Control total de sistemas

Un juego para lammers.

Índice

1. **BREVE TEORÍA**
2. **PRÁCTICA**

1. Presentación

- **Javier Blanco**
  - Director académico en Comunix
    - Docente en hacking ético
    - Consultor en ciberseguridad

1. CONCEPTOS BASE

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

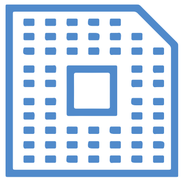
- **ASCII**

Código de caracteres basado en el alfabeto latino (Teclado)

2. MALWARE

- **El *malware* (del inglés *malicious software*),** programa malicioso o programa maligno, también llamado ***badware*, código maligno.**

3. TERMINOLOGÍA BASE

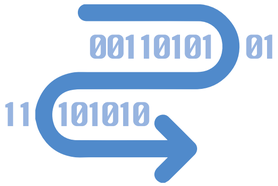


- **Ensamblador**

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

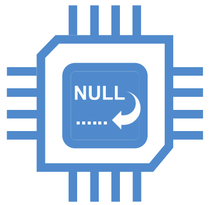
- **Debugger**

o depurador, aplicación para depurar los errores de programación



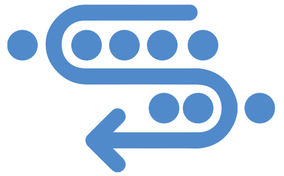
- **Bypasear**

Alternativa para evitar un bloqueo



- **NOP**

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



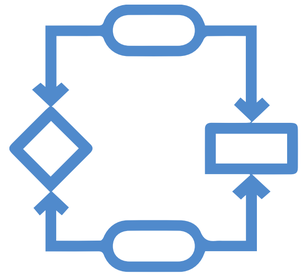
- **NOP**

Técnicas para bypasear un sistema de seguridad

4. AV: ANTIVIRUS

- **Firma**

Código hexadecimal almacenado en una base de datos de los AV



- **Heurística**

Arte de descubrir mediante algoritmos predictivos comportamientos potencialmente peligrosos

5. ANÁLISIS DE VIRUS

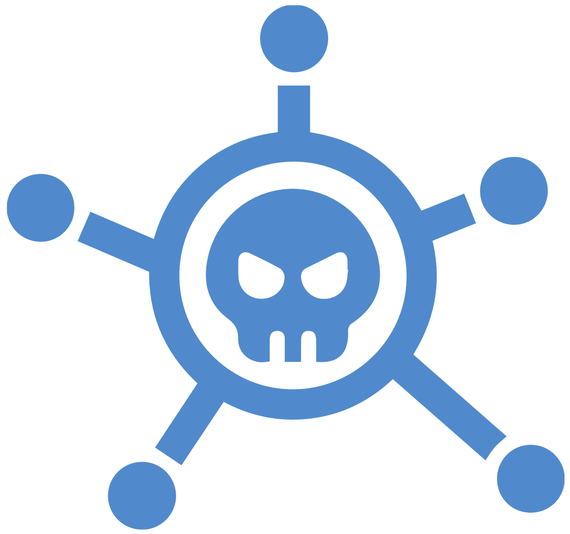
▪ Ingeniería inversa

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

6. CONCEPTOS MALWARE



- **Bindear**

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

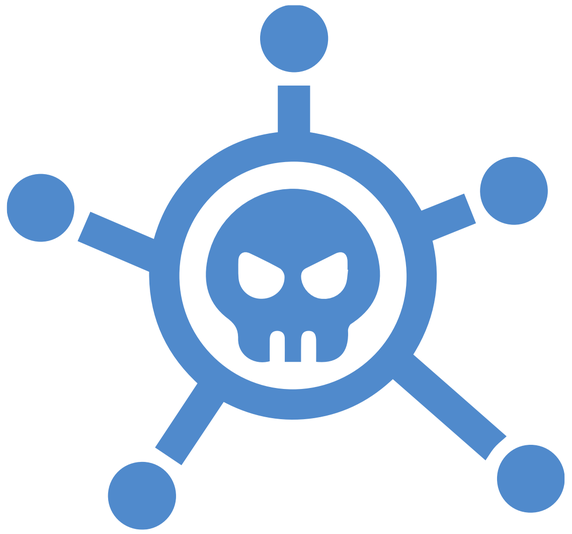
- **Joiner**

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

- **Builder**

  Entorno gráfico para cifrar archivos.

