Análisis de Malware con IDAT PRO y Ollydbg

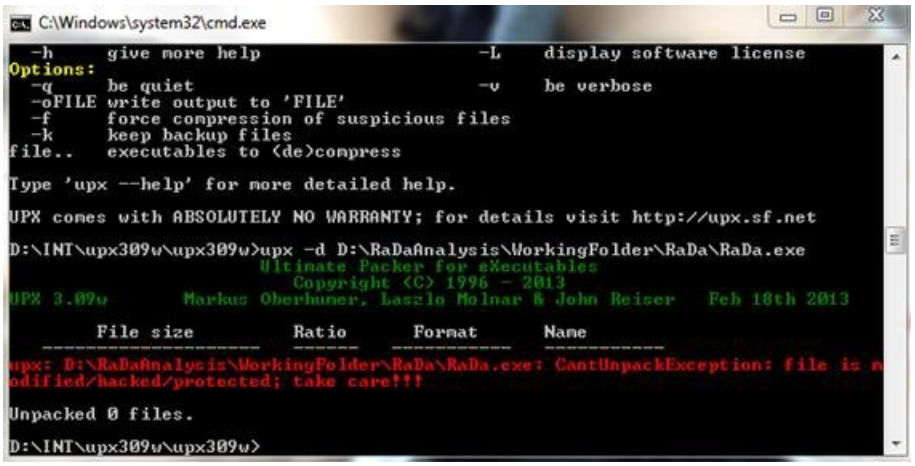
Curso : Análisis de Malware con IDAT PRO y Ollydbg

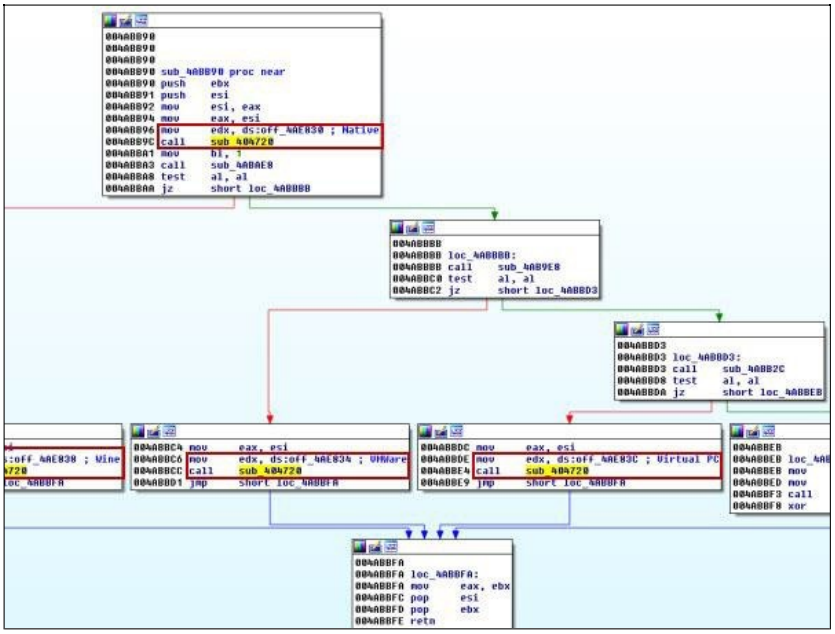
Duración : 24 Horas

I. DESCRIPCIÓN

El software malicioso o malware, juega un papel en la mayoría de intrusiones informáticas e incidentes de seguridad. Cualquier software que hace algo que cause daño a un usuario, un equipo o la red pueden ser considerados malware, incluyendo virus, troyanos, gusanos, rootkits, scareware, spyware y ransomware.

Análisis de malware es el arte de identificar la estructura de software malicioso para entender cómo funciona, cómo identificarlo y cómo derrotar o eliminarlo. Este curso está orientado a poder enseñarte a identificar los malware, las acciones que este realiza y como eliminarlos.





II. COMPETENCIA

Al final del curso, el alumno:

- Obtendrás los conocimientos necesarios para poder identificar las acciones que realiza un malware cuando ingresa a un sistema operativo.
- Podrás desarrollar medidas de protección y limpieza de los malware analizados.

III. METODOLOGÍA

El curso contará con sesiones teórico-prácticas. Se empleará material audiovisual con la finalidad de facilitar los procesos de adquisición y evaluación del aprendizaje. Durante las clases se buscará la participación activa de los alumnos mediante el desarrollo de ejercicios, analisis en vivo de malware y aprendizaje de tecnicas utilizadas por estos programas.

