Análisis de malware

Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx

Escenario

- Regreso oficina después de un fin de semana de 3 días.
- Quejas de que un servidor Windows esta lento.
- Primer paso: Buscar fallas a nivel hardware.
- Segundo paso: Buscar en el sistema operativo.
  - Se ven archivos que no estaban en el servidor la última vez que se accedió a él.
  - Deducción: servidor comprometido por algún tipo de software malicioso.
- Contar con un Disaster Recovery Plan, que permita regresar al servidor a una condición previa a la de la infección.

Terminos

- Virus
- Gusanos
- Caballos de troya
- Spyware
- Adware
- Puertas traseras
- Rootkits
- Sniffers
- Reverse Code Engineering
- Disassemblers
- Debuggers
- Decompiler

Lámina 3 Dr. Roberto Gómez Cárdenas

Preparation
Identification
Containment
Eradication
Recovery
Lessons learned.

Lámina 4 Dr. Roberto Gómez Cárdenas

¿Para que el análisis de malware?

- ¿Para que se requiere llevar a cabo análisis de malware si no trabajo para un distribuidos de anti-virus?
- Objetivos
  - Entender como funciona una pieza específica de malware, con el objetivo de implementar defensas para proteger la red de la organización.

Lámina 5 Dr. Roberto Gómez Cárdenas

Preguntas responde análisis malware

- ¿Cómo se infecto esta máquina con este malware?
- ¿Qué es lo que hace exactamente este malware?

Lámina 6 Dr. Roberto Gómez Cárdenas

Tipos análisis de malware

- Dos tipos
  - Análisis estático de código.
    - Revisar el código y caminar a través de él para entender de mejor forma lo que el malware esta haciendo.
  - Análisis dinámico de código
    - Como se comporta el código cuando es ejecutado.
- No hay una regla fija, pero se sugiere empezar con el estático para después llevar a cabo el dinámico.
- Verificar las leyes existentes relacionadas con ingeniería inversa

Lámina 7 Dr. Roberto Gómez Cárdenas

Herramientas

- VMWare
  - Máquina virtual
- BgInfo
  - Proporciona información importante del sistema como hostname, dirección IP, versión sistema operativo, etc.
- Process Explorer
  - Indica que archivos, llaves de registro y otros objetos se han abierto, que DDLs se han cargado.
- Process Monitor
  - Monitoreo de sistema de archivos, registro, procesos, threads y actividad de los DDL en tiempo real.

Lámina 8 Dr. Roberto Gómez Cárdenas

Herramientas

- Psfile
  - Lista de archivos abiertos de forma remota.
- RootkitRevealer
  - Lleva a cabo una búsqueda de rootkits conocidos.
- Streams
  - Aplicación que da a conocer NFTS alternate streams.
- Strings
  - Aplicación que busca strigs ANSI y UNICODE en imágenes binarias.
- Nmap
  - Escaneao de puertos

Lámina 9 Dr. Roberto Gómez Cárdenas

Herramientas

- TCPView
  - Herramienta que proporciona información acerca de conexiones TCP y UDP, incluyendo las direcciones locales y remotas así omo el estado de la conexión TCP.
- Windump
  - Versión windows del sniffer tcpdump
- Fport
  - Identifica puertos desconocidos y las aplicaciones asociadas a ellos.
- Hfind
  - Parte del Forensic Toolkit
  - Aplicación que busca en el disco archivos ocultos.

Lámina 10 Dr. Roberto Gómez Cárdenas

Herramientas

- Vision
  - Reporta todos los puertos TCP y UDP abiertos, y los mapea al proceso y/o aplicación asociada.
- Filewatch
  - Un monitor de cambio en archivos.
- Attacker
  - Una aplicación apara escuchar un puerto TCP/UDP
- MD5sums
  - Generada huellas digitales MD5 para verificación de integridad.
  - Se recomienda usar otro tipo de herramienta que produzca huellas en base a otro algoritmo.

Lámina 11 Dr. Roberto Gómez Cárdenas

Herramientas

- Winalysis
  - Monitorea cambios en archivos, el registro, usuarios, grupos, seguridad, servicios, recursos compartidos, trabajos calendarizados, ambiente del sistema y más.
- Winhex
  - Editor hexadecimal.
  - Puede elegir el editor hexadecimal que prefiera.

