DGTIC UNAM CERT

Análisis dinámico de DLLs maliciosas

Ing. Jonathan Banfi Vázquez

Objetivo

- Desarrollar herramientas orientadas al análisis de “Bibliotecas de Enlace Dinámico" para sistemas operativos Windows.

- Lo anterior es por la necesidad de estudiar y documentar diversas amenazas, que si bien no son un archivo ejecutable autónomo, tienen funciones específicas que se llevan a cabo por solicitud de algún proceso causando daño en los sistemas de cómputo.

Introducción

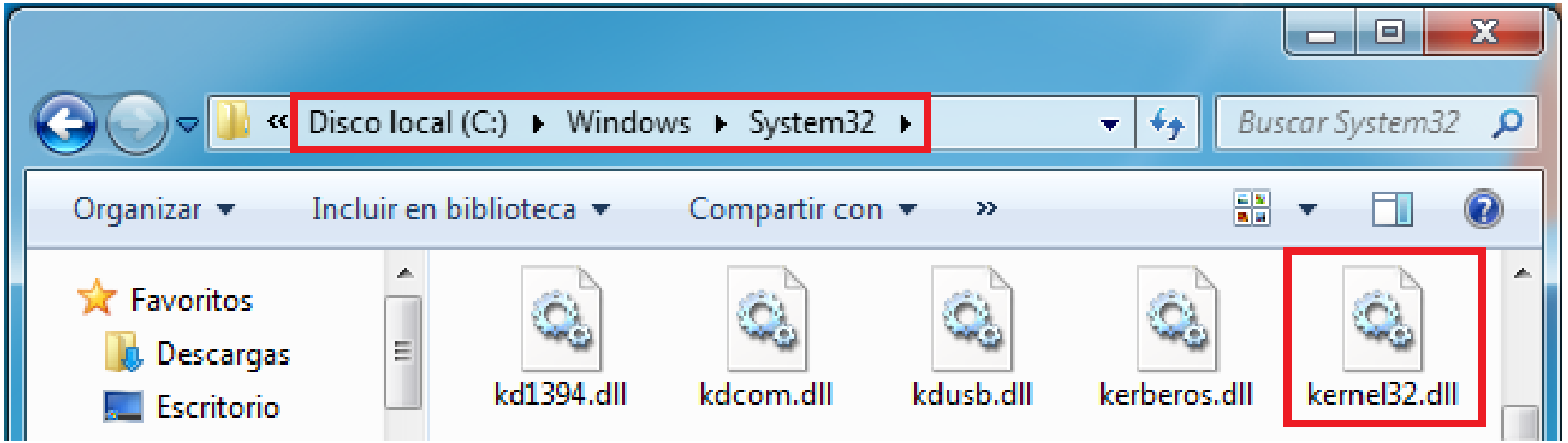
DLL (*Dynamic Library Link*)

- Archivos que contienen funciones que se ejecutan por solicitud de algún proceso.

- No se puede hacer doble clic sobre los archivos DLL para correrlos puesto que no son una entidad autónoma.

Introducción

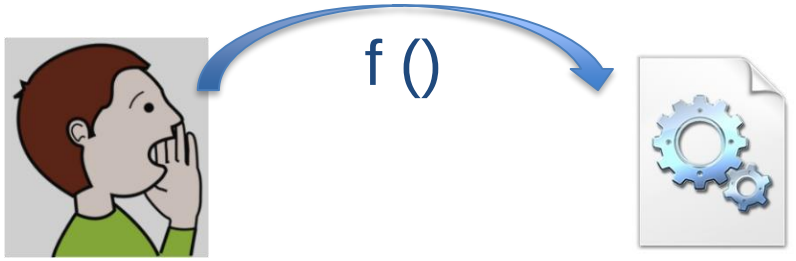
DLL (*Dynamic Library Link*)



Introducción

Llamadas al sistema

- También conocidas como “llamadas a la API”.



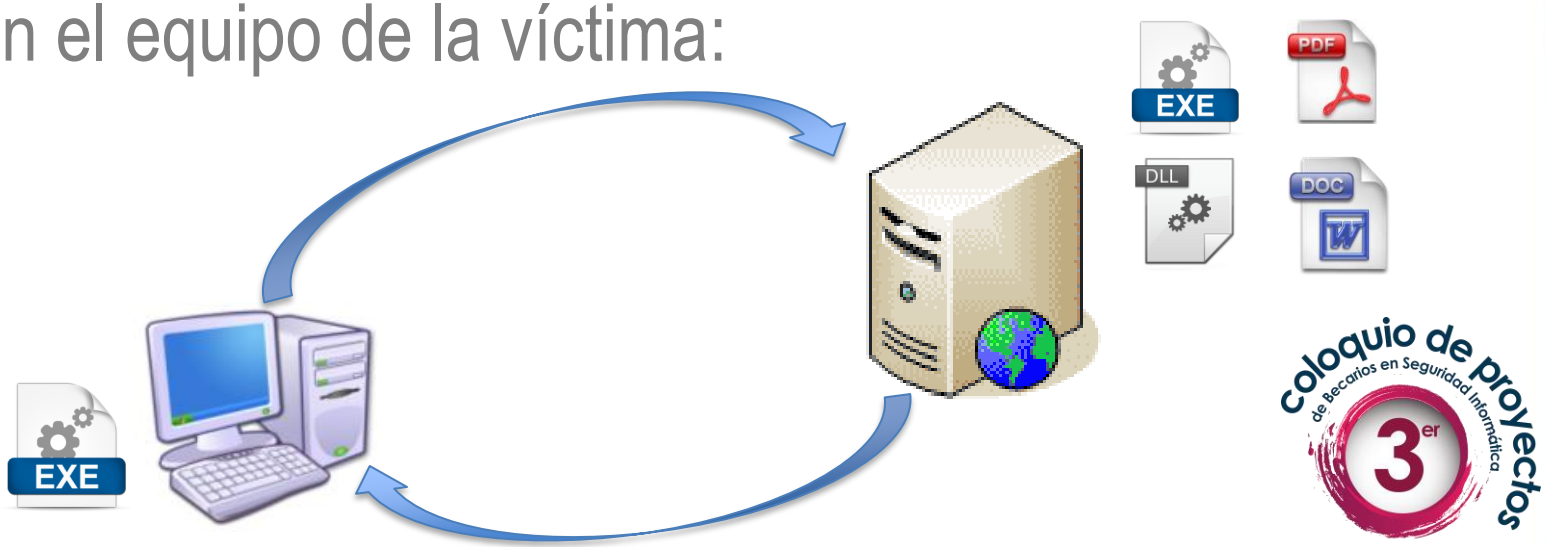
- Dan a los programas la manera de interactuar con el sistema operativo y *hardware*.

