Tema 2: Herramientas y Métodos de Análisis de Malware

Análisis de Malware

Ciber GUARD

Departamento de Sistemas de Comunicación y Control

UNED ETS de Ingeniería Informática

Índice

Introducción (I)

- El Malware se define como el código informático, en cualquiera de sus posibles formas, que realiza acciones maliciosas sobre un sistema
- Canales: e-mail, web, USB, etc.
- Tipos de Malware: Virus, Troyanos, RAT, Botnets, Rootkit, …
- Efectos: Robo, Corte del servicio, Escalada de privilegios, DoS, Bloqueos, …

Introducción (II)

- Tipos de análisis de Malware:
  - Estático
  - Dinámico
  - De código
  - De memoria
- Técnicas de ofuscación de malware
  - Codificación simple
  - Encriptado de malware
  - Desempaquetado de malware
- Advanced Persistent Threats, APTs

Índice

El lenguaje ensamblador (I)

- Representación de la información a nivel de bit
  - Byte, Word, Dword, Qword
- Elementos:
  - Memoria (little-endian / big endian, punteros)
  - CPU
  - Lenguaje Máquina
- Compilación de programas:
  - En Disco
  - En Memoria

El lenguaje ensamblador (II)

- Registros de CPU
  - Registros de propósito general
  - Puntero
  - Registros de control
- Transferencia de información:
  - Registro-Registro
  - Memoria-Registro
  - Registro-Memoria

Operaciones en lenguaje ensamblador

- Aritméticas y a nivel de bit
- Saltos y condiciones
- Bucles
- Funciones
- La Pila (Stack)
- Vectores y cadenas
- Estructuras

Índice

Clasificación según su funcionalidad

- Tipos de arquitecturas: 32 bits (x86) o 64 bits (x64)
- Clasificación:
  - Desensamblador
    - Estático
    - De código máquina a código ensamblador
  - Depurador
    - Estático / Dinámico
    - Depurar el código malicioso (instrucciones, registros, accesos a memoria,...)
    - Depuración de binarios
  - Decompilador
    - A lenguaje de alto nivel

IDA Pro

- Muy Potente la versión comercial
- Ingeniería inversa, análisis de malware, vulnerabilidades, …
- Multiplataforma y variedad de formatos de archivo
- Versión de evaluación (con limitaciones)
  - No posibilidad de depurar
  - No guarda la base de datos
  - Sin IDAPython
- Versión libre (con limitaciones)
  - Sólo depurar con ficheros de 32-bits
  - No guarda la base de datos
  - Sin IDAPython

Otras herramientas

- x64dbg
  - Depurador de código abierto x32 / x64
  - Control total en tiempo de ejecución
- Utilizar en un entorno controlado
- dnSpy
  - Depurador y Decompilador . NET
- Otros desensambladores / depuradores: radare2, WinDbg, Ollybdg, ...

Índice

Métodos de depuración del malware

- Seleccionar el programa a depurar
- Examinar y controlar procesos
  - Depurar un proceso en tiempo de ejecución
  - Iniciar un proceso nuevo
- Depuración de programas
  - Controlar la ejecución
  - Interrumpir un programa con puntos de interrupción
- Métodos de depuración
  - Ejecutar
  - Ejecución de instrucción individual (o una llamada a función)
  - Ejecutar hasta volver de una instrucción
  - Ejecutar hasta el cursor o una instrucción seleccionada

Tema 2: Herramientas y Métodos de Análisis de Malware

Análisis de Malware

Ciber GUARD

Departamento de Sistemas de Comunicación y Control

UNED ETS de Ingeniería Informática