Grupo 5

integrantes:
Yohana Zapata Bedoya
karol Hernandez
Juan Pablo Cediel Alfonso
Johaymen Alvarez
Felipe Arregui

Actividad Deberán leer cada una de las noticias asignadas y responder en un documento de Google Presentations para todas las mesas, las siguientes consignas:

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?
El sitio decía que distribuía una versión oficial de Tor pero era una versión modificada, cuando el usuario lo abre pide actualizar y descarga un instalador adicional. Esta versión tiene deshabilitada una comprobación de firma digital para los complementos instalados para el Navegador Tor. Por lo tanto, los atacantes pueden modificar cualquier complemento y el navegador lo cargará sin alertar acerca del fallo en la verificación de firma digital.

● ¿Hay más de una amenaza aplicada?
Desde nuestro punto de vista no, solo es un troyano donde aplicaron varias técnicas como Execution, Persistence, Collection, Command and Control, Impact.

● ¿Qué solución o medida recomendarían? Una vez resueltas, volveremos a la sala principal en la cual el grupo debe compartir sus respuestas a los demás compañeros y compañeras, exponiendo la problemática y el análisis que realizaron.
Cuando se quiera descargar el navegador Tor en este caso, o para otros, siempre se debe verificar que el sitio sea el oficial, con esto evitamos que los ciberdelincuentes ataquen nuestros equipos, de igual manera contar con un buen antivirus para proteger nuestro equipo y datos.