

Análisis de malware

Análisis dinámico básico

Gustavo Romero López - gustavo@ugr.es

Updated: 3 de marzo de 2025

Departamento de Ingeniería de Computadores, Automática y Robótica

Por donde vamos...

Parte 1: Análisis básico

Capítulo 1: Técnicas estáticas básicas

Capítulo 2: Análisis de malware en máquinas virtuales

Capítulo 3: Análisis dinámico básico

Parte 2: Análisis estático avanzado

Capítulo 4: Curso intensivo de ensamblador x86

Capítulo 5: IDA Pro

Capítulo 6: Reconocimiento de construcciones de C en ensamblador

Capítulo 7: Análisis de programas maliciosos para Windows

Parte 3: Análisis dinámico avanzado

Parte 4: Funcionalidad del malware

Parte 5: Anti-ingeniería inversa

Parte 6: Temas especiales

Lo que ya sabéis hacer...

Análisis estático:

- ⊙ Identificar ficheros: MD5, SHA1, SHA256,...
- ⊙ Antivirus: www.virustotal.com
- ⊙ Detección de empaquetado: PEid y UPX
- ⊙ Cadenas: strings
- ⊙ Formato PE:
 - PEview
 - Depends
 - objdump
 - Resource Hacker
- ⊙ Desensamblado: IDA Pro

Lo que os falta por aprender...

Análisis Dinámico:

- ⊙ Entorno seguro
 - sandbox: Cuckoo, Joe Sandbox, Microsoft Sandbox
 - máquina virtual: Gnome Boxes, VMware, VirtualBox
- ⊙ Process Monitor
- ⊙ Process Explorer
- ⊙ Regshot
- ⊙ ApateDNS + INetSim
- ⊙ Wireshark
- ⊙ Depuración:
 - OllyDbg/Immunity Debugger: modo usuario
 - Windbg: modos usuario y núcleo

- ⊙ Examen de la ejecución del malware.
- ⊙ El análisis estático puede acabar en un callejón sin salida...
 - ofuscado/empaquetado/cifrado
 - conocimientos insuficientes/exceso de dificultad
- ⊙ Observar el comportamiento del malware puede ser más eficaz y sencillo.
- ⊙ Podemos hacerlo de dos formas:
 - En vivo: monitorizar mientras se ejecuta.
 - A posteriori: comparar el sistema antes y después.
- ⊙ La mejor forma de averiguar que hace el malware.
- ⊙ Usar sólo después de un análisis estático básico.

Entorno aislado (“*SandBox*”)

- ⊙ Definición: mecanismo de seguridad para ejecutar programas en un entorno seguro.
- ⊙ Mejor cuanto más se parezca a un sistema real
- ⊙ Automatizan el proceso de rastreo de actividad y elaboran informes sobre el comportamiento del malware.
- ⊙ Ejemplos:
 - Cuckoo:
<https://cuckoosandbox.org/https://cuckoo.cert.ee>
 - Joe Sandbox: <https://www.joesecurity.org>
 - Microsoft Sandbox
- ⊙ Inconvenientes:
 - pueden ser detectados
 - vulnerabilidades en el anfitrión
 - sin opciones desde el intérprete de órdenes
 - sin interacción de red
 - diferencias con un sistema real: entorno, registro,...

Entorno aislado (“*SandBox*”)

- ⊙ Permite observar el la actividad del malware sobre....
 - procesos/hebras
 - sistema de ficheros
 - mutex
 - registro
 - red
 - antivirus
- ⊙ Inconvenientes:
 - no utiliza opciones de línea de órdenes
 - no registra todos los eventos por falta de tiempo
 - puede ser detectado por el malware
 - comportamiento anómalo por diferencias con un sistema real
 - no lanzamiento de DLLs
 - falta de conclusiones precisas

Ejecución de malware

Ejecutables (*.exe):

