

Coloquio de proyectos
de Becarios en Seguridad Informática

3^{er}

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*)

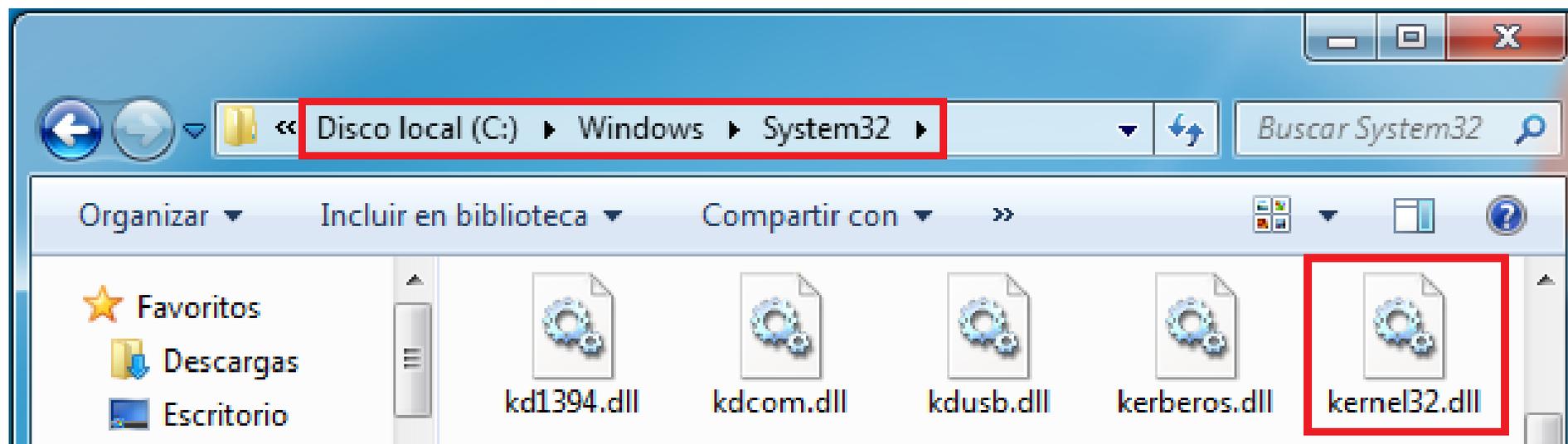
- Archivos que contienen funciones que se ejecutan por solicitud de algún proceso.



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

Introducción

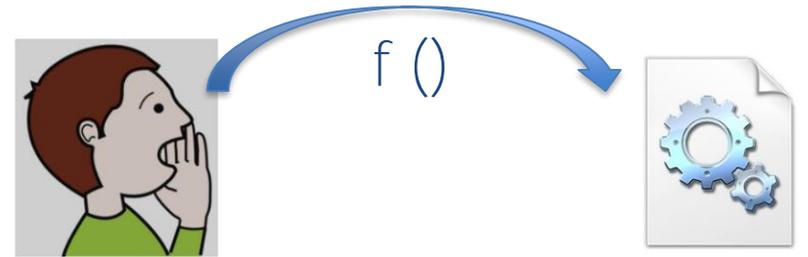
DLL (*Dynamic Library Link*)



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

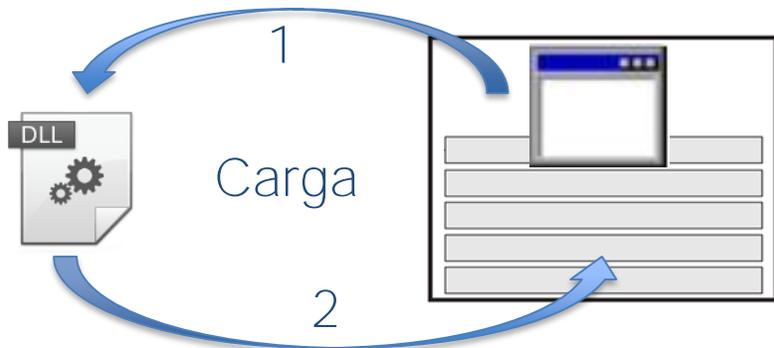
- Tienden a ser ejecutables muy pequeños.
- Pueden pasar desapercibidos ante motores de detección de software malicioso.



