

## Mesa 5

Nota :

<https://www.welivesecurity.com/la-es/2019/10/22/navegador-tor-trojanizado-robar-bitcoins-darknet/>

¿Qué tipo de amenaza es?

Troyano

¿Cómo comienza y cómo se propaga esta amenaza?

Al hacer clic en el botón “Actualizar el Navegador Tor”, el visitante es redirigido a un segundo sitio web con la posibilidad de descargar un instalador de Windows.

Se propaga utilizando dos sitios web que afirman distribuir la versión oficial del navegador Tor en ruso.

## Mesa 5

¿Hay más de una amenaza aplicada ?

Hay más de una amenaza debido a que el troyano lleva implícito un navegador Tor controlado por delincuentes (Spyware).

¿Qué solución o medida recomendarían ?

**Paso 1:** Descarga e instala un antivirus actualizado. **Paso 2:** Desconectarse de internet.

## Mesa 5

**Paso 3:** Borrar caché y cookies. **Paso 4:** Reinicia la computadora en "Modo a prueba de fallos" **Paso 5:** deshabilites la Restauración de Sistema o el "System Restore". Algunas veces los virus pueden esconder archivos en la Restauración de Sistema . **Paso 6:** haz un escaneo completo de la computadora. **Paso 7:** Si ves que el antivirus tiene problemas para remover un virus tienes que ejecutar MSCONFIG. **Paso 8:** Luego de que todos los virus hayan sido puestos en cuarentena o removidos reinicia la PC, conéctate a internet y ejecuta Windows Update para descargar aquellas actualizaciones que sean recomendadas para tu equipo. **Paso 9:** Windows, en su página oficial recomienda que utilicemos una herramienta anti-spyware para proceder a la búsqueda y eliminación del programa espía.