Introducción

Downloader

- Se conecta a equipos remotos para descargar archivos maliciosos y posteriormente iniciarlos en el equipo de la víctima:

  - ❑ URLDownloadToFile()
  - ❑ ShellExecute() / WinExec()



Introducción

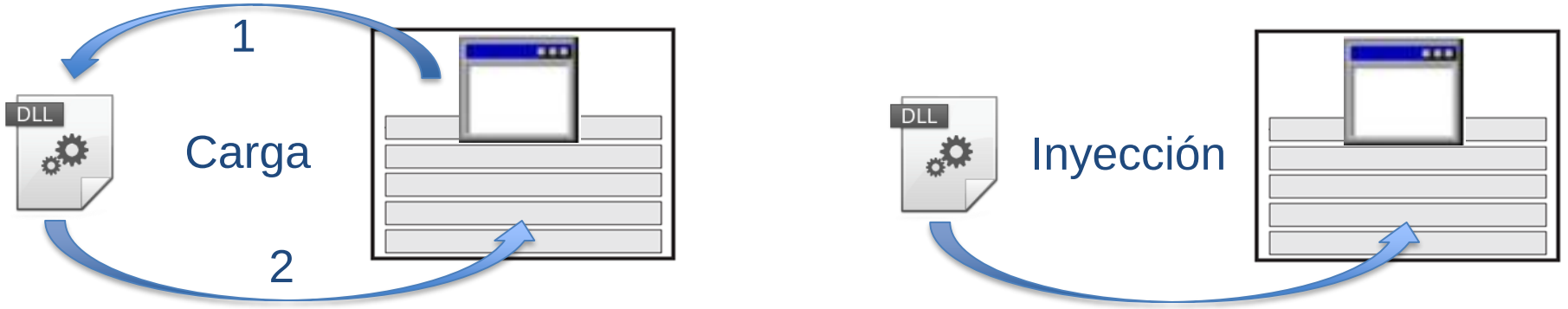
Downloader

- Tienden a ser ejecutables muy pequeños.
- Pueden pasar desapercibidos ante motores de detección de software malicioso.

Introducción

Inyección de DLLs

- Es la inserción de código de la DLL en el espacio de direcciones de algún proceso para que pueda ejecutarse.

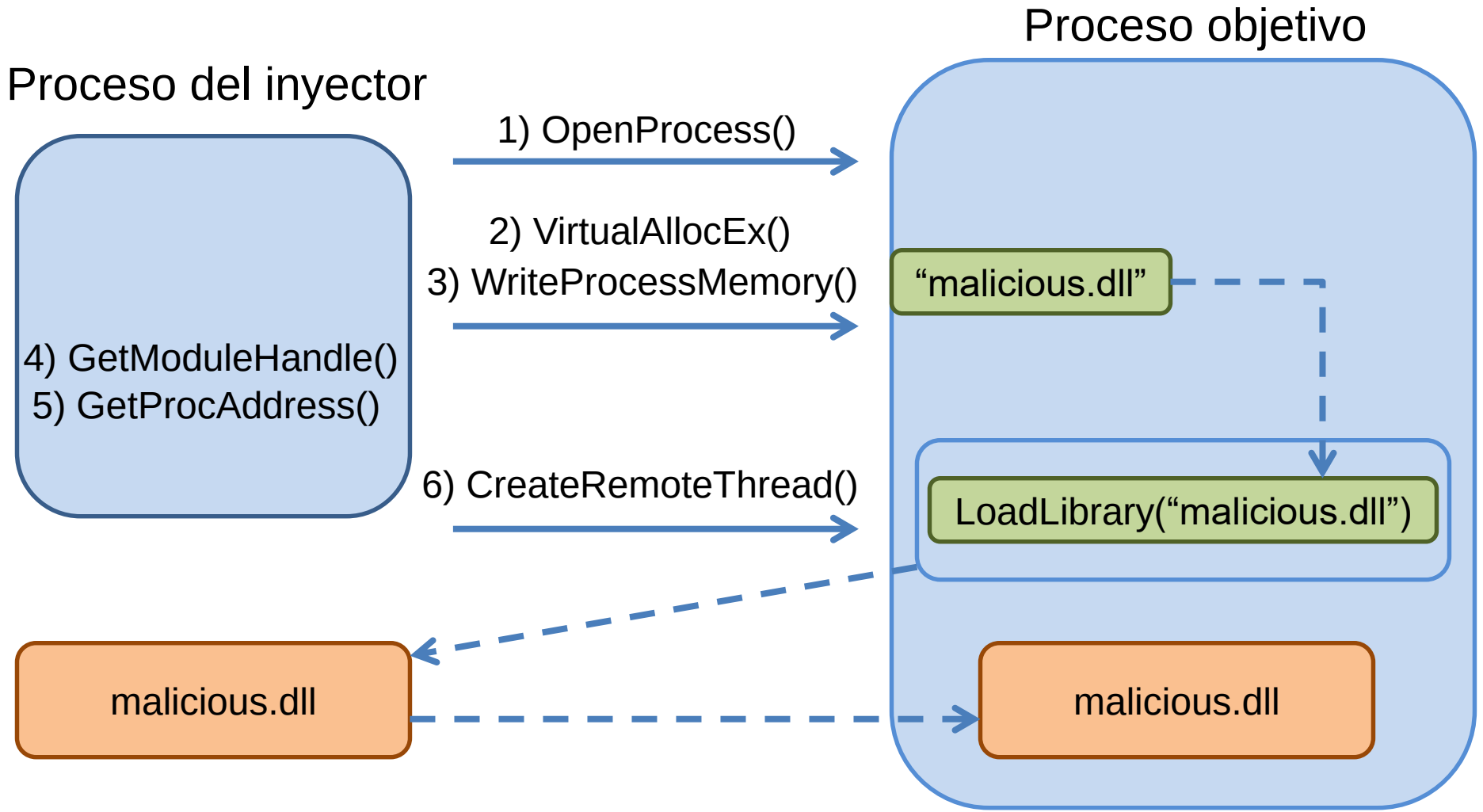


Introducción

Inyección de DLLs

- Existen varias técnicas:
  - ❑ Windows *hooks* con SetWindowsHookEx()
  - ❑ **Uso de la función CreateRemoteThread()**

Introducción



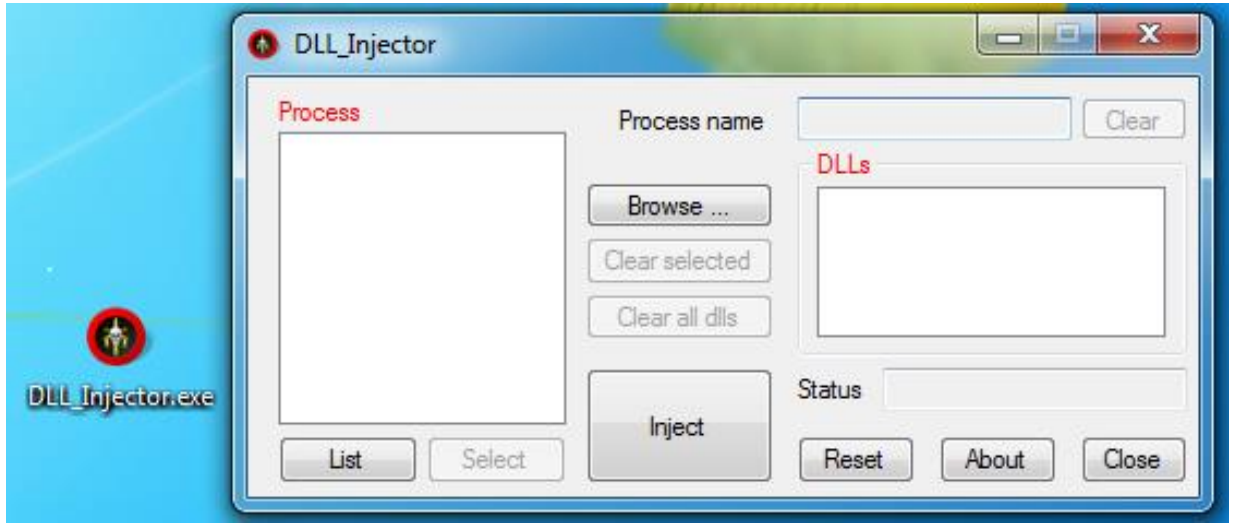
Herramientas de análisis

- A continuación se mostrarán dos herramientas que ayudan a realizar análisis dinámico de DLLs maliciosas:

Herramientas de análisis

DLL_Injector

- Herramienta programada en Visual Basic con interfaz gráfica para inyectar una o varias DLLs en un determinado proceso.



