Análisis de malware

Prácticas de análisis dinámico básico

Gustavo Romero López - gustavo@ugr.es

Updated: 3 de marzo de 2025

Departamento de Ingeniería de Computadores, Automática y Robótica

Prácticas de análisis dinámico básico

- En *Practical Malware Analysis* proponen 4 ejercicios:
  - ejercicios: páginas 61 y 62
  - códigos: https://pccito.ugr.es/am/practicas/03
  - soluciones: páginas 482 a 493
- El verdadero reto será analizar una muestra de malware real.

https://pccito.ugr.es/am/practicas/03/Lab03-01.exe

Analice el fichero Lab03-01.exe mediante herramientas de análisis dinámico básico.

1. ¿Qué cadenas hay en su interior?
2. ¿Como afecta al sistema (“*host-based indicators*”)?
   - ficheros
   - registro
   - DLLs
   - mutex
3. ¿Usa la red? ¿Cómo? (“*network-based signatures*”)
   - URLs
   - DNS
   - IPs
   - cadenas de agente

Solución Lab03-01.exe

1. Parece estar comprimido. La única función importada es `ExitProcess` a pesar de que aparezcan numerosas cadenas que no parecen estar ofuscadas.
2. Crea un mutex llamado `WinVMX32`, se copia en `C:\ Windows\System32\vmx32to64.exe` y provoca su ejecución en el arranque de sistema haciendo que la clave de registro `HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run\VideoDriver` apunte a la copia.
3. Emite un paquete de red de 256 bytes con lo que a primera vista parecen datos aleatorios tras resolver `www.practicalmalwareanalysis.com`.

https://pccito.ugr.es/am/practicas/03/Lab03-02.dll

Analice el fichero Lab03-02.dll mediante herramientas de análisis dinámico básico.

1. ¿Cómo hacer que este se instale?
2. ¿Cómo hacer que se ejecute?
3. ¿Bajo qué proceso se ejecuta?
4. ¿Qué filtros de Process Monitor utilizaría para buscar información?
5. ¿Cómo afecta al sistema?
6. ¿Cómo utiliza la red?

Solución Lab03-02.dll I

1. Instalar con "`rundll32.exe Lab03-02.dll,installA`".
2. Para hacer que se ejecute debemos iniciar el servicio que instala con "`net start IPRIV`".
3. Utilice `Process Explorer` para averiguar que proceso `svchost.exe` ejecuta el servicio a simple vista o con la opción de encontrar DDLs y la cadena `Lab03-02.dll`.
4. En `Procmon` filtraremos con el número de proceso encontrado con `Process Explorer`.

Solución Lab03-02.dll II

5. El malware instala el servicio `IPRIV` que muestra el nombre "Intranet Network Awareness (INA+)" y la descripción "Depends INA+, Colects and stores network configuration and location information, and notifies applications when this information changes". Se instala de manera persistente en el registro en "`HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: %CurrentDirectory%\Lab03-02.dll`". Si renombramos el fichero `Lab03-02.dll` como `malware.dll` entonces se instala con ese otro nombre.

Solución Lab03-02.dll III

6. Resuelve el dominio `www.practicalmalwareanalysis.com` y se conecta a través del puerto 80 utilizando lo que parece ser HTTP. Realiza la petición "`GET serve.html`" y utiliza la cadena de cliente de usuario "`%ComputerName% Windows XP 6.11`".

https://pccito.ugr.es/am/practicas/03/Lab03-03.exe

Ejecute Lab03-03.exe mientras lo monitoriza en un entorno seguro.

1. ¿Qué nota al monitorizar el malware con Process Explorer?
2. ¿Puede identificar alguna cambio en la memoria en vivo?
3. ¿Cómo afecta al sistema?
4. ¿Cuál es el propósito de este programa?

Solución Lab03-03.exe

1. Este malware lleva a cabo un reemplazo de proceso en `svchost.exe`.
2. Comparando la imagen en memoria de `svchost.exe` con su imagen en disco podemos comprobar que no es la misma. En memoria aparecen las cadenas "practicalmalwareanalysis.log" y "[ENTER]" pero en disco no está ninguna.
3. Crea el fichero `practicalmalwareanalysis.log`.
4. Lanza un *keylogger*.

https://pccito.ugr.es/am/practicas/03/Lab03-04.exe

Ejecute Lab03-04.exe mientras lo monitoriza en un entorno seguro.

1. ¿Qué pasa al ejecutar este fichero?
2. ¿Qué obstaculiza el análisis dinámico?
3. ¿Hay otras formas de ejecutar este programa?

Solución Lab03-04.exe

1. Al ejecutar el malware haciendo doble click en él se borra inmediatamente.
2. Podemos suponer que es necesario proporcionar algún parámetro mediante la línea de órdenes.
3. Probando las cadenas que parecen parámetros, como “-in” no permite avanzar. Es necesario un análisis más en profundidad.