Lámina 12 Dr. Roberto Gómez Cárdenas

Herramientas ingeniería inversa

- Editor hexadecimal
  - Winhex, Hex Workshop, Ultraedit, Hacker's View
- Des-ensamblador
  - IDA, WDasm, Sourcer 7,
- Descompresor
  - Deshrink, PeUNLOCK,
- Depurador
  - Debug, Soft-Ice (El más usado), TR, dbg,
- Analizador de archivos
  - File Monitor
- Dumpeadores de memoria
  - UserModeProcessDumper, Memory Dumper Pro
- Monitor del registro
  - Registry monitor (Win95).

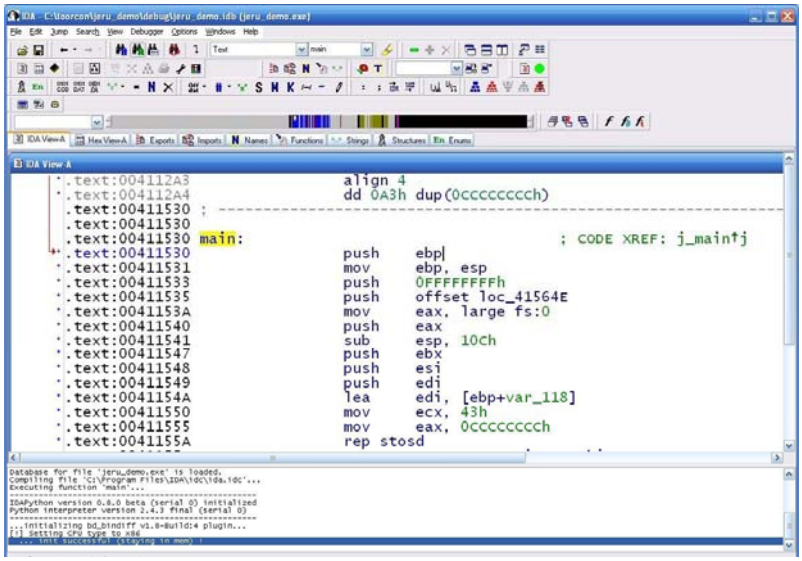
Lámina 13 Dr. Roberto Gómez Cárdenas

Desensamblador IDA Pro

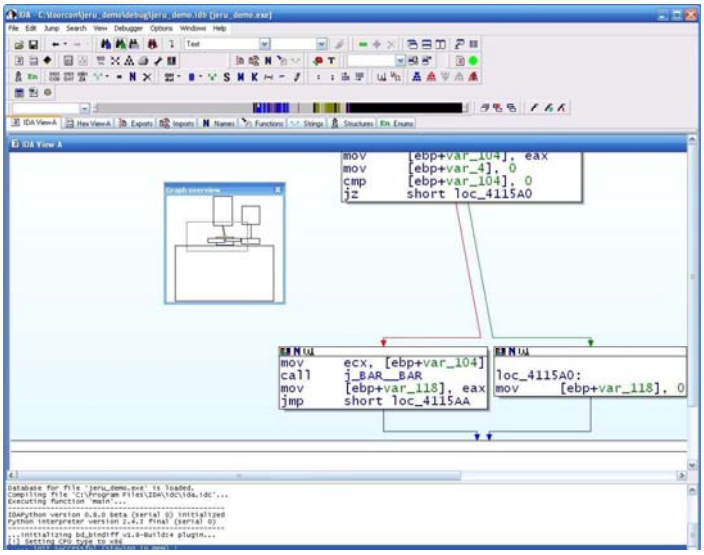
- IDA Pro es la mejor herramienta en esta categoría.
- Desensambladores convierten un binario a ene lenguaje ensamblador .
- El programa no corre, análisis estático.
- Soporta más de 30 procesadores.
- Hecho para ingenería inversa.
- Identificación de librerías .
- Programable (SDK y scripts)

Lámina 14 Dr. Roberto Gómez Cárdenas

Screenshot IDA Pro



Screenshot IDA Pro



Depuradores

- Ejecutan el programa
  - Línea por línea
  - Usando breakpoints
- Los más comunes
  - WinDBG
  - OllyDbg
  - GDB
  - Softice