Herramientas de análisis

DLL_Injector

- Lista los procesos que corren en el sistema operativo ordenados alfabéticamente y van seguidos por su identificador de proceso.

- Valida que se haya seleccionado un proceso y al menos una DLL para llevar a cabo la inyección.

Herramientas de análisis

DLL_Injector

- La sección *status* muestra los mensajes para indicar al usuario si falta seleccionar un proceso, la DLL o si la inyección se realizó correctamente.

Herramientas de análisis

DLL_Shot

- Herramienta programada en C# con interfaz gráfica para identificar DLLs inyectadas o cargadas en cualquier proceso.

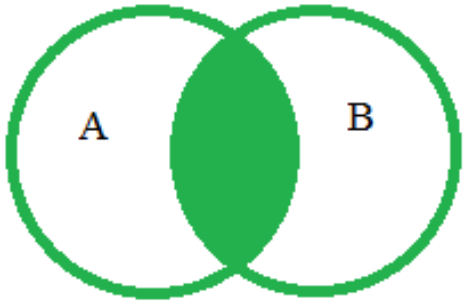
Herramientas de análisis

DLL_Shot

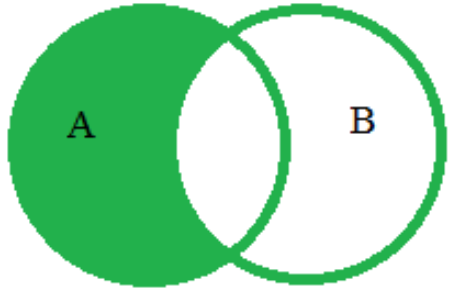
- Lo anterior, es mediante la comparación de las Bibliotecas de Enlace Dinámico activas en el sistema antes y después de la ejecución de *malware* o de la inyección DLL.

