Análisis de Malware

Comprensión y Análisis de Código Malicioso

Uso de herramientas, búsqueda en logs, funcionalidad y propósito del malware.

SECCION 1
Conceptos y Definiciones

Clase 3

Análisis dinámico, estático y online.

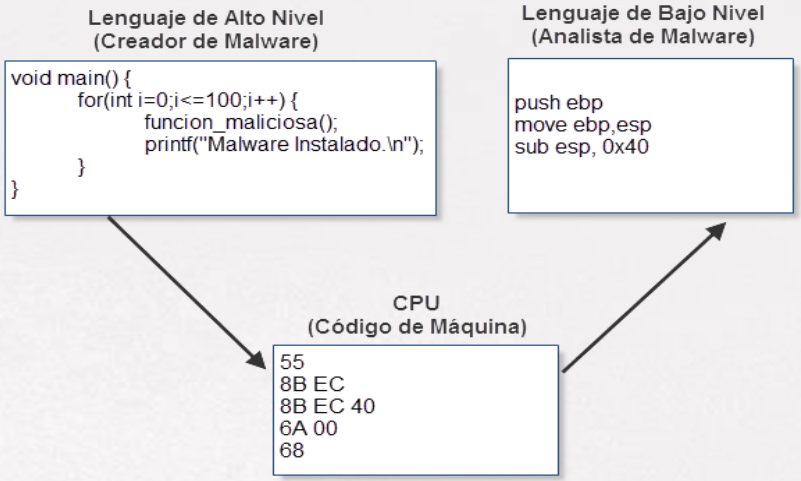
.

- El análisis estático de códigos maliciosos hace referencia **al estudio de una amenaza sin tener que ejecutarla.** Un primer acercamiento nos va a permitir conocer si el malware está empaquetado, en qué lenguaje de alto nivel fue desarrollado y otras tantas características más; Por ejemplo, podríamos ver qué librerías importa, las funciones que va a utilizar, el tamaño de sus secciones y otros datos de importancia.

- **Desensamblado (OllyDbg, IDA Pro)**

Esta técnica básica de análisis estático, nos permiten conocer desde afuera, información acerca del código malicioso.

Aprender a desensamblar códigos maliciosos a través del uso de técnicas de Ingeniería Inversa es una habilidad que lleva tiempo desarrollar y puede resultar complicada.