OllyDbg

- Hecho para ingeniería inversa
- Programable (SDK)
- Muchos plugins

Screenshot OllyDbg

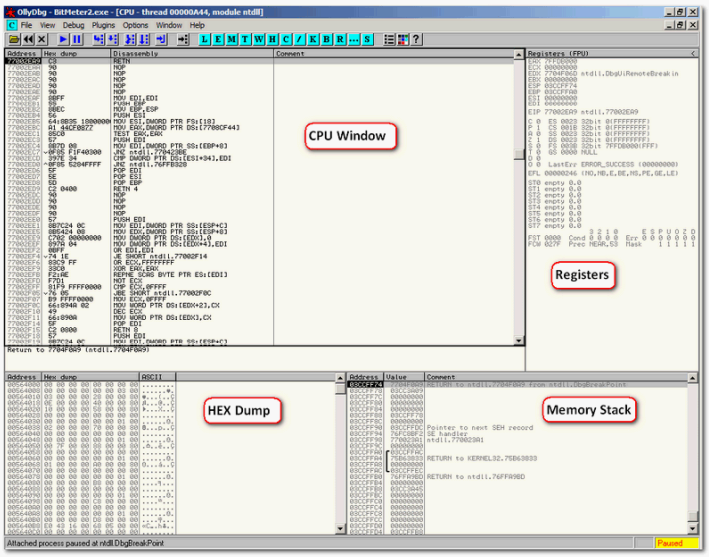


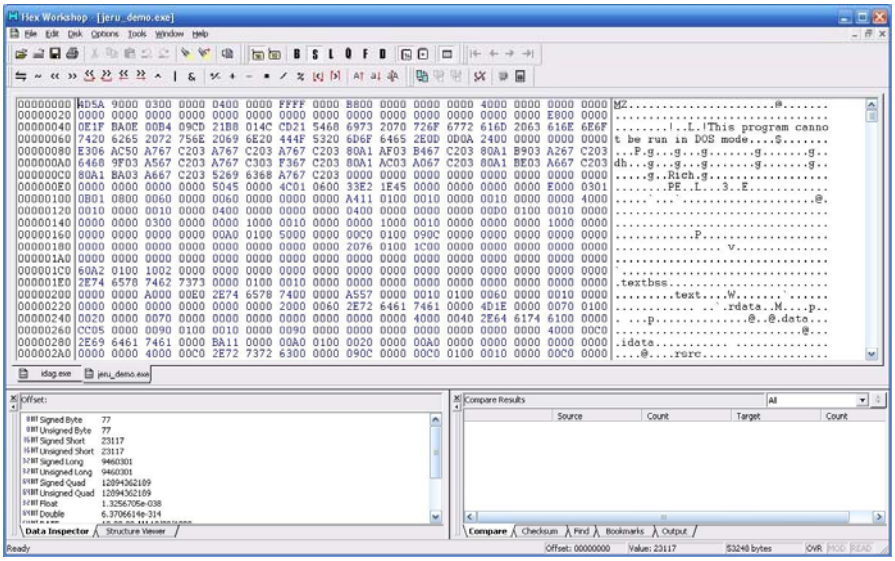
Lámina 19 Dr. Roberto Gómez Cárdenas

Code packers

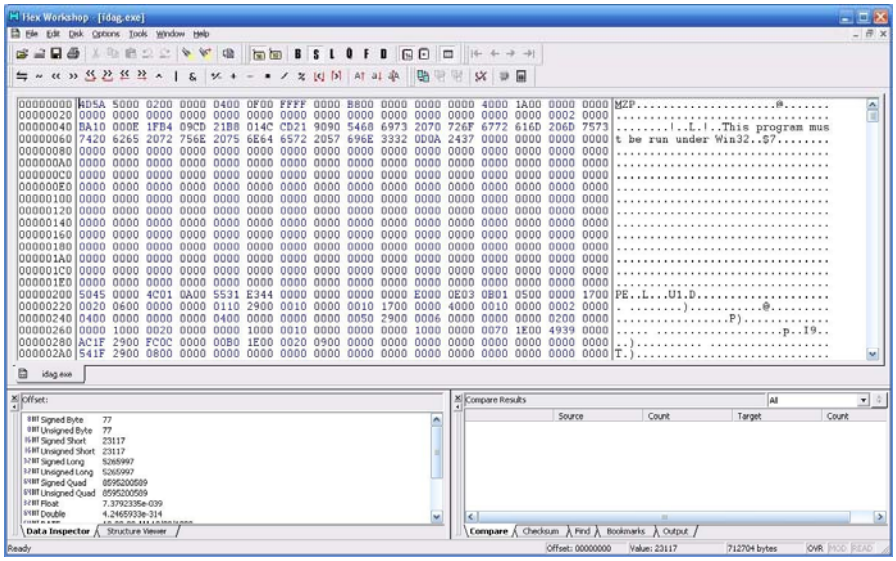
- En el 2004, 90% virus computadoras 32 bits usan un run-time packer como UPX o ASPCK.
- Comprensión de código.
- Aplicaciones descomprimida en la memoria del sistema.
  - Detección y borrado de código es más complicado.
  - Hacer el código más pequeño y menos detectable.
  - Posible cifrar el código dentro del packer.