Herramientas de análisis

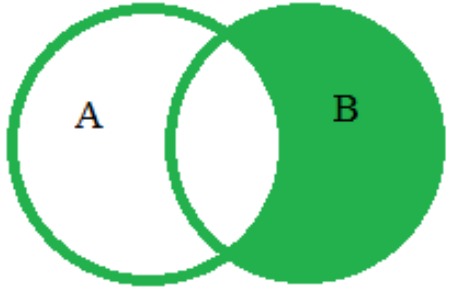
DLL_Shot



A ∩ B
DLLs sin cambios



A - B
DLLs removidas



B - A
DLLs agregadas

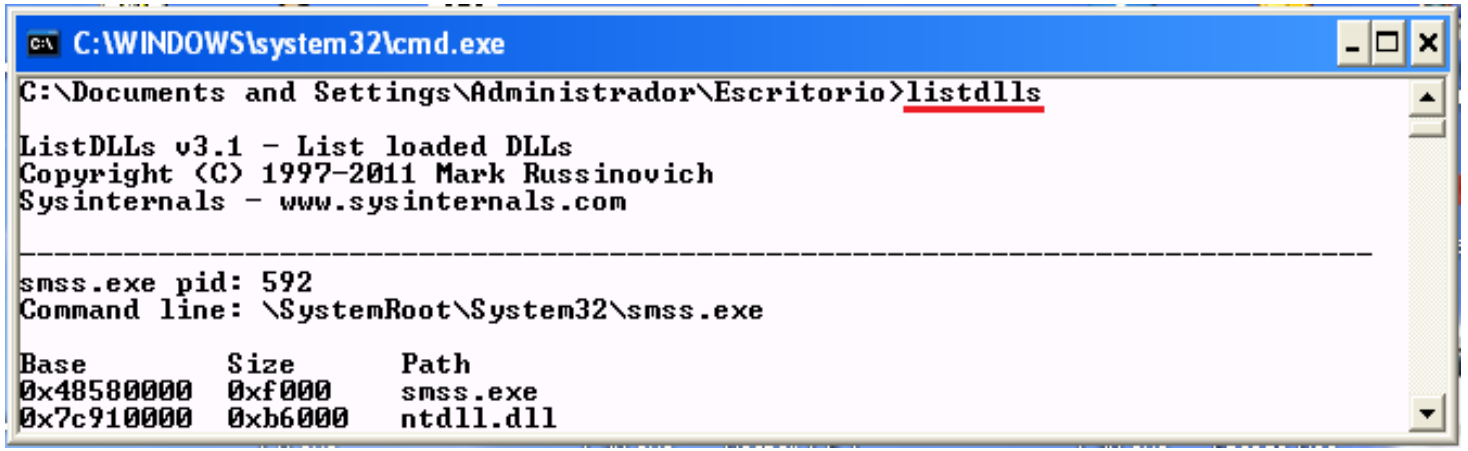
Herramientas de análisis

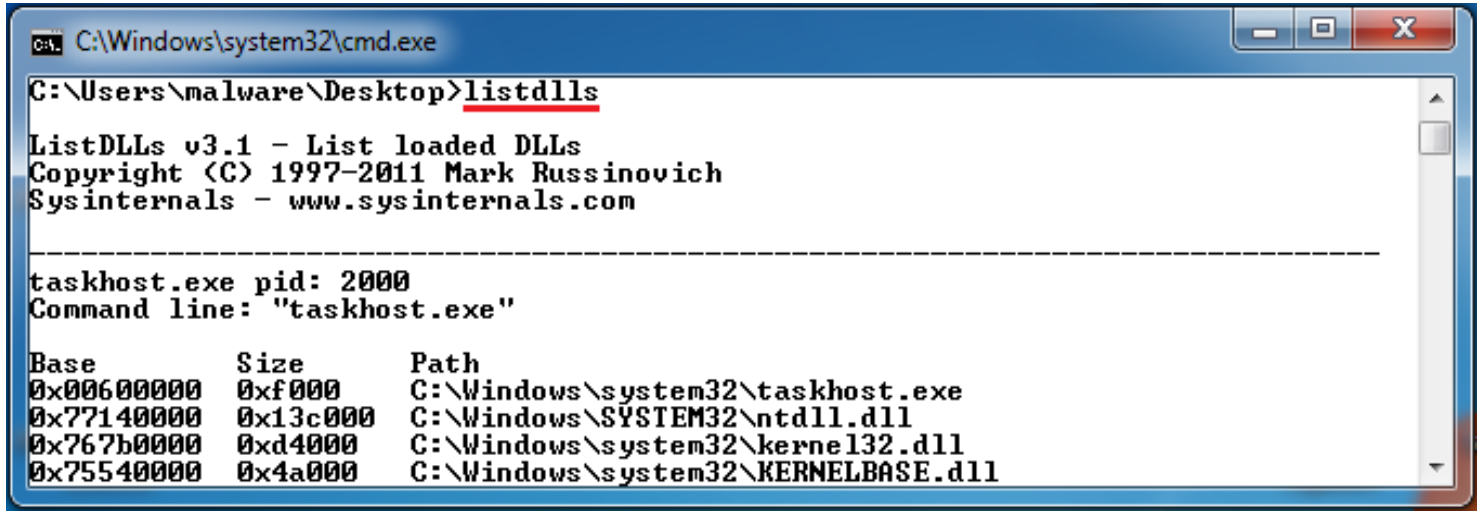
DLL_Shot

- Usa expresiones regulares para identificar:
  - El nombre de cada proceso junto con PID.
  - Las DLLs dependiendo el sistema operativo, puesto que la salida en Windows XP difiere con Windows 7 y 8.1.

Herramientas de análisis

DLL_Shot





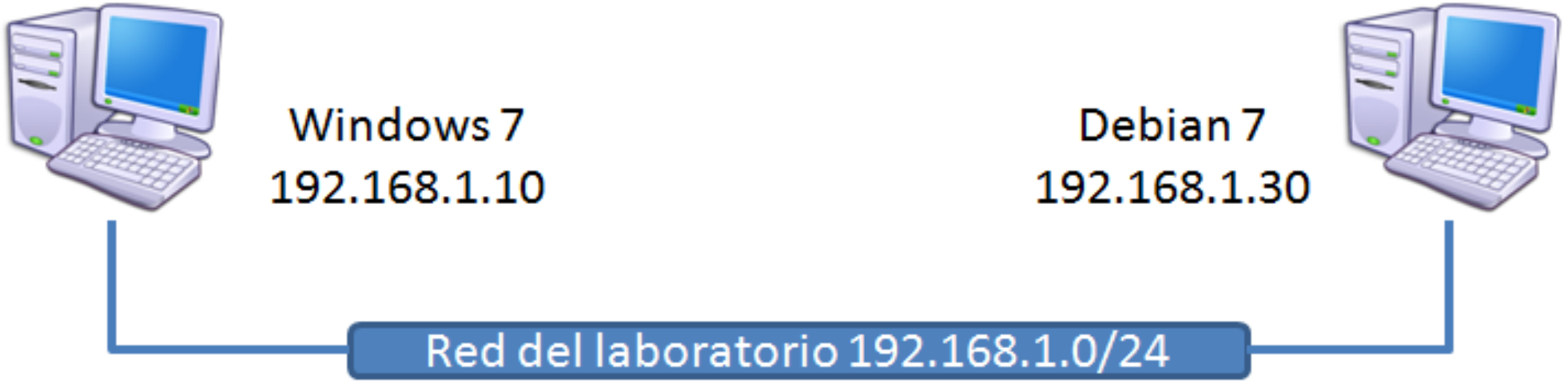
Herramientas de análisis

DLL_Shot

- La comparación de ambos estados se imprime directamente en un proceso del “Bloc de notas” con la finalidad de no modificar el Sistema de archivos de Windows.

Análisis de DLLs maliciosas

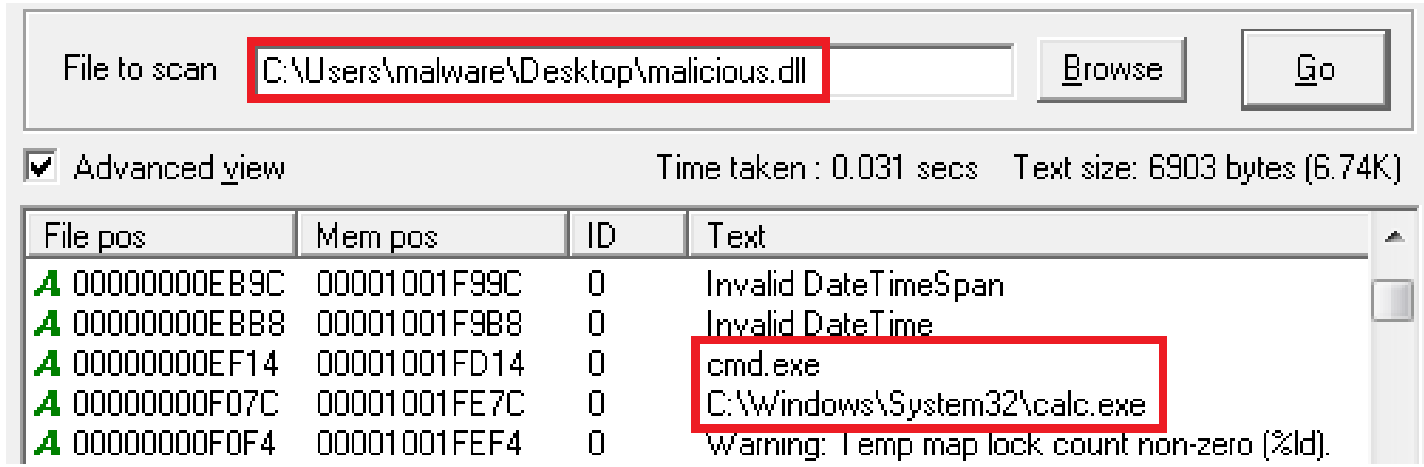
Laboratorio



Análisis de DLLs maliciosas

1) Realizar inspección de cadenas.

Se muestra cmd.exe y calc.exe

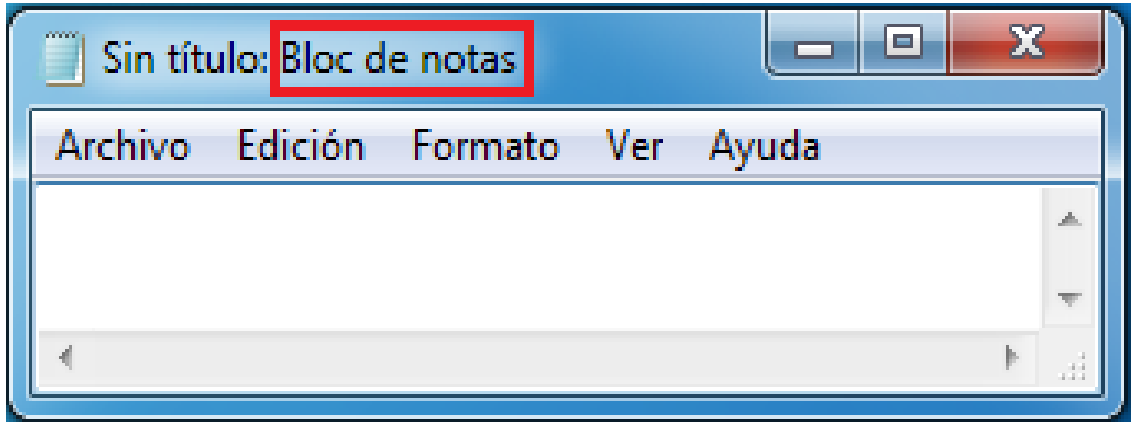


Hay varias posibilidades...

