Práctica 2 - Ofuscación de malware

Introducción

En el presente caso práctico el estudiante tiene que crear un entorno virtual mediante el software de virtualización VirtualBox (https://www.virtualbox.org/), o bien puede utilizar VMWare (https://www.vmware.com/es.html) como alternativa en su versión libre.
En lo que se refiere a software específico, fundamentalmente se utilizarán programas indicados en el capítulo 9 (Malware Obfuscation Techniques) del libro Learning Malware Analysis: PEstudio y x64dbg (que integra la herramienta Scylla).

Pasos a seguir

1. Instala los siguientes programas en la máquina virtual Windows de tu entorno controlado (ten en cuenta que tendrás que permitir el acceso a Internet o transferir los archivos necesarios a través de carpetas compartidas, portapapeles compartido o similar). Describe brevemente los programas que utilices:
    a. PEstudio
    b. X64dbg
    c. Scylla
2. Elige uno o varios ficheros de malware a nivel local y de red que consideres de entre la documentación del curso virtual, u otro que consideres de interés.
    a. Muy importante: no lo descargues desde la máquina virtual anfitriona y no lo ejecutes mientras sigas conectado a Internet (aunque sea dentro de la máquina virtual). Deberías hacerlo desde la máquina virtual de Ubuntu.
    b. Puedes utilizar ejemplos del libro "Practical Malware Analysis" (https://practicalmalwareanalysis.com/labs/), de los sitios web recomendados en el libro base, entre otros. Dicha documentación también está disponible en O'Really.
3. Asegúrate de haber aislado completamente la máquina virtual que vayas a utilizar (puedes utilizar la MV Windows o Linux, aunque se recomienda la utilización de Windows y la monitorización de la red con Linux, tal y como se hizo en la práctica anterior).
4. Deshabilita el Servicio de Windows Defender de la máquina Windows, ya que puede interferir cuando se ejecuta un malware. Se debe hacer en el editor de directivas de grupo local de Windows. Generalmente en Configuración del equipo | Plantillas administrativas | Componentes de Windows | Windows Defender. En el panel derecho, hacer doble click en Desactivar la política de Windows Defender.
5. Analiza el malware seleccionado desde el punto de vista de la ofuscación de código vista en los contenidos teóricos de la asignatura, elaborando un informe acerca de todas las características encontradas:
    a. Cifrado César, Base64 y XOR.
    b. Identificación de *cryptosignatures*.
6. Analiza el malware seleccionado desde el punto de vista del empaquetado de ejecutables. Para ello, asegúrate de que eliges un malware que haya sido previamente empaquetado (tratado con un *packer*), o en caso contrario, puedes elegir un malware nuevo que esté empaquetado o empaquetarlo con una herramienta como UPX (https://upx.github.io/):

a. Realiza el proceso de desempaquetado manual que se ha explicado en los contenidos teóricos y en la bibliografía básica.
b. Elige una herramienta de desempaquetado automático entre las propuestas en los contenidos teóricos (TitanMist, IDA Pro, x64dbg, etc.) y realiza un desempaquetado automático del ejecutable, documentando la salida obtenida.

Entrega

Sigue los pasos del caso práctico que haya desarrollado y realiza un informe sobre el mismo, problemas encontrados, y las conclusiones obtenidas. El informe debería ser no mayor de 10 páginas, y teniendo en cuenta que el destinatario es el jefe de un departamento técnico, que desea tomar decisiones técnicas.