Introducción a la Informática

Equipo Nro.: 5

Fuente:

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

• ¿Qué tipo de amenaza es?

Troyano

• ¿Cómo comienza y cómo se propaga esta amenaza?

Se ha estado propagando utilizando dos sitios web que afirman distribuir la versión oficial del navegador Tor en ruso. El primero de los sitios muestra al visitante un mensaje en ruso que dice que tiene un Navegador Tor obsoleto. El mensaje se muestra incluso si el visitante tiene la versión más actualizada del Navegador Tor. 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

• ¿Hay más de una amenaza aplicada?

Creemos que no. Solamente lo utilizaron para robar dinero digital de las billeteras de bitcoin de usuarios que entraban a realizar compras a la darkweb.

•¿Qué solución o medida recomendarían?

Para el caso de que tengan la versión troyanizada del software, con actualizarlo a la versión más reciente sería suficiente. Los atacantes solo modificaron partes no esenciales del software basados en la versión 7.5.