Coloquio de proyectos de Becarios en Seguridad Informática 3er

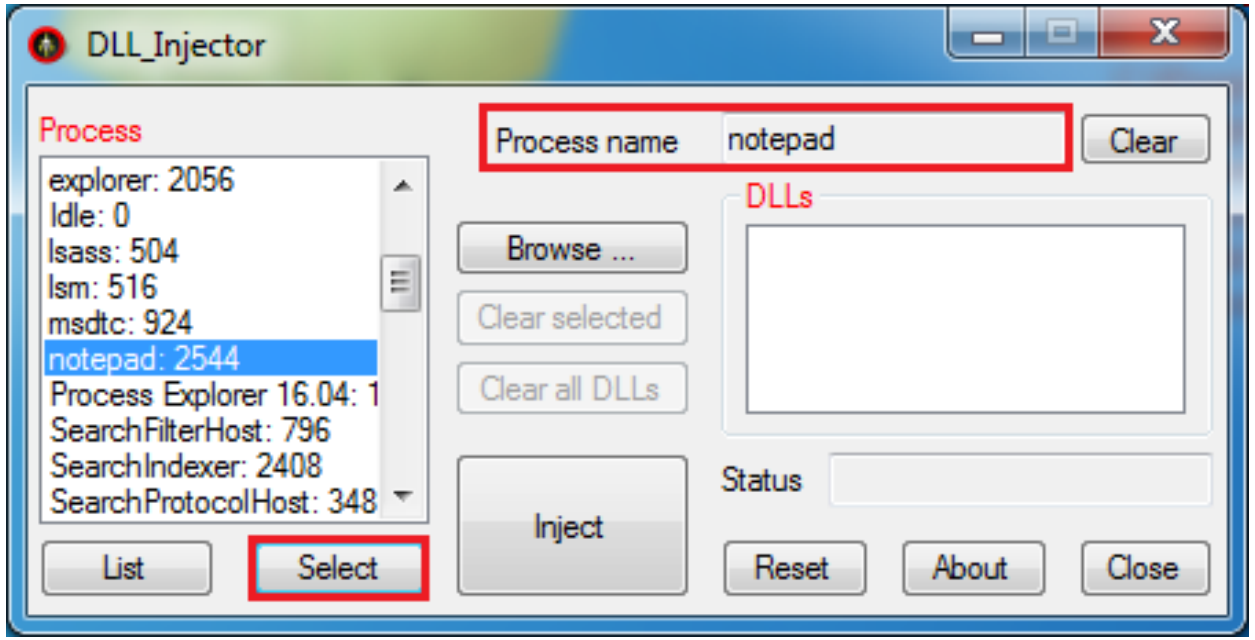
Análisis de DLLs maliciosas

2) Ejecutar el programa en el cual se inyectará la DLL maliciosa.



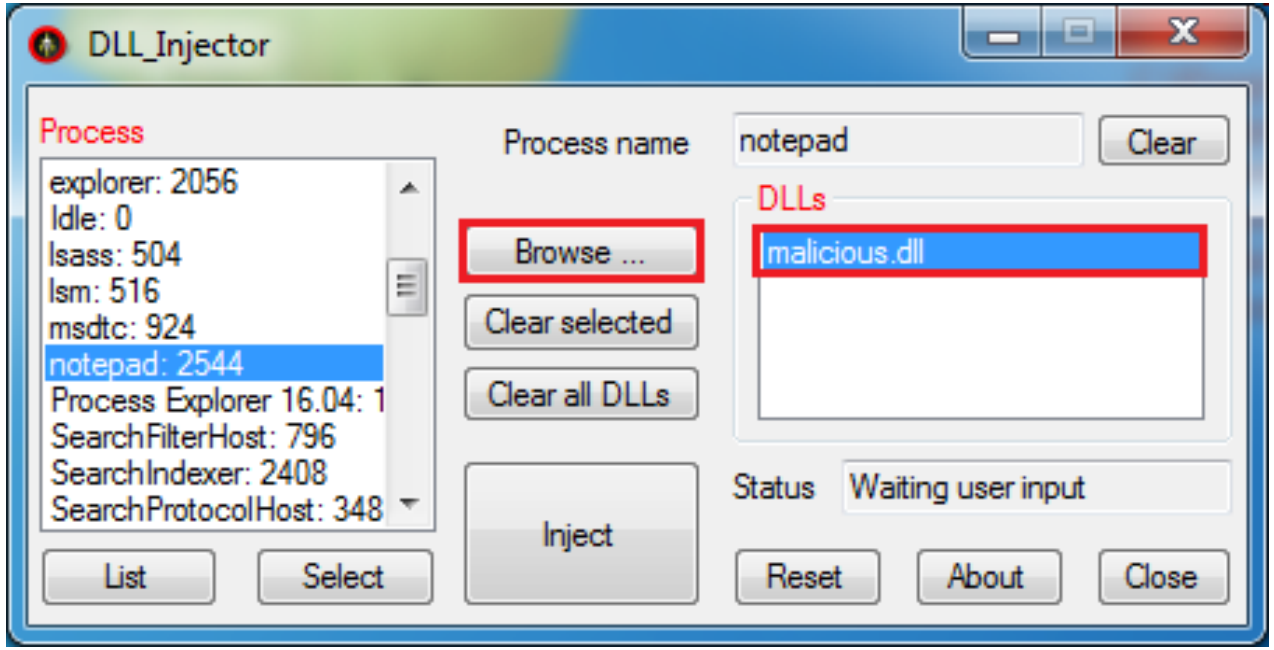
Análisis de DLLs maliciosas

3) Mostrar los procesos del sistema con el botón ***List*** y seleccionar el proceso objetivo en el **DLL_Injector**.