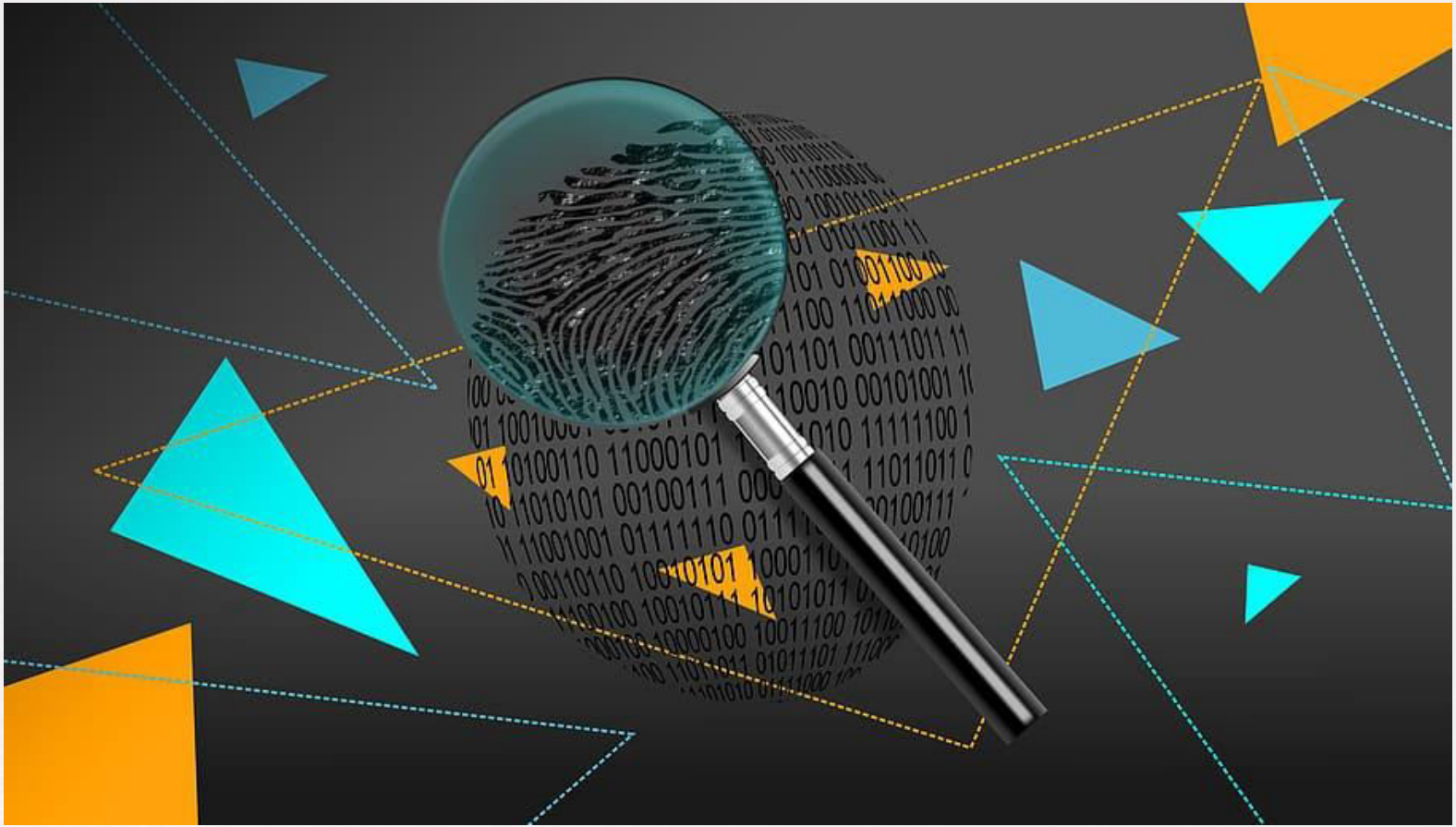


HERRAMIENTAS PARA ANÁLISIS ONLINE DE MALWARE

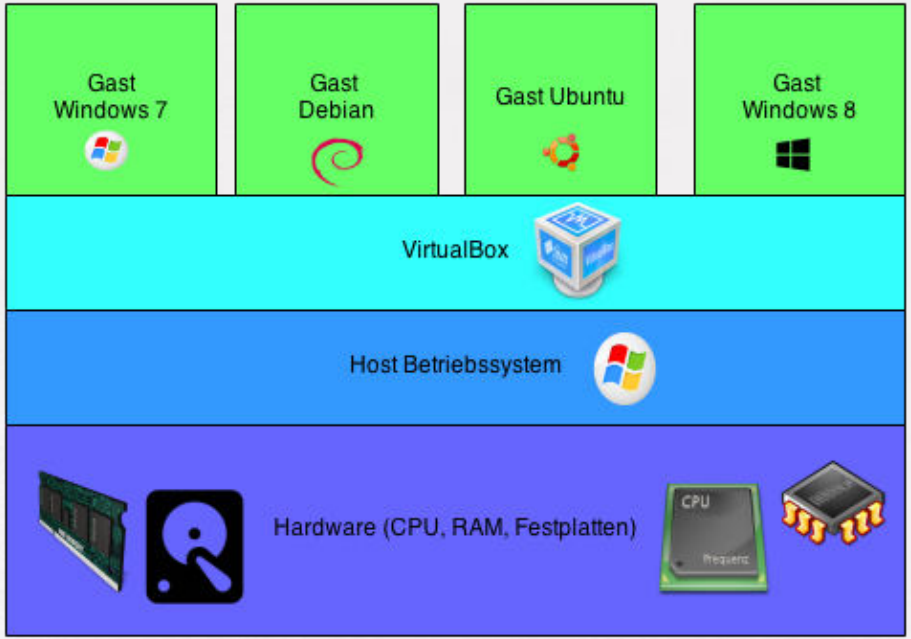
El análisis de malware en línea nos entrega mayores detalles como por ejemplo: el nombre por el cual es conocido comúnmente el malware, el país de origen del mismo, las librerías que usa, clasificación y otros. Algunas de estas herramientas:

- https://www.virustotal.com/
- https://sandbox.anlyz.io/
- https://fortiguard.com/
- https://virusdesk.kaspersky.com/

En todas ellas es requerido que subamos el archivo sospechoso, luego de eso usualmente se corre un breve análisis para indicarnos si existe ya un reporte sobre ese mismo archivo en cuyo caso se nos entrega un reporte inmediatamente. Cuando el archivo en cuestión no ha sido analizado previamente, o bien se nos pide esperar en línea mientras se conduce el análisis, o nos solicita un correo para contactarnos posteriormente.



El análisis DINAMICO; Es mas sencillo, basta con observar ayudado de herramientas evidentemente, cual es la ejecución del malware directamente en el sistema, mientras es registrada toda su actividad en una maquina virtual o sandbox.




CRACKS
DATA VIRUS
MALICIOUS SOFTWARE
THEFT
SOCIAL MEDIA ATTACKS
CYBERWARFARE
VIRUS
SOFTWARE FAILURE
NETWORK SNIFFING
YOUR DATA SAFETY
SPYWARE
HUMAN ERROR
SOFTWARE ERROR
STOLEN INFORMATION
TROJAN
CYBER ATTACKS
PASSWORD CRACKING
HACKING
FRAUD
CYBERCRIMINALS
TROJAN
ADWARE
SYSTEM PENETRATION
CYBERSTALKING

¡Nos vemos en la siguiente Clase!