6. CONCEPTOS MALWARE



- **Stub**

  Archivo que encapsula un archivo cifrado con él mismo con el objetivo de desempaquetar el archivo cifrado del EOF sobre la víctima.

- **EOF**

  Final de Archivo.

7. CARACTERÍSTICA 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

8. TIPOS DE MALWARE

- **Adware**

  Genera publicidad.

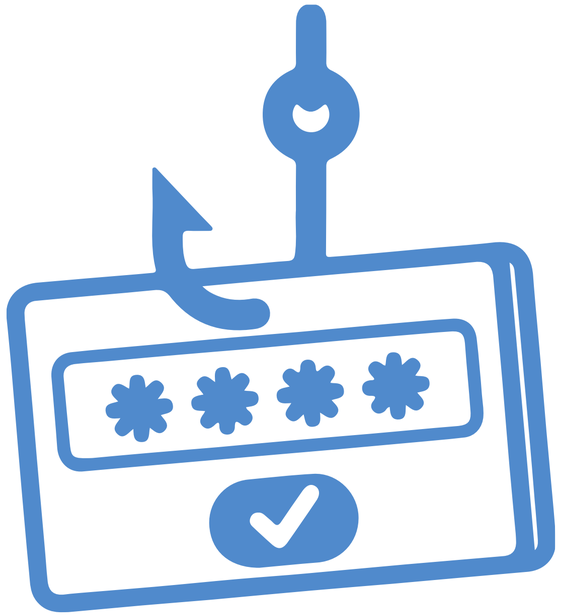
- **Clickers**

  Encargado de generar tráfico hacia la publicidad y pulsar sobre esta.

- **Ransomware / locker**

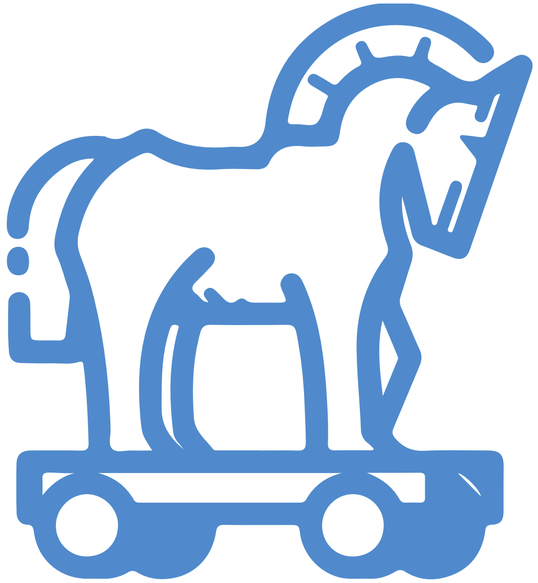
  Restringe el acceso al sistema o parte de él mediante claves criptográficas

8. TIPOS DE MALWARE



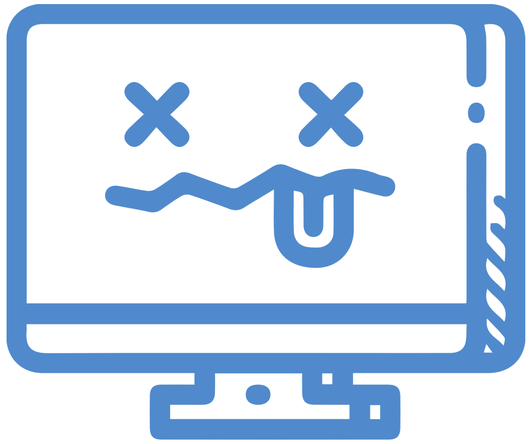
- **Spyware**
  Aplicación con el objetivo de extraer información.
- **Gusano**
  Malware con objetivo de extenderse por la red
- **Phishing**
  Recolectan datos principalmente bancarios

9. TIPOS DE VIRUS



- **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

9. TIPOS DE VIRUS



- **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.

GRACIAS