Introducción

Inyección de DLLs

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



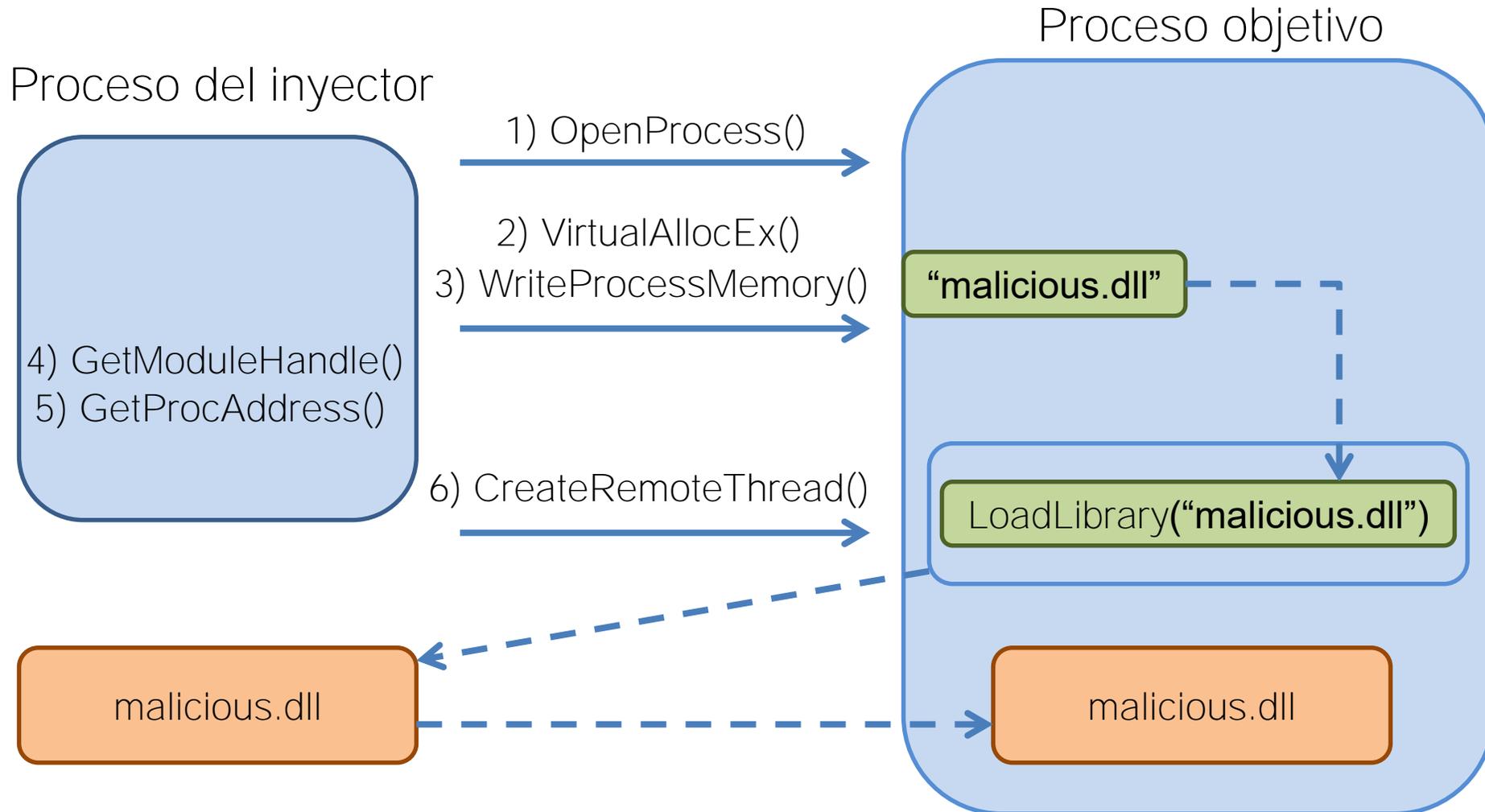
Introducción

Inyección de DLLs

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



Introducción



Herramientas de análisis

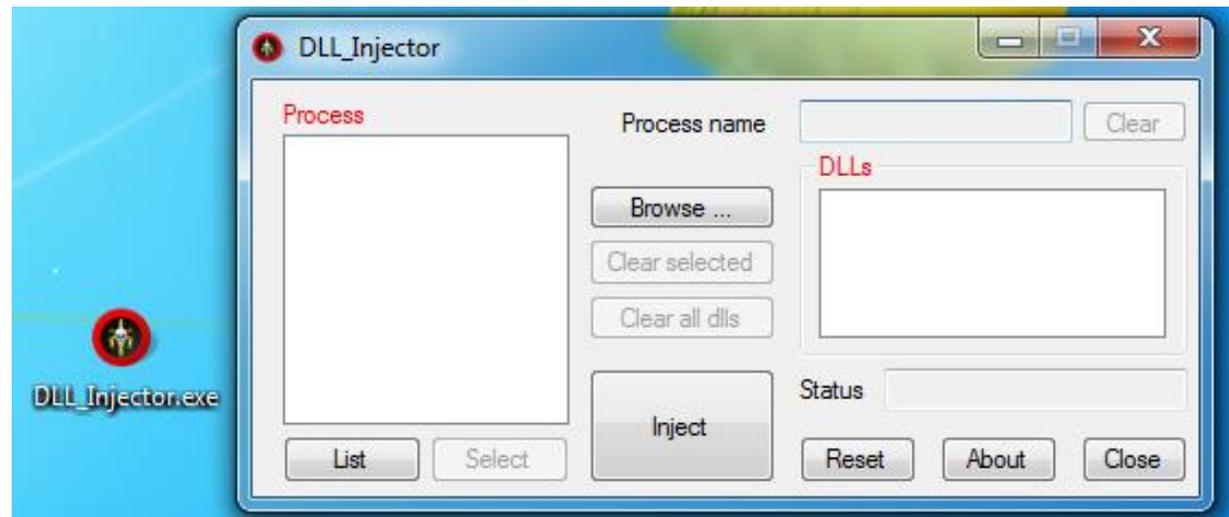
- A continuación se mostrarán dos herramientas que ayudan a realizar análisis dinámico de DLLs maliciosas:



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.



