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 1

Malware: Definición, Características y tipos.


MALWARE

0-9

- **Decimal**

Sistema de base 10 (0123456789)

0-1

- **Binario**

Sistema de base 2

16 ABCDEF

- **Hexadecimal**

Sistema de numeración de base 16 (0123456789ABCDEF)

ASCII

- **ASCII**

Código de caracteres basado en el alfabeto latino (Teclado)

Ensamblador

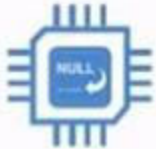
lenguaje de programación de más bajo nivel. Es el usado para programar los microprocesadores

Debugger

o depurador, aplicación para depurar los errores de programación

Bypasear

Alternativa para evitar un bloqueo



NOP

Operación nula escrita en ensamblador. Cuando llega a esta operación, continúa hasta la siguiente operación válida.

NOP

Técnicas para bypasear un sistema de seguridad

- **Bindear**

  Metodología usada para unir un ejecutable con otro archivo, resultando otro ejecutable.

- **Joiner**

  Metodología usada para unir un ejecutable con otro archivo, resultando otro ejecutable.

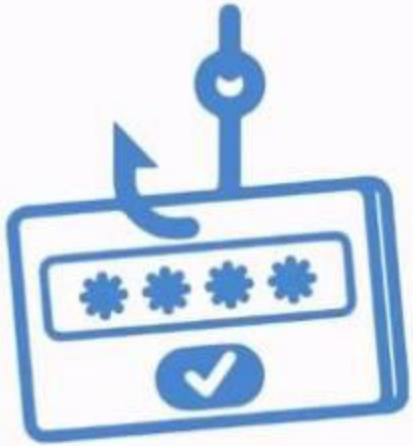
- **Builder**

  Entorno gráfico para cifrar archivos.

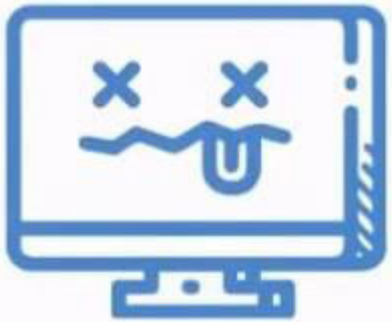
●Tipo de Malware

- **Adware**
  Genera publicidad.
- **Clickers**
  Encargado de generar tráfico hacia la publicidad y pulsar sobre esta.
- **Ransomware / locker**
  Restringe el acceso al sistema o parte de él mediante claves criptográficas

- **Troyano**
  Virus que debe ser ejecutado por la víctima
- **Malware**
  Crea un daño específico para el usuario
- **Keylogger**
  Troyano que roba la información, normalmente mediante keyloggers



- **Spyware**
  Aplicación con el objetivo de extraer información.
- **Gusano**
  Malware con objetivo de extenderse por la red
- **Phishing**
  Recolectan datos principalmente bancarios



- **RAT**

  Herramientas de administración remotas, normalmente con disposición de Backdoors.

- **Rootkits**

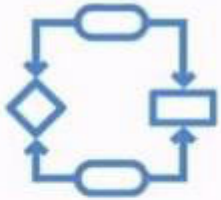
  Conjunto de aplicaciones ocultas para el equipo, con el objetivo de disponer de un acceso externo para futuras acciones.

●Cualidades del Malware

- **Persistencia**
  Capacidad para mantenerse en el sistema.
- **Ofuscación**
  técnica de modificación del código fuente de una aplicación para evitar ingeniería inversa.
- **Backdoor**
  Puerta trasera. Sistema encargado de evadir las medidas de seguridad, dando acceso fácil a otro dispositivo.
- **FUD**
  Full undetectable

Firma

Código hexadecimal almacenado en una base de datos de los AV



Heurística

Arte de descubrir mediante algoritmos predictivos comportamientos potencialmente peligrosos

▪ Ingeniería inversa

proceso con el objetivo de obtener información a partir de un producto, con el fin de determinar cuáles son sus componentes y de qué manera interactúan entre sí

▪ Sandbox

Entorno controlado y aislado para el estudio de programas

Análisis de malware es el arte de la disección del software malicioso para entender cómo funciona, cómo identificarlo y cómo derrotarlo o eliminarlo.

Se procura obtener la máxima cantidad de información de un código malicioso, sin ejecutarlo, y para ello, existen igual herramientas en Linux como Windows, y distros especificas para tal fin.

¡Nos vemos en la siguiente Clase!