manera con esta versión “troyanizada” del mismo, el cual es totalmente funcional, comienzan a adueñarse de datos y a cambiar direcciones de billeteras virtuales por otras adulteradas, y de esa manera hacerse de estas transacciones.

No se modifico el código fuente del navegador, sino que se modificaron algunas de las configuraciones predeterminadas del navegador y de algunas de las extensiones.

La solución preventiva sería educar a los usuarios para distinguir los sitios reales de este tipo de sitios los cuales pueden ser similares tanto en apariencia como en nombre de dominio, pero no lo son.