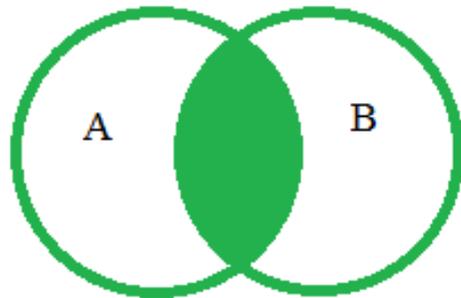
Herramientas de análisis

DLL_Shot

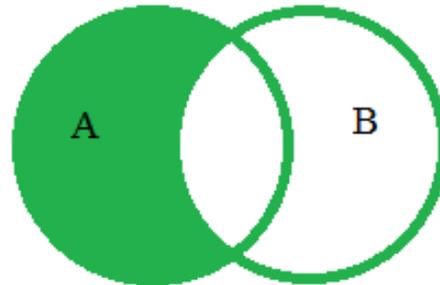
- Lo anterior, es mediante la comparación de las Bibliotecas de Enlace Dinámico activas en el sistema antes y después de la ejecución de *malware* o de la inyección DLL.

Herramientas de análisis

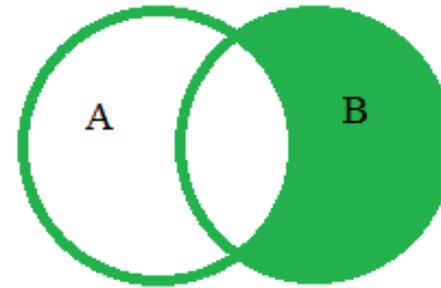
DLL_Shot



$A \cap B$
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

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrador\Escritorio>listdlls

ListDLLs v3.1 - List loaded DLLs
Copyright (C) 1997-2011 Mark Russinovich
Sysinternals - www.sysinternals.com

-----

smss.exe pid: 592
Command line: \SystemRoot\System32\smss.exe

Base      Size      Path
0x48580000 0xf000    smss.exe
0x7c910000 0xb6000   ntdll.dll
  
```

```

C:\Windows\system32\cmd.exe
C:\Users\malware\Desktop>listdlls

ListDLLs v3.1 - List loaded DLLs
Copyright (C) 1997-2011 Mark Russinovich
Sysinternals - www.sysinternals.com

-----

taskhost.exe pid: 2000
Command line: "taskhost.exe"