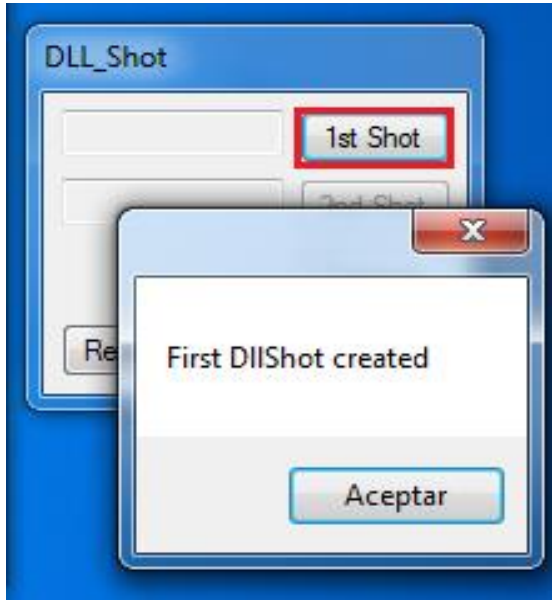
Análisis de DLLs maliciosas

4) Buscar la DLL maliciosa con el botón ***Browse ...***



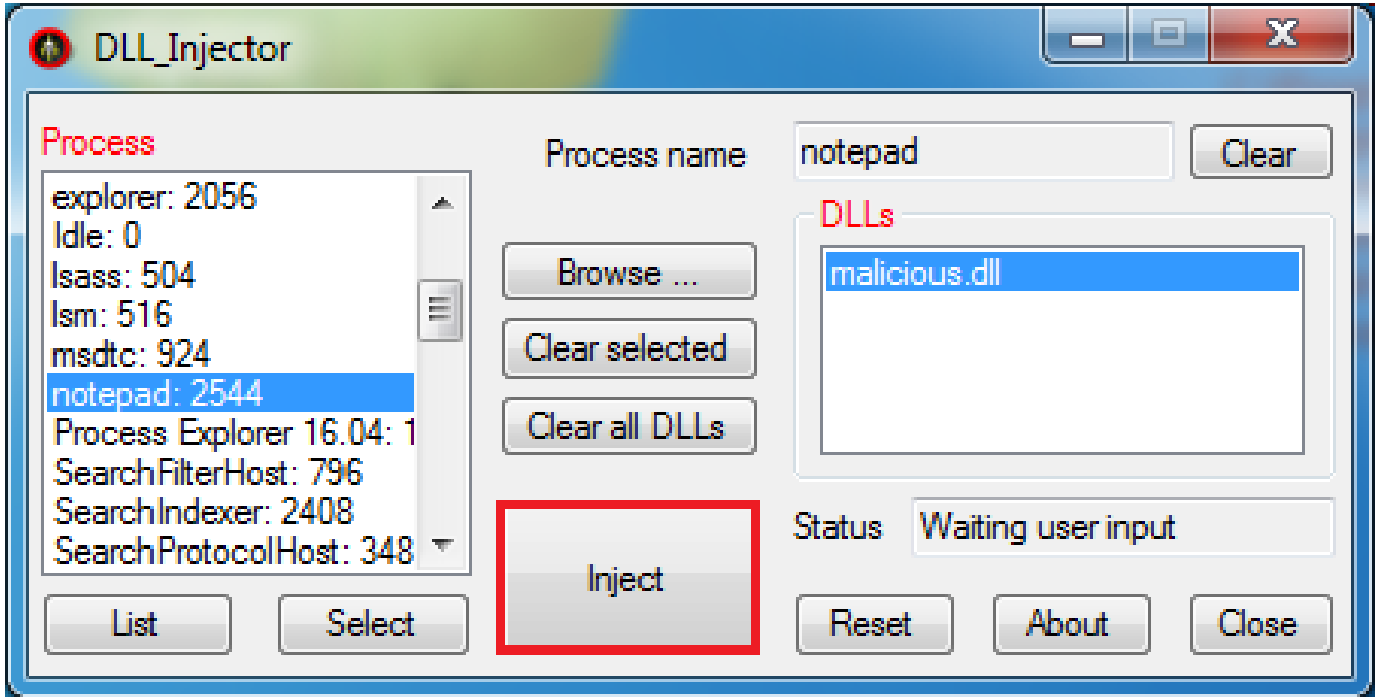
Análisis de DLLs maliciosas

5) Tomar el primer *shot* con la herramienta **DLL_Shot**.



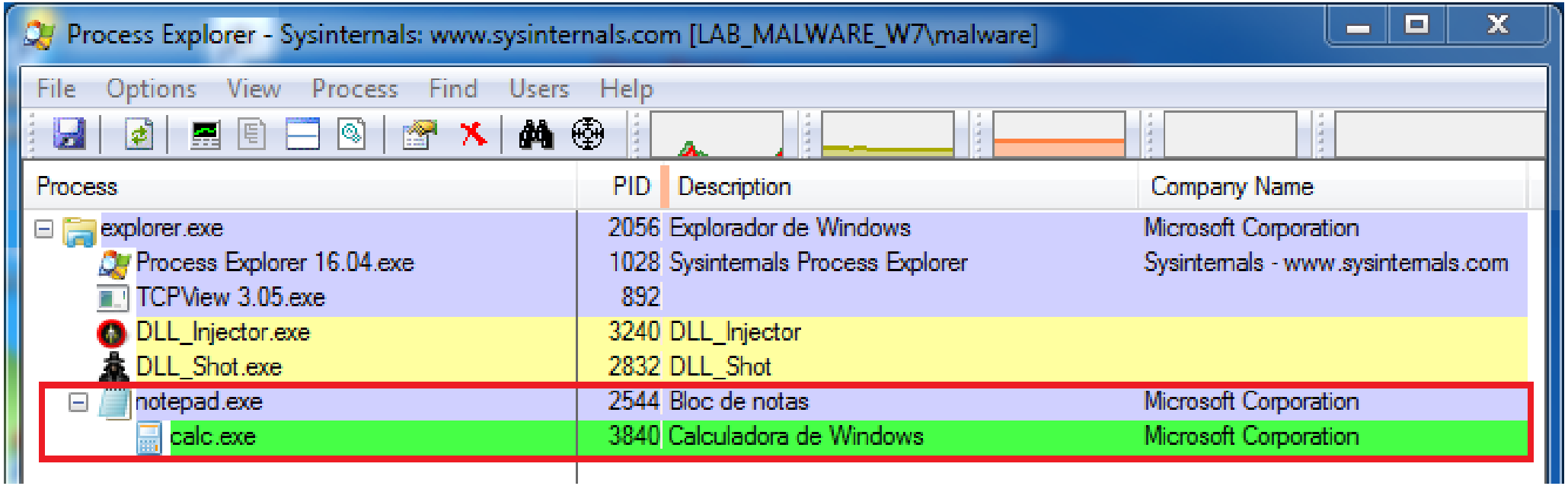
Análisis de DLLs maliciosas

6) Inyectar la DLL en el proceso objetivo.