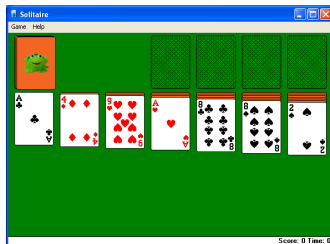
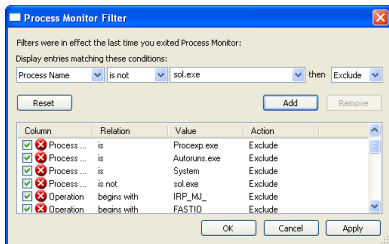
- ⦿ doble click desde un interfaz gráfico
- ⦿ ejecución desde el intérprete de órdenes:
`c:\virus.exe`

Bibliotecas de enlace dinámico (*.dll):

- ⦿ `c:\>rundll32.exe rip.dll, Install`
- ⦿ Convertir DLL en ejecutable cambiando su cabecera
- ⦿ Instalar DLL como un servicio y ejecutarlo
`c:\>rundll32.exe iprx32.dll, InstallService ServiceName`
`c:\>net start ServiceName`

Process Monitor

- Monitoriza: registro, sistema de ficheros, red y procesos.
- Genera tanta información que es vital filtrarla.
- Ejercicio: ¿Que hace el solitario de Windows?
 1. Arranca Process Monitor
 2. Detener la captura de eventos
 3. Crea el filtro:
“Process Name is not sol.exe then Exclude”
 4. Reactivar la captura de eventos
 5. Lanza el solitario



Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
1.23.20.3108884	sol.exe	2180	Process Start		SUCCESS	Parent PID: 1628, Command lin...
1.23.20.3108912	sol.exe	2180	Thread Create		SUCCESS	Thread ID: 2152
1.23.20.3183103	sol.exe	2180	QueryNameInformationFile	C:\WINDOWS\system32\sol.exe	SUCCESS	Name: \WINDOWS\system32\...
1.23.20.3184368	sol.exe	2180	Load Image	C:\WINDOWS\system32\sol.exe	SUCCESS	Image Base: 0x1000000, Imag...
1.23.20.3185268	sol.exe	2180	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7e900000, Imag...
1.23.20.3185363	sol.exe	2180	QueryNameInformationFile	C:\WINDOWS\system32\sol.exe	SUCCESS	Name: \WINDOWS\system32\...
1.23.20.3186380	sol.exe	2180	CreateFile	C:\WINDOWS\Prefetch\SOL.EXE-1C0C14EB.pf	NAME NOT FOUND	Desired Access: Generic Read...
1.23.20.3187807	sol.exe	2180	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec...	NAME NOT FOUND	Desired Access: Read
1.23.20.3188033	sol.exe	2180	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Read
1.23.20.3188282	sol.exe	2180	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\Control\Illegal...	NAME NOT FOUND	Length: 1.024
1.23.20.3196635	sol.exe	2180	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
1.23.20.3197856	sol.exe	2180	CreateFile	C:\WINDOWS\system32\...	SUCCESS	Desired Access: Execute/Trave...
1.23.20.3199119	sol.exe	2180	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Imag...
1.23.20.3200786	sol.exe	2180	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
1.23.20.3200993	sol.exe	2180	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWORD, Length: 4...
1.23.20.3201217	sol.exe	2180	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
1.23.20.3201314	sol.exe	2180	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec...	NAME NOT FOUND	Desired Access: Read
1.23.20.3211346	sol.exe	2180	Load Image	C:\WINDOWS\system32\msvcr.dll	SUCCESS	Image Base: 0x77c10000, Imag...
1.23.20.3213520	sol.exe	2180	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d00000, Imag...
1.23.20.3219764	sol.exe	2180	Load Image	C:\WINDOWS\system32\vpqit4.dll	SUCCESS	Image Base: 0x77e70000, Imag...
1.23.20.3221174	sol.exe	2180	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f00000, Imag...
1.23.20.3222851	sol.exe	2180	Load Image	C:\WINDOWS\system32\vgd32.dll	SUCCESS	Image Base: 0x77f10000, Imag...
1.23.20.3228389	sol.exe	2180	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x7e410000, Imag...
1.23.20.3230039	sol.exe	2180	FileSystemControl	C:\WINDOWS\system32\...	SUCCESS	Control: FSCTL_... VOLUME...
1.23.20.3230838	sol.exe	2180	QueryOpen	C:\WINDOWS\system32\cards.dll	SUCCESS	CreationTime: 14/04/2008 14:0...
1.23.20.3231628	sol.exe	2180	CreateFile	C:\WINDOWS\system32\cards.dll	SUCCESS	Desired Access: Execute/Trave...
1.23.20.3235087	sol.exe	2180	CreateFileMapping	C:\WINDOWS\system32\cards.dll	SUCCESS	SyncType: SyncTypeCreateSec...
1.23.20.3235372	sol.exe	2180	CreateFileMapping	C:\WINDOWS\system32\cards.dll	SUCCESS	SyncType: SyncTypeOther
1.23.20.3235531	sol.exe	2180	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, S...
1.23.20.3235724	sol.exe	2180	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Saler\CodeIdentifiers	SUCCESS	Desired Access: Query Value
1.23.20.3236120	sol.exe	2180	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Saler\CodeIdentifiers\T...	SUCCESS	Type: REG_DWORD, Length: 4...
1.23.20.3236338	sol.exe	2180	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Saler\CodeIdentifiers	SUCCESS	
1.23.20.3236486	sol.exe	2180	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Saler\CodeIdentifiers	NAME NOT FOUND	Desired Access: Query Value
1.23.20.3237258	sol.exe	2180	CloseFile	C:\WINDOWS\system32\cards.dll	SUCCESS	
1.23.20.3240786	sol.exe	2180	Load Image	C:\WINDOWS\system32\cards.dll	SUCCESS	Image Base: 0x6fc10000, Imag...
1.23.20.3241962	sol.exe	2180	Load Image	C:\WINDOWS\system32\shell32.dll	SUCCESS	Image Base: 0x7c900000, Imag...
1.23.20.3247815	sol.exe	2180	Load Image	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	Image Base: 0x77f60000, Imag...
1.23.20.3249259	sol.exe	2180	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide\Assembl...	NAME NOT FOUND	Desired Access: Enumerate Sub...
1.23.20.3249997	sol.exe	2180	QueryOpen	C:\WINDOWS\system32\sol.exe.Local	NAME NOT FOUND	
1.23.20.3250726	sol.exe	2180	QueryOpen	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595...	SUCCESS	CreationTime: 11/04/2020 15:2...
1.23.20.3251388	sol.exe	2180	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595...	SUCCESS	Desired Access: Execute/Trave...

Showing 667 of 39,339 events (1.%)

Process Monitor loaded by virtual memory

Process Explorer

- ⦿ Gestor de tareas que permite analizar en detalle el uso que los procesos hacen del sistema.
- ⦿ Identificación mediante colores:
 - servicios: rosa
 - procesos: azul
 - procesos nuevos: verde (temporal)
 - procesos finalizados: rojo (temporal)
- ⦿ Opciones más interesantes:
 - Verificar: compara la imagen de un proceso en memoria con su original en disco (binarios firmados).
 - Comparar cadenas: diferencias sustanciales indicarían un reemplazo de proceso.
 - Utilizar Dependency Walker: localizar uso de DLLs.
 - Analizar documentos maliciosos: uso de recursos.

Process Explorer

⦿ Ejercicio: ¿Cuántas hebras lanza Firefox?

The screenshot shows a Windows XP desktop with two windows open. The left window is Process Explorer, displaying a list of running processes. The right window is the 'firefox.exe:1224 Properties' dialog, showing the 'Threads' tab.