Base      Size      Path
0x00600000 0xf000    C:\Windows\system32\taskhost.exe
0x77140000 0x13c000  C:\Windows\SYSTEM32\ntdll.dll
0x767b0000 0xd4000   C:\Windows\system32\kernel32.dll
0x75540000 0x4a000   C:\Windows\system32\KERNELBASE.dll
  
```

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



Windows 7
192.168.1.10

Debian 7
192.168.1.30



Red del laboratorio 192.168.1.0/24

Análisis de DLLs maliciosas

1) Realizar inspección de cadenas.

Se muestra cmd.exe y calc.exe



File to scan: C:\Users\malware\Desktop\malicious.dll

Advanced view Time taken : 0.031 secs Text size: 6903 bytes (6.74K)

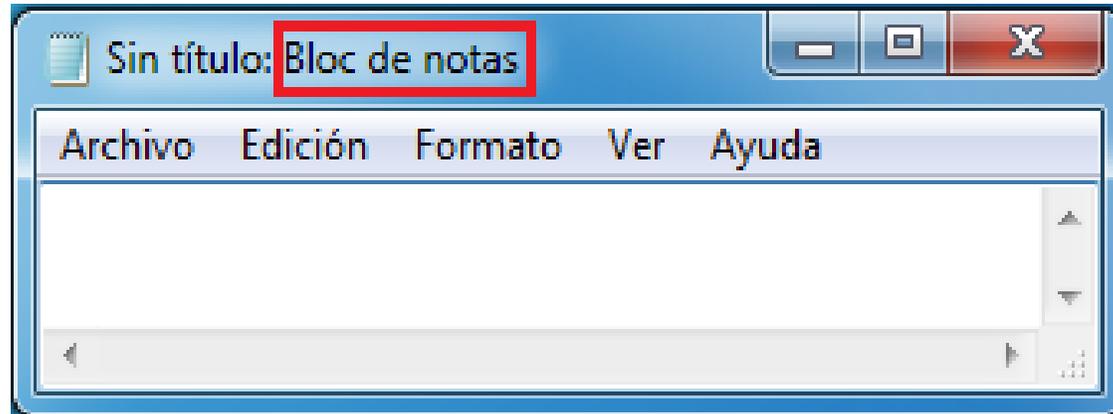
File pos	Mem pos	ID	Text
A 00000000EB9C	00001001F39C	0	Invalid DateTimeSpan
A 00000000EBB8	00001001F3B8	0	Invalid DateTime
A 00000000EF14	00001001FD14	0	cmd.exe
A 00000000F07C	00001001FE7C	0	C:\Windows\System32\calc.exe
A 00000000F0F4	00001001FEF4	0	Warning: Temp map lock count non-zero (%ld).