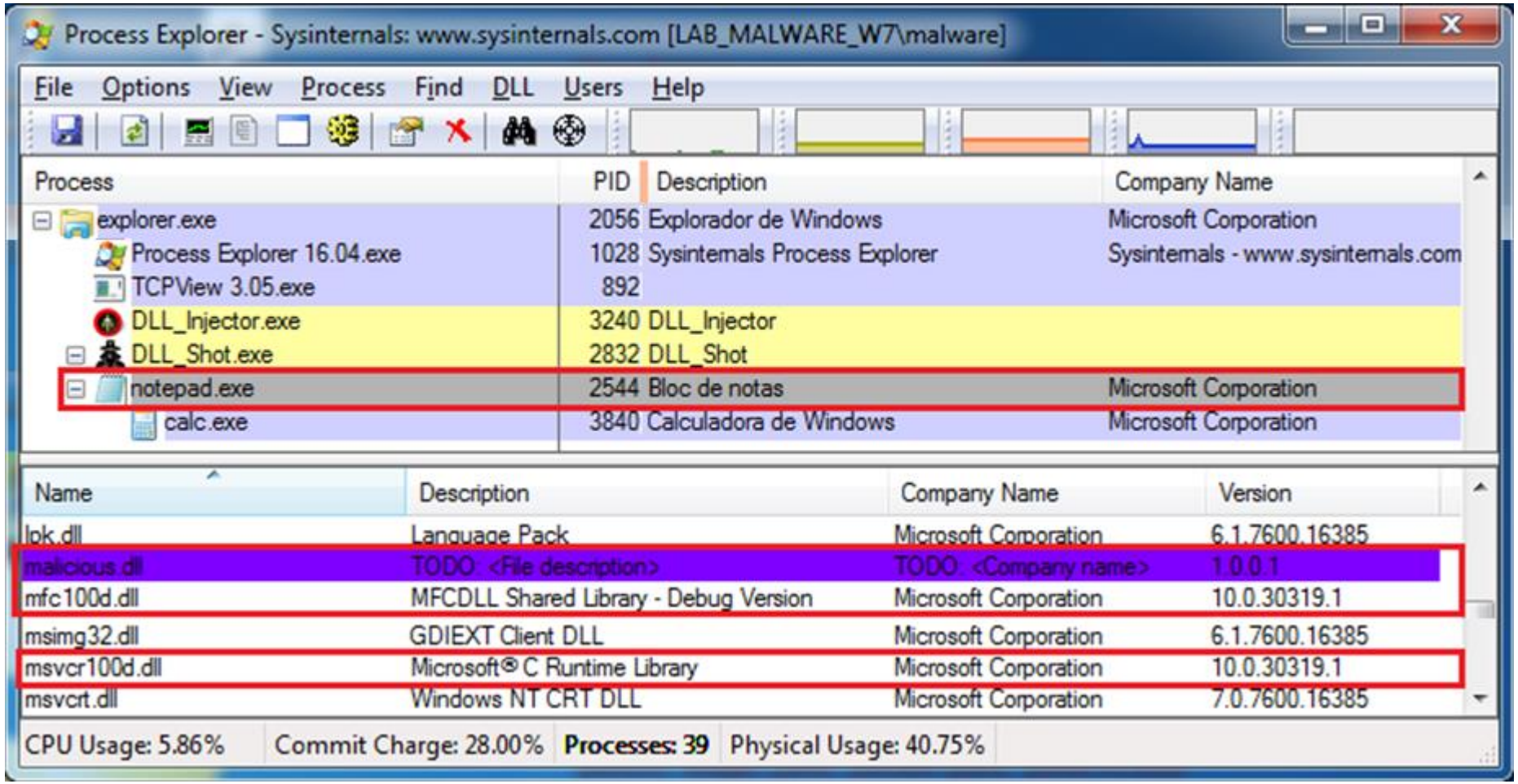


Análisis de DLLs maliciosas

7) Observar la actividad de procesos.

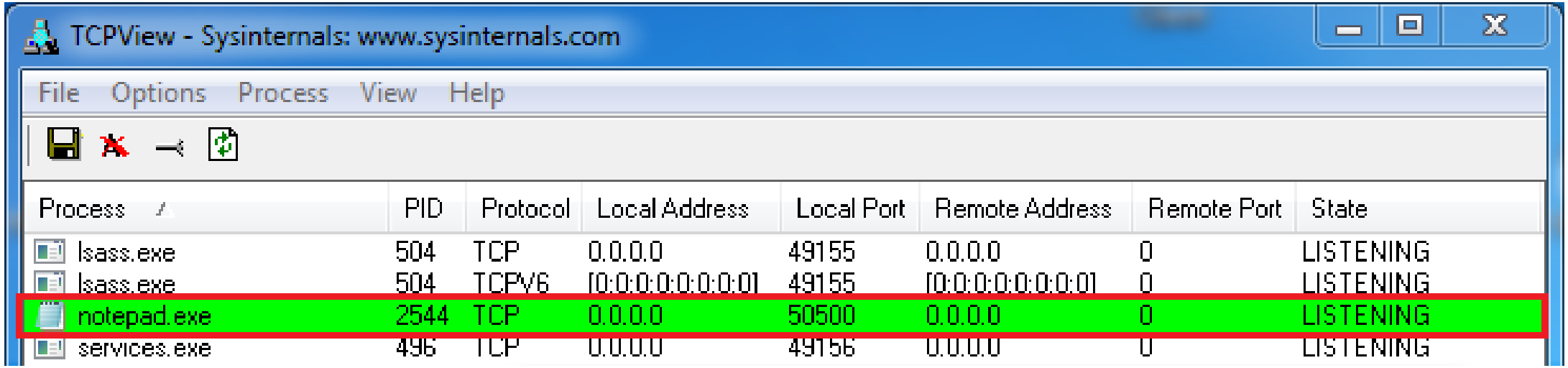


Análisis de DLLs maliciosas



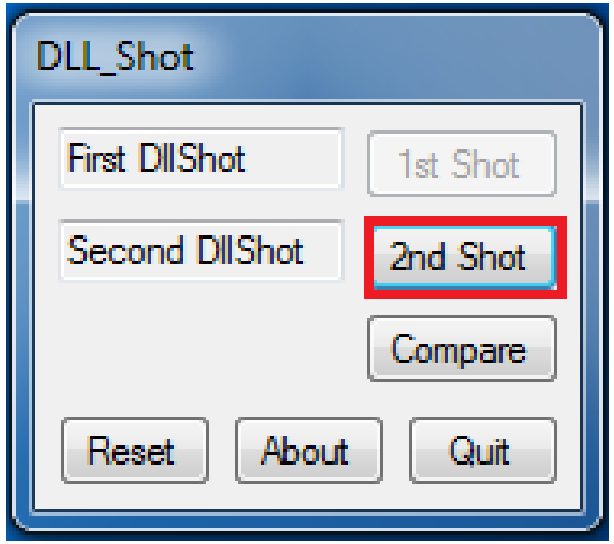
Análisis de DLLs maliciosas

8) Observar la actividad de red.