Process Explorer - Sysinternals: www.sysinternals.com [UGR-B1EF6CCDB53\gustavo] [Admin]

Process	CPU	Private Bytes	Working Set	PID	Description
System Idle Process	99.00	0 K	16 K	0	
System	0 K	0 K	212 K	4	
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs
smss.exe	196 K	440 K	364	Windows NT Session Manager	
csrss.exe	1.736 K	4.208 K	588	Client Server Runtime Process	
winlogon.exe	6.312 K	4.676 K	612	Windows NT Logon Application	
services.exe	1.664 K	3.452 K	656	Services and Controller app	
VBoxService.exe	3.260 K	4.236 K	836	VirtualBox Guest Additions Service	
svchost.exe	3.036 K	4.940 K	884	Generic Host Process for Windows Services	
svchost.exe	1.916 K	4.432 K	964	Generic Host Process for Windows Services	
svchost.exe	23.976 K	35.860 K	1060	Generic Host Process for Windows Services	
wscntfy.exe	548 K	2.404 K	1584	Windows Security Center Notification	
svchost.exe	1.280 K	3.560 K	1104	Generic Host Process for Windows Services	
svchost.exe	1.456 K	3.868 K	1172	Generic Host Process for Windows Services	
spoolsv.exe	3.100 K	4.812 K	1456	Spooler SubSystem App	
svchost.exe	1.252 K	3.744 K	1976	Generic Host Process for Windows Services	
alg.exe	1.116 K	3.552 K	1416	Application Layer Gateway Service	
lsass.exe	3.844 K	6.412 K	668	LSA Shell (Export Version)	
explorer.exe	25.008 K	10.116 K	1628	Windows Explorer	
VBoxTray.exe	2.060 K	4.184 K	1748	VirtualBox Guest Additions Tray	
ctfmon.exe	892 K	3.272 K	1764	CTF Loader	
processp.exe	46.936 K	51.672 K	1944	Sysinternals Process Explorer	
firefox.exe	135.132 K	138.420 K	1224	Firefox	

firefox.exe:1224 Properties

Image Performance Performance Graph Disk and Network
Threads TCP/IP Security Environment Strings

Count: 48

T.	CPU	CSwitch	Start Address
204	< 0.01	3	ucrtbase.dll+0x3d5b0
216			xul.dll+0x62c09c
236	< 0.01	10	ucrtbase.dll+0x3d5b0
240			ucrtbase.dll+0x3d5b0
276			ucrtbase.dll+0x3d5b0
404			ucrtbase.dll+0x3d5b0
560			kernel32.dll+0x10729
568			ucrtbase.dll+0x3d5b0
992			ucrtbase.dll+0x3d5b0
1028			firefox.exe+0x5eed
1096	< 0.01	12	ucrtbase.dll+0x3d5b0
1124			ucrtbase.dll+0x3d5b0
1308			ucrtbase.dll+0x3d5b0
1324			ucrtbase.dll+0x3d5b0
1388			xul.dll+0x62c09c
1420			ucrtbase.dll+0x3d5b0
1476			ole32.dll+0x1e507
1600			xul.dll+0x62c09c
1624	< 0.01	11	ucrtbase.dll+0x3d5b0
1704			ucrtbase.dll+0x3d5b0
1772			ucrtbase.dll+0x3d5b0
1868			ucrtbase.dll+0x3d5b0
1884	< 0.01	12	ucrtbase.dll+0x3d5b0
1920			xul.dll+0x62c09c
1940			kernel32.dll+0x10729
2032			ucrtbase.dll+0x3d5b0

Thread ID: 1028 Stack Module
Start Time: 2:03:59 13/04/2020
State: Wait:UserRequest Base Priority: 8
Kernel Time: 0:00:00.640 Dynamic Priority: 10
User Time: 0:00:02.093
Context Switches: 9,565

