Respuestas clase 2

Rodrigo Castillo junto a David Martinez

11 de agosto de 2020

1. Primera razón

La primera razon por la cuál alguien querría analizar un malware es para buscar a sus creadores, pues muchos ataques informáticos son catastróficos para las empresas y por esta razón es bueno buscar a sus culpables

2. Segunda razón

Para dimensionar el daño potencial que pueda tener un archivo malicioso en un computador : Muchas veces nosotros descargamos contenido del cuál no sabemos su procedencia, por lo tanto, es bueno poder analizar que acciones está teniendo este contenido en nuestros dispositivos y de esta manera poder hacer un balance para saber si este contenido nos beneficia o nos perjudica.

3. Tercera Razon

Para entender el Malware, entender el malware puede prevenirnos de futuros ataques informáticos en muchas ocaciones, nos puede enseñar como prevenirlo y en un ambiente de seguridad ofensiva , como ejecutarlo.

Además de todo lo anterior, entender el malware puede ser facinante y puede contribuir con otras diciplinas de la informática, con esto, construir herramientas que nos puedan beneifciar en un futuro.

4. Diferencia entre Host based signatures y Antivirus signatures

Host based signatures detectan cambios inesperados en el codigo malicioso y cambios en las firmas de antivirus, se enfocan en las acciones que el malware de hacen al sistema.

Los antivirus lo que hacen es comparar el malware con el malware conocido con el malware que quiere verificar. de esta manera, reconoce el malware, sin embargo, el malware puede presentarse en diferentes codificaciones, por lo que mediante algoritmos de codificación es posible bypassear un antivirus.