Hay varias posibilidades...



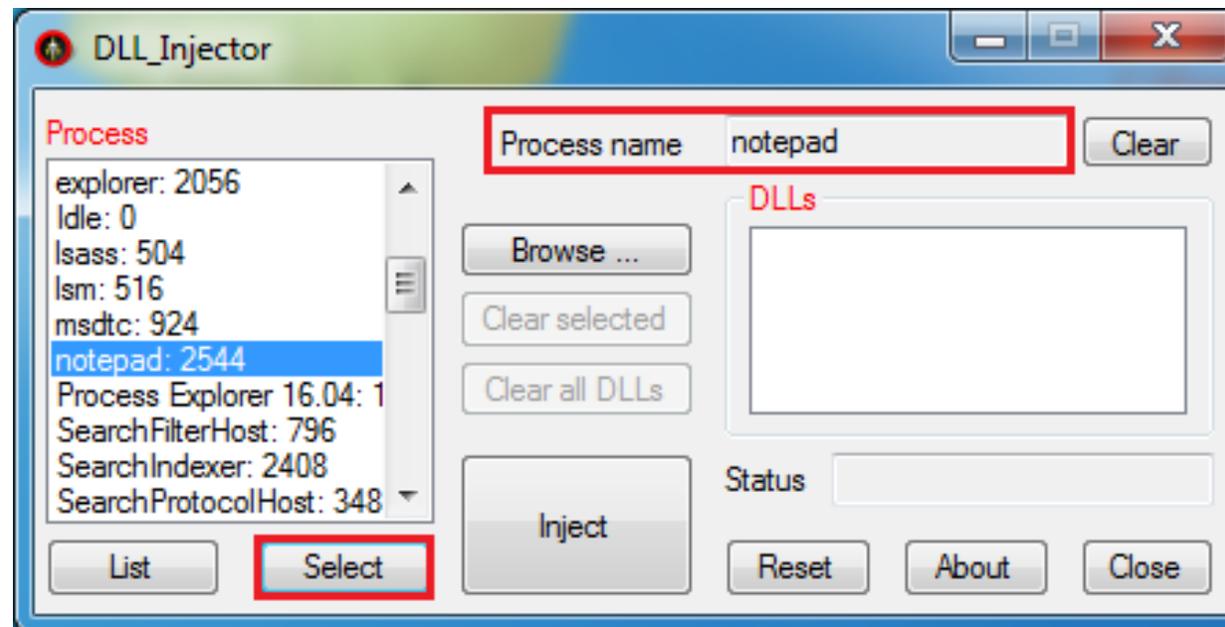
Análisis de DLLs maliciosas

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



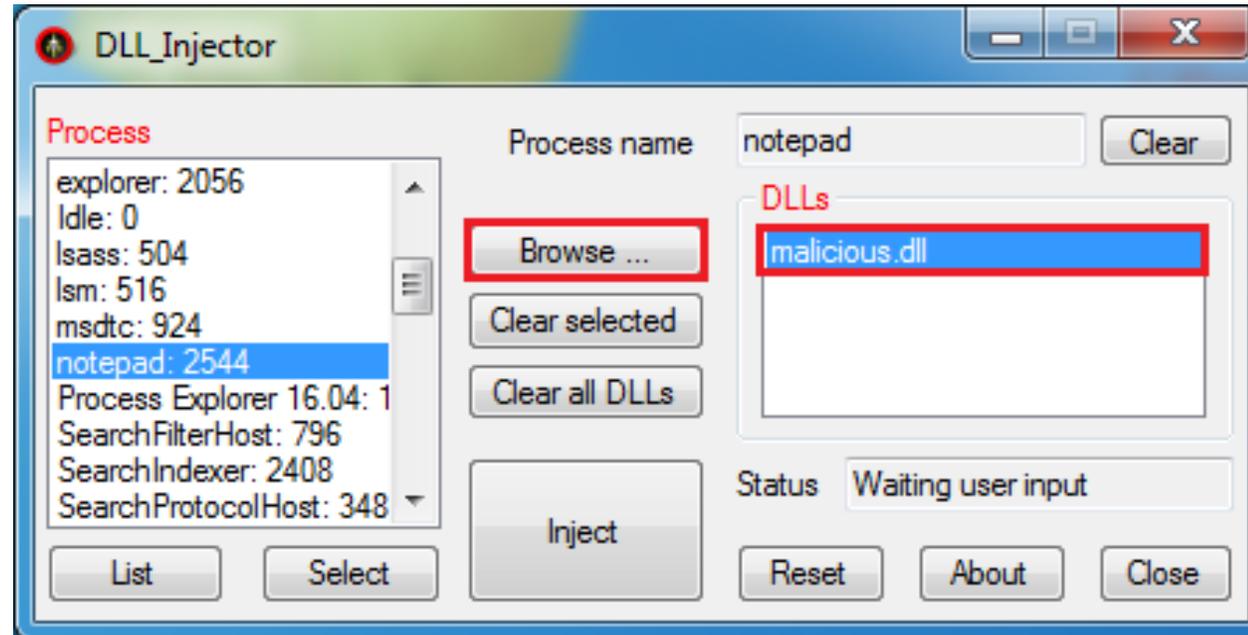
Análisis de DLLs maliciosas

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



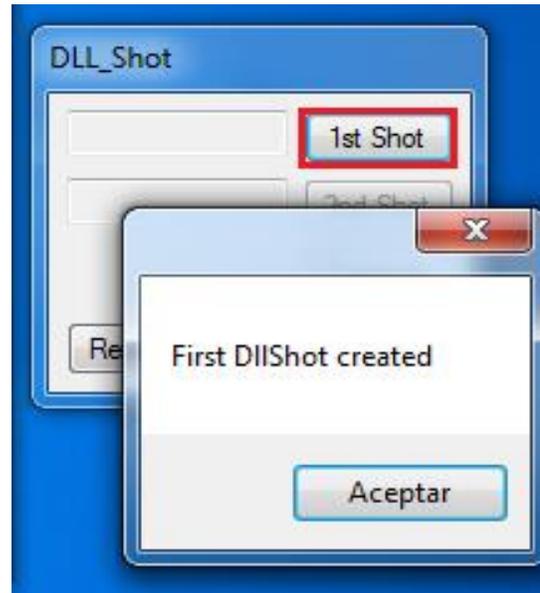
Análisis de DLLs maliciosas

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



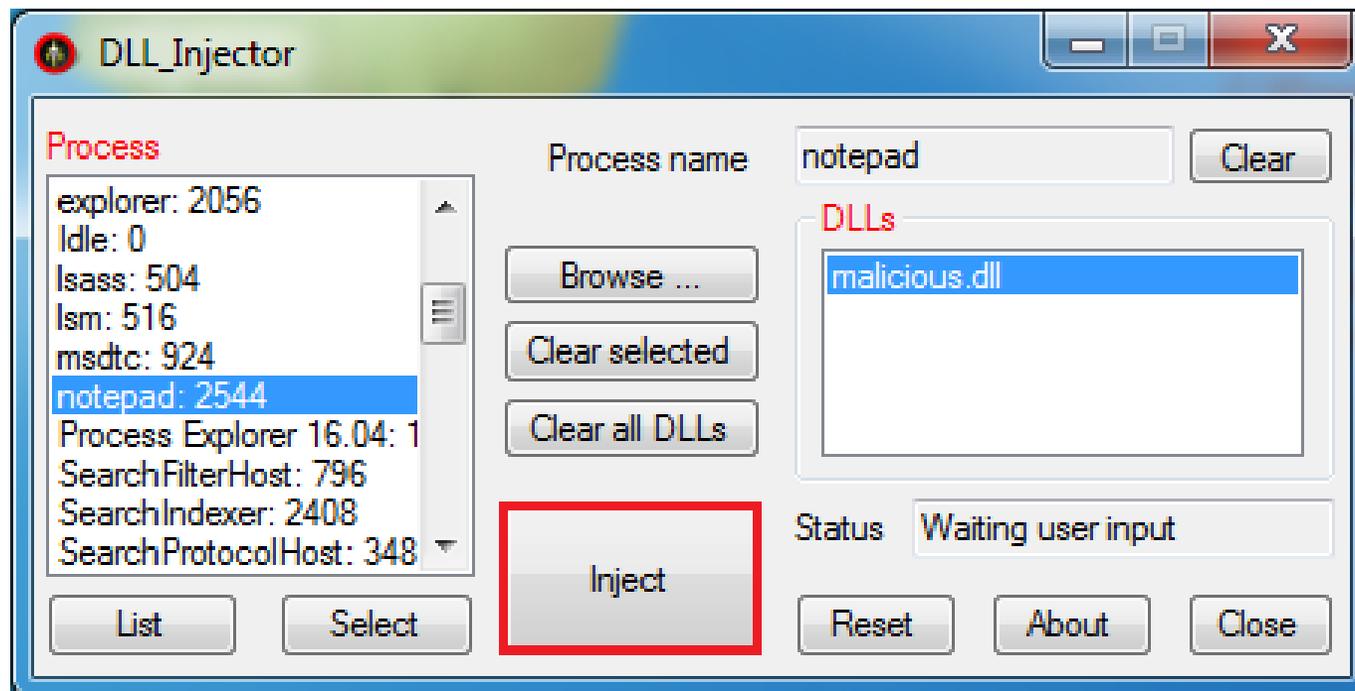
Análisis de DLLs maliciosas

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



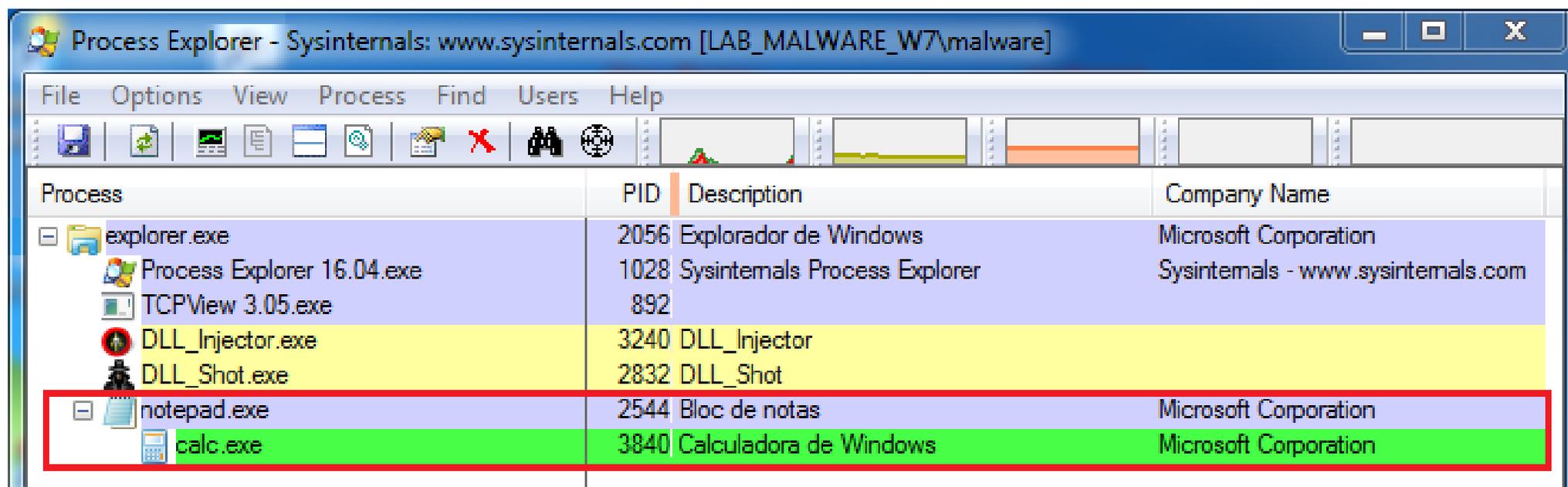
Análisis de DLLs maliciosas

6) Inyectar la DLL en el proceso objetivo.



Análisis de DLLs maliciosas

7) Observar la actividad de procesos.



Process	PID	Description	Company Name
explorer.exe	2056	Explorador de Windows	Microsoft Corporation
Process Explorer 16.04.exe	1028	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com