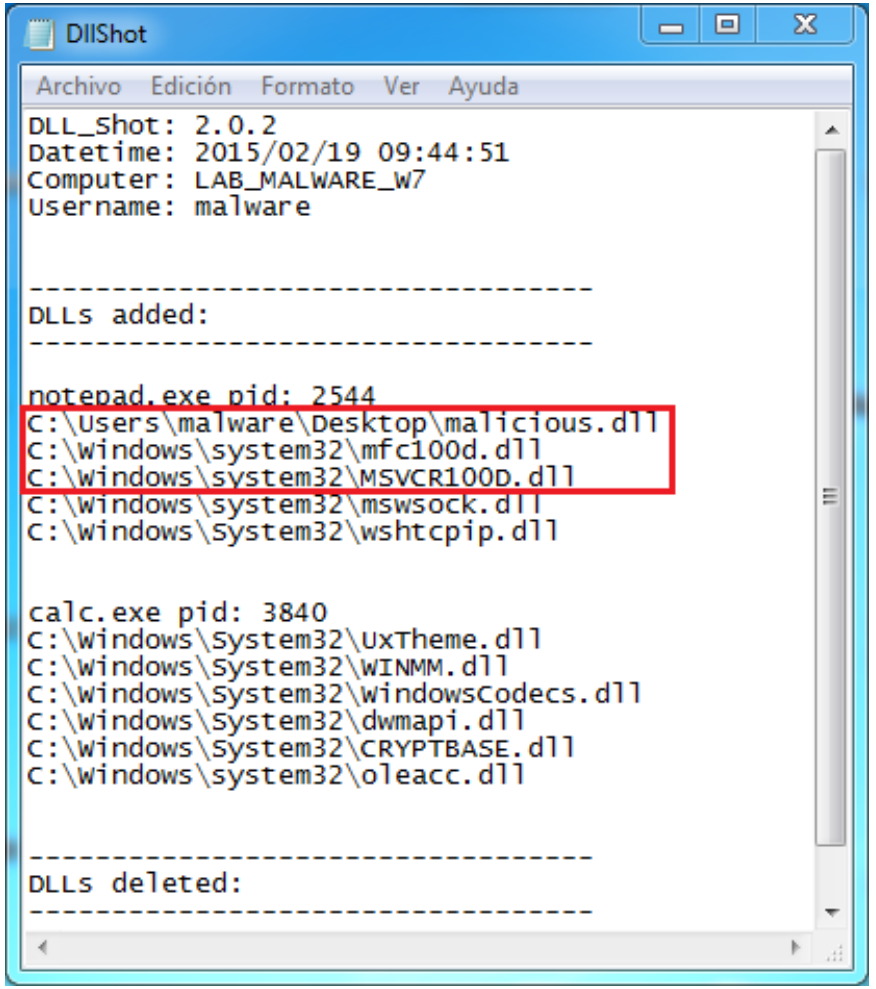
Análisis de DLLs maliciosas

9) Tomar el segundo *shot*.



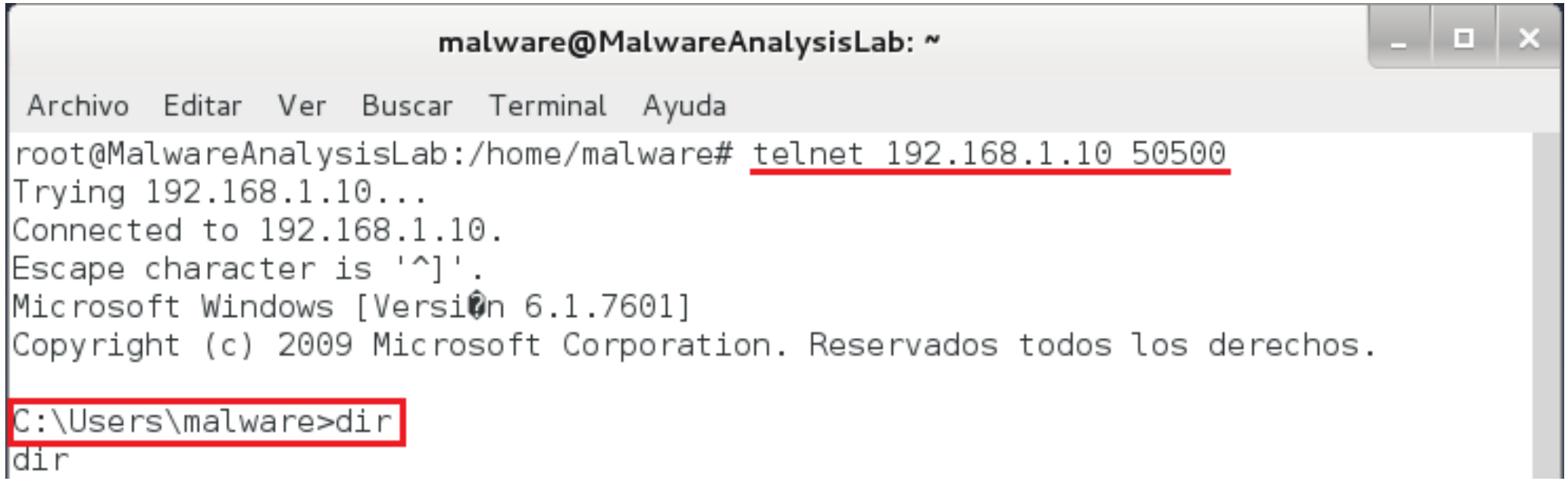
Análisis de DLLs maliciosas

10) Comparar resultados.



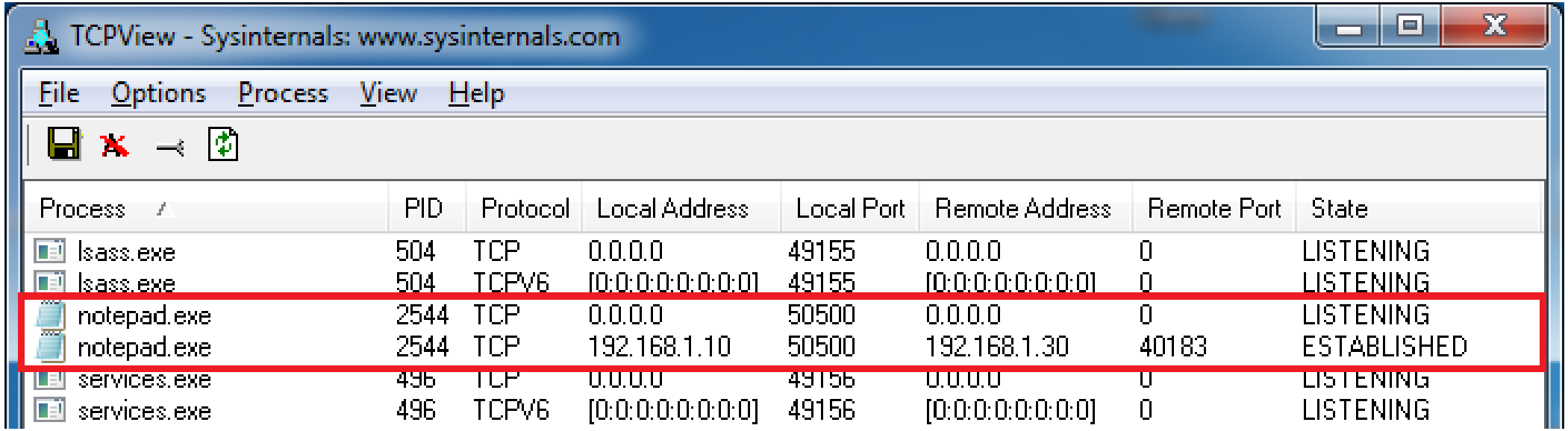
Análisis de DLLs maliciosas

- Verificar el servicio asociado al puerto local 50500 que implementa la DLL maliciosa.



Análisis de DLLs maliciosas

- Se establece una conexión de red al puerto 50500 y otra instancia del proceso objetivo se queda en modo escucha:



Conclusiones

Ventajas:

- Análisis de varias DLLs sospechosas al mismo tiempo.
- Registro de DLLs cargadas en nuevos procesos o inyectadas.
- Identificación de procesos objetivo por PID.
- No modifican el sistema de archivos.
- Registro de procesos terminados.

Limitaciones:

- DLL_Shot no captura actividad intermedia.
  - ✓ Complementar con Process Monitor.
- DLL_Injector puede ser clasificado como malicioso.
- Uso de Microsoft .Net Framework 2.0.
  - ✓ Instalarlo previamente.

Ing. Jonathan Banfi Vázquez

CSI/UNAM-CERT

56 22 81 69

jonathan.banfi@cert.unam.com