Permissions Kill Suspend
OK Cancel

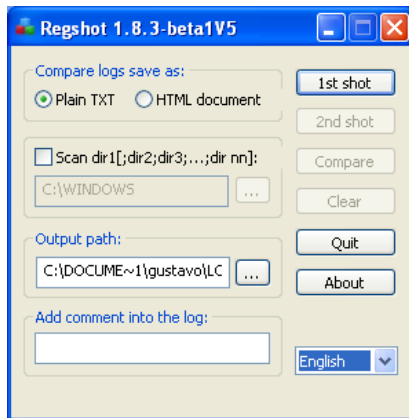
CPU Usage: 1.00% Commit Charge: 23.69%

Descargas Marcadores Historial Complementos Sync

start Process Explorer - Sys... Página de inicio de M... 2:05

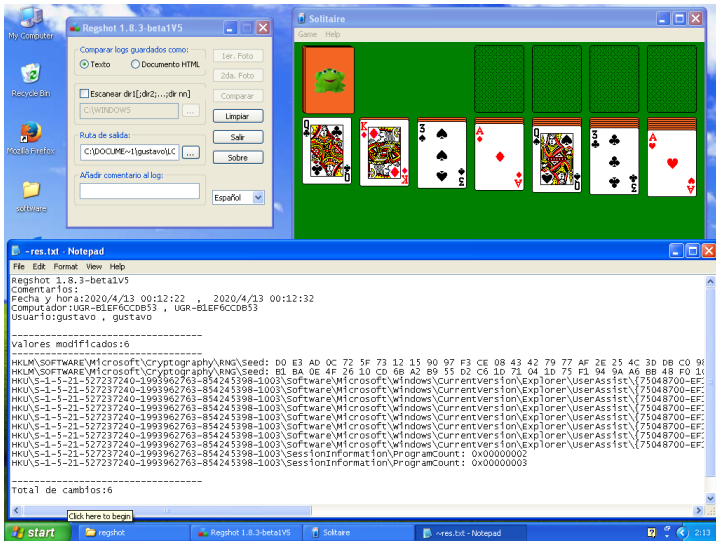
Comparando instantáneas del registro: **Regshot**

- ⦿ Permite tomar y comparar instantáneas del registro.
- ⦿ Uso:
 - 1º foto
 - ejecutar malware
 - 2ª foto
 - comparar



Comparando instantáneas del registro: **Regshot**

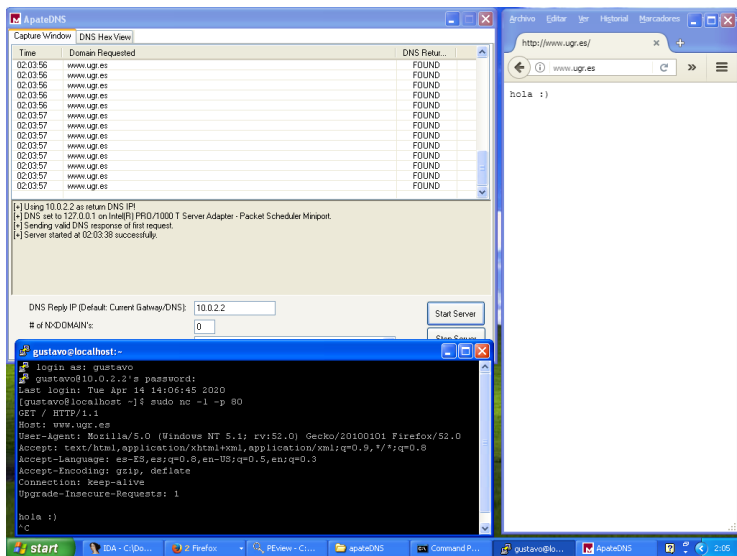
⊙ Ejercicio: ¿Afecta el solitario al registro de Windows?