TCPView 3.05.exe	892		
DLL_Injector.exe	3240	DLL_Injector	
DLL_Shot.exe	2832	DLL_Shot	
notepad.exe	2544	Bloc de notas	Microsoft Corporation
calc.exe	3840	Calculadora de Windows	Microsoft Corporation

Análisis de DLLs maliciosas

Process Explorer - Sysinternals: www.sysinternals.com [LAB_MALWARE_W7\malware]

File Options View Process Find DLL Users Help

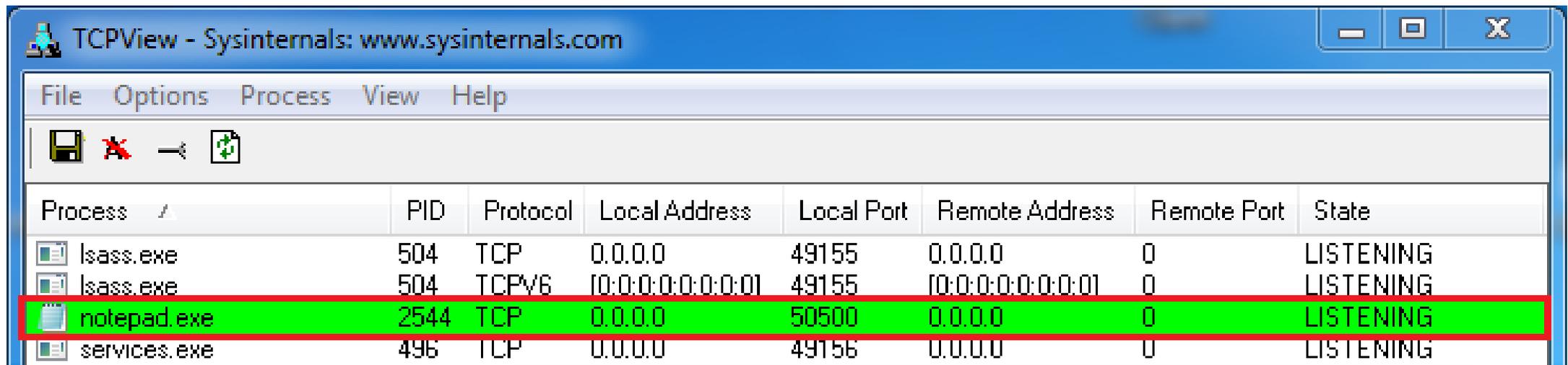
Process	PID	Description	Company Name
explorer.exe	2056	Explorador de Windows	Microsoft Corporation
Process Explorer 16.04.exe	1028	Sysinternals Process Explorer	Sysinternals - www.sysinternals.com
TCPView 3.05.exe	892		
DLL_Injector.exe	3240	DLL_Injector	
DLL_Shot.exe	2832	DLL_Shot	
notepad.exe	2544	Bloc de notas	Microsoft Corporation
calc.exe	3840	Calculadora de Windows	Microsoft Corporation

Name	Description	Company Name	Version
lok.dll	Language Pack	Microsoft Corporation	6.1.7600.16385
malicious.dll	TODO: <File description>	TODO: <Company name>	1.0.0.1