IV. DURACION

El curso tendra una duración de 24 Horas

V. CONTENIDO

1. ANALISIS ESTATICO BASICO

- Escaneo de Antivirus: Un primer paso util
- Hashing: Sacando un Fingerprint del Malware
- Encontrando Strings
- Malware Empaquetado y Ofuscado
- Detectando Packers con PEiD
- Formato de Archivo PE(Portable Executable)
- Enlazando Librerías y Funciones
- Linking: Static, Runtime,y Dynamic
- Analizando Enlaces a funciones dinámicas con Dependency Walker
- Funciones Importadas
- Funciones Exportadas
- Análisis estático en la Practica
- PotentialKeylogger.exe: Un Unpacked Executable
- PackedProgram.exe: Un callejón sin Salida
- La Cabecera y Secciones de archivos PE
- Examinando Archivos PE con PEview
- Revisando la Sección de Recursos con Resource Hacker
- Usando otras herramientas de archivos PE

2. ANALISIS DE MALWARE EN MAQUINAS VIRTUALES

- La estructura de una Virtual Machine
- Creando tu Maquina de Análisis de Malware
- Configurando VMware
- Usando tu máquina de Análisis de Malware
- Conectando un Malware a Internet
- Conectando y desconectando Dispositivos Periféricos (USB, CDROM, ..
- Tomando Snapshots
- Transfiriendo archivos desde una Máquina virtual
- El riesgo de usar una Máquina Virtual VMware para análisis de malware

3. ANALISIS DINAMICO BASICO

- Sandboxes: Un enfoque rápido y oscuro
- Usando un Sandbox para análisis de malware
- Corriendo un Malware
- Monitoreando con Process Monitor
- Analizando con Procmon
- Filtrado en Procmon
- Viendo los procesos con Process Explorer
- Display en Process Explorer
- Usando la opción: Verify
- Comparando Strings
- Usando Dependency Walker
- Analizando documentos maliciosos
- Comparando Registros de Windows con Regshot
- Falseando una Network
- Usando ApateDNS
- Monitoreando con Netcat
- Packet Sniffing con Wireshark
- Usando INetSim
- Realizando análisis dinámico en la práctica

4. ANALISIS ESTATICO AVANZADO

ANALIZANDO X86 DISASSEMBLY

- Niveles de abstracción
- Ingeniería Reversa
- Arquitectura x86
- Memoria Principal
- Instrucciones X86
- Opcodes y Endianness

- Operandos
- Registros
- Instrucciones simples
- El Stack
- Condicionales
- Metodo Main en C
- Architectura Intel x86

5. IDA PRO

- Cargando un ejecutable
- La interface de IDA Pro
- Modos de Ventanas Disassembly
- Ventanas útiles para el análisis
- Retornando a la vista por default
- Navegando en IDA Pro
- Buscando
- Usando Cross-References
- Code Cross-References
- Data Cross-References
- Analizando Funciones
- Usando Opciones Graficas
- Mejorando el desmontaje
- Renombrando Locations
- Comentarios
- Formateando Operandos
- Usando Constantes nombradas
- Redefiniendo Code y Data
- Extendiendo IDA con Plug-ins
- Usando IDC Scripts
- Usando IDAPython
- Usando Plug-ins Comerciales

6. ANALYZING MALICIOUS WINDOWS PROGRAMS

- API de Windows
- Tipos y Notaciones Hungarian
- Handles
- Funciones de Archivos del Sistema
- Archivos especiales
- Registros de Windows
- Registry Root Keys
- Regedit
- Programas que corren automaticamente
- Tipicas funciones de Registro

- Analizando el Registro en la Practica
- API Networking
- Socket compatibles con Berkeley
- El Servidor y Lado del Cliente en Networking
- La API WinINet
- Despues de Correr un malware
- DLLs
- Processes
- Threads
- Coordinación entre procesos con Mutexes
- Services
- Kernel vs. User Mode

7. ANALISIS DINAMICO AVANZADO

DEBUGGING

- Source-Level vs. Assembly-Level Debuggers
- Kernel vs. User-Mode Debugging
- Usando un Debugger
- Single-Stepping
- Stepping-Over vs. Stepping-Into
- Pausando la ejecución con Breakpoints
- Excepciones
- Excepciones comunes
- Modificando la Ejecución con un Debugger
- Modificando un Programa Ejecutable en la Practica

8. OLLYDBG

- Cargando Malware
- Abriendo un Ejecutable
- Atachando un Procesoen Memoria
- La Interfaces de OllyDbg
- Memory Map
- Rebasing
- Viendo Threads y Stacks
- Ejecutando el Codigo
- Breakpoints
- Breakpoints Software
- Breakpoints Conditional
- Breakpoints Hardware
- Breakpoints Memory
- Cargando DLLs
- Traceando
- Call Stack

- Run Trace
- Tracing Poison Ivy
- Manejando Excepciones
- Patching
- Analizando Shellcode
- Plug-ins
- OllyDump
- Ocultando Debugger
- Bookmarks