Lámina 20 Dr. Roberto Gómez Cárdenas

Ejecutable normal



Ejecutable empaquetado



Identificación del empaquetado

- Softwate PEiD

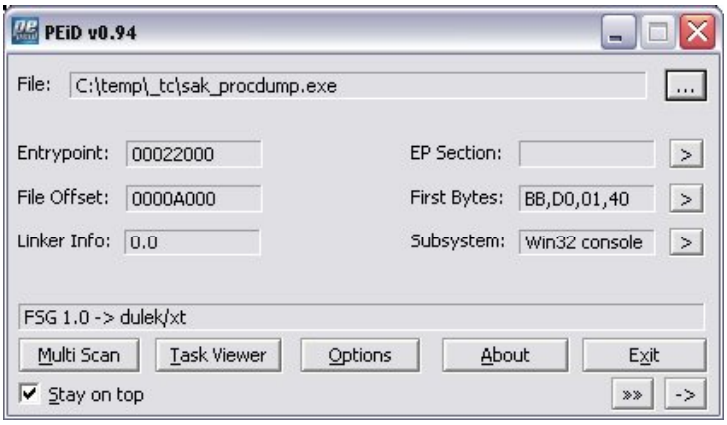


Lámina 23 Dr. Roberto Gómez Cárdenas

Malware puede contener scripts

- Cambiar configuración del sistema.
- Deshabilitar firewall de windows.
- Cambiar configuración del DNS.
- Parchar/actualizar el sistema.
- Instalar un servidor SMTP.
- Instalar herramientas conexión remota Netcat y VNC.

Lámina 24 Dr. Roberto Gómez Cárdenas

Adquisición malware

- Honeynets
- Visita sitios web infectados.
- Correo
- Google search

Lámina 25 Dr. Roberto Gómez Cárdenas

Análisis estático

- No analizar computadora en red.
- Instalar maquinas virtuales.
- Instalar sistema operativo en maquinas virtuales.
- Copiar/instalar herramientas.
- Obtener huellas digitales de todas las herramientas.
- Correr varios antivirus,
- Abrir con editor hexadecimal.
- Determinar si usa un packer como UPX
- Búsqueda strings
- Desensamblar el malware
- Ingeniería inversa

Lámina 26 Dr. Roberto Gómez Cárdenas

Análisis dinámico

- Malware es ejecutado y se observan cambios realizados en el sistema.
- Asegurarse VM esta en Host-Only networking
- Tomar un snapshot del sistema antes de iniciar análisis (uso de Winalysis).
  - Process Explorer, TCPView, Windump, Explorer.
- Correr 15 minutos, correindo Proceess Explorer y TCPView.
- Tomar otro snapshot
- Comparar los snapshots tomados.
- Correr PE y TCPView buscando por cambios.
- Examinar tráfico red capturado con windump.

Lámina 27 Dr. Roberto Gómez Cárdenas

Process Explorer

- Observar nuevos procesos corriendo y ver donde están ubicados.
- Es posible que se encuentren en el registro y entonces el malware será cargado en cada arranque.
- Cualquier proceso instalado por el malware deber ser investigado.

Lámina 28 Dr. Roberto Gómez Cárdenas

TCPView

- Buscar por nuevos procesos en escucha, que pueden recibir instrucciones de servidores instalados en el sistema por el malware.
- Si un proceso en escucha se instaló en la máquina, investigarlo.
- Intentar conectarse a él de varias formas
  - telnet, netcar, o web browser
- Seguir escuchando al proceso que creo el proceso en escucha e investigar.

Lámina 29 Dr. Roberto Gómez Cárdenas

Network Traffic

- Observar como funciona el malware.
- Tomar notas de cómo se ve el tráfico.
- Útil para escribir listas de control de acceso y reglas para el IDS.
- Si se baja un backdoor, configurar servidor para que lo baje y conectarse al sistema y ver lo que el atacante ve.

Lámina 30 Dr. Roberto Gómez Cárdenas