mfc100d.dll	MFC DLL Shared Library - Debug Version	Microsoft Corporation	10.0.30319.1
msimg32.dll	GDIEXT Client DLL	Microsoft Corporation	6.1.7600.16385
msvcr100d.dll	Microsoft® C Runtime Library	Microsoft Corporation	10.0.30319.1
msvcr7.dll	Windows NT CRT DLL	Microsoft Corporation	7.0.7600.16385

CPU Usage: 5.86% Commit Charge: 28.00% Processes: 39 Physical Usage: 40.75%

Análisis de DLLs maliciosas

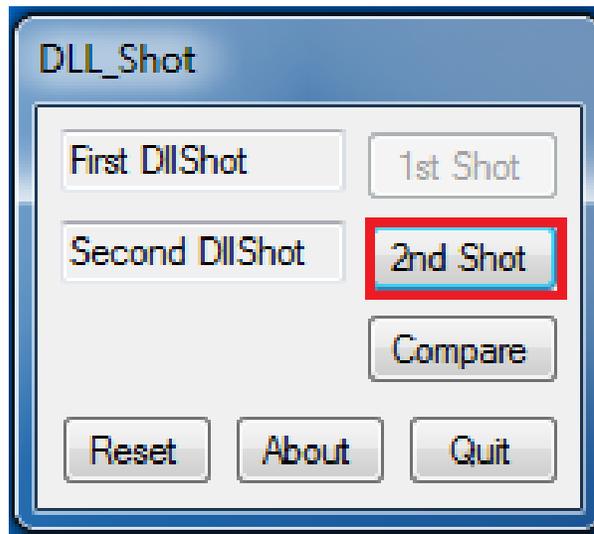
8) Observar la actividad de red.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	504	TCP	0.0.0.0	49155	0.0.0.0	0	LISTENING
lsass.exe	504	TCPV6	[0:0:0:0:0:0:0:0]	49155	[0:0:0:0:0:0:0:0]	0	LISTENING
notepad.exe	2544	TCP	0.0.0.0	50500	0.0.0.0	0	LISTENING
services.exe	496	TCP	0.0.0.0	49156	0.0.0.0	0	LISTENING

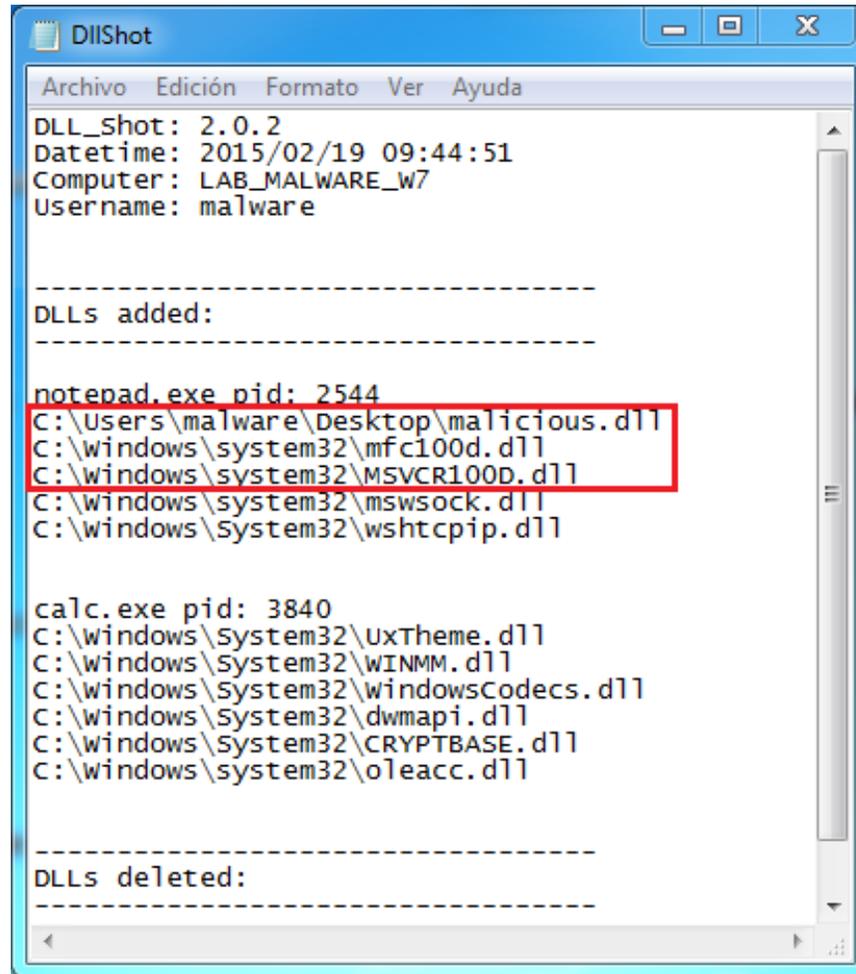
Análisis de DLLs maliciosas

9) Tomar el segundo *shot*.



Análisis de DLLs maliciosas

10) Comparar resultados.



```
DIIShot
Archivo Edición Formato Ver Ayuda
DLL_Shot: 2.0.2
Datetime: 2015/02/19 09:44:51
Computer: LAB_MALWARE_w7
Username: malware

-----
DLLs added:
-----
notepad.exe pid: 2544
C:\Users\malware\Desktop\malicious.dll
C:\windows\system32\mfcm100d.dll
C:\windows\system32\MSVCR100D.dll
C:\windows\system32\mswsock.dll
C:\windows\system32\wshtcpip.dll

calc.exe pid: 3840
C:\windows\system32\uxTheme.dll
C:\windows\system32\WINMM.dll
C:\windows\system32\windowsCodecs.dll
C:\windows\system32\dwmapi.dll
C:\windows\system32\CRYPTBASE.dll
C:\windows\system32\oleacc.dll

-----
DLLs deleted:
-----
```

Análisis de DLLs maliciosas

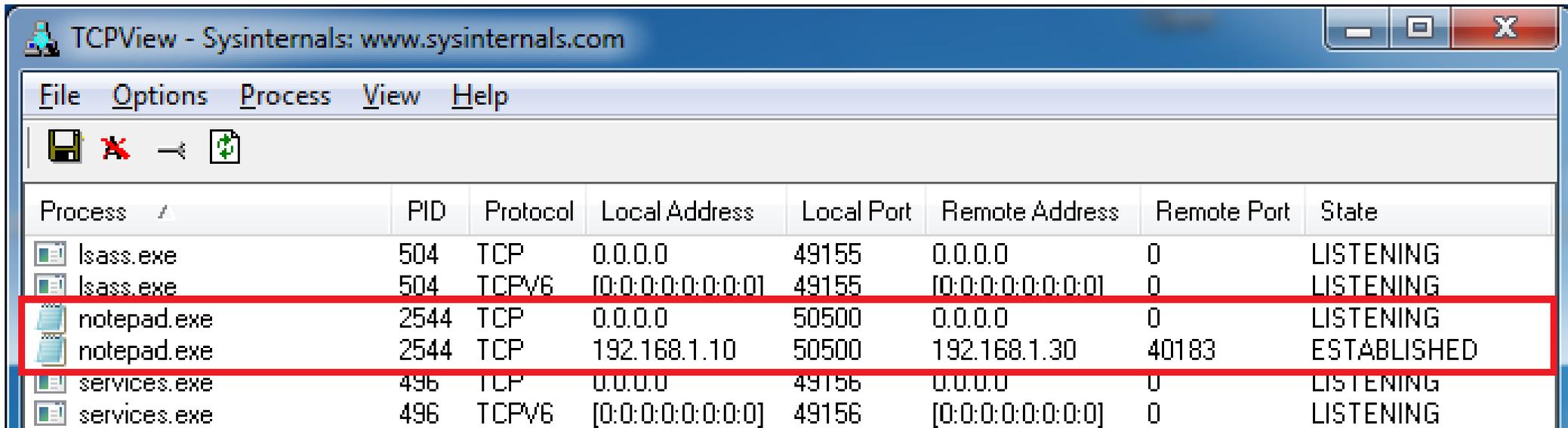
- Verificar el servicio asociado al puerto local 50500 que implementa la DLL maliciosa.

```
malware@MalwareAnalysisLab: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@MalwareAnalysisLab:/home/malware# telnet 192.168.1.10 50500
Trying 192.168.1.10...
Connected to 192.168.1.10.
Escape character is '^]'.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\malware>dir
dir
```

Análisis de DLLs maliciosas

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



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
lsass.exe	504	TCP	0.0.0.0	49155	0.0.0.0	0	LISTENING
lsass.exe	504	TCPV6	[0:0:0:0:0:0:0:0]	49155	[0:0:0:0:0:0:0:0]	0	LISTENING
notepad.exe	2544	TCP	0.0.0.0	50500	0.0.0.0	0	LISTENING
notepad.exe	2544	TCP	192.168.1.10	50500	192.168.1.30	40183	ESTABLISHED
services.exe	496	TCP	0.0.0.0	49156	0.0.0.0	0	LISTENING
services.exe	496	TCPV6	[0:0:0:0:0:0:0:0]	49156	[0:0:0:0:0:0:0:0]	0	LISTENING

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