Simulando una red

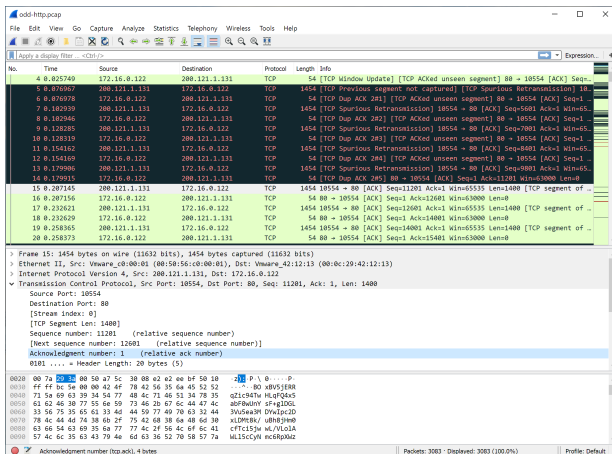
- ⊙ El malware suele comunicarse con servidores de control.
- ⊙ Crear una red falsa permite obtener pistas:
 - DNSs
 - IPs
 - paquetes que utilizar como identificadores
- ⊙ **ApateDNS**: servidor DNS bajo nuestro control.
- ⊙ **Netcat**: la navaja suiza del TCP/IP.
 - stdin -> red
 - red -> stdout

- ⦿ Ejercicio: Haga que la página web de la UGR le salude.

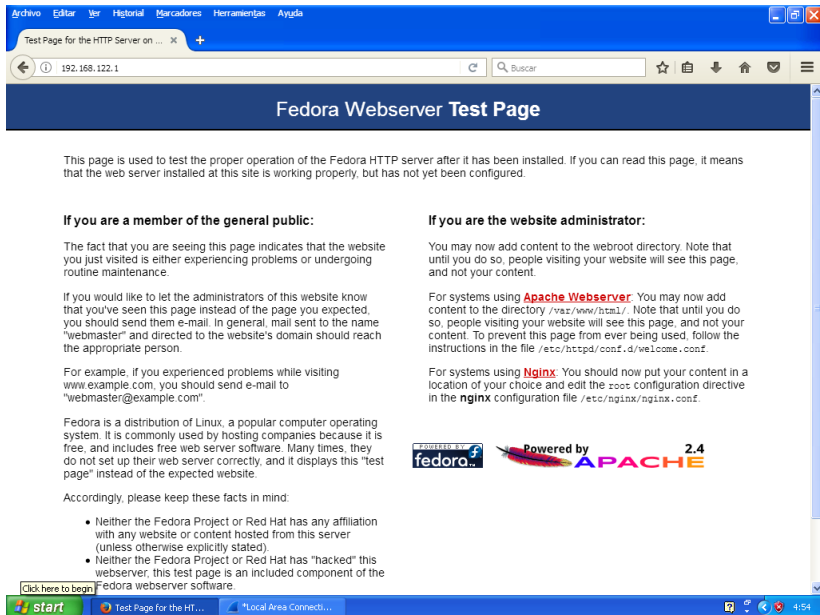


Capturando tráfico de red con Wireshark

- Intercepta y almacena tráfico de red.
- Facilita la visualización y el análisis tanto de paquetes individuales como de intercambios secuenciados.



Wireshark: diálogo Firefox <→> HTTPD



Wireshark: diálogo Firefox <→ HTTPD

Local Area Connection [Wireshark 1.10.14 (v1.10.14-0-g825f971 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	10.0.2.15	192.168.122.1	TCP	62	cognex-insight > http [SYN] Seq=0 win=64240 Len=0 MSS=1460 SA
2	0.00052600	192.168.122.1	10.0.2.15	TCP	60	http > cognex-insight [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0
3	0.00053700	10.0.2.15	192.168.122.1	TCP	54	cognex-insight > http [ACK] Seq=1 Ack=1 win=64240 Len=0
4	0.00072500	10.0.2.15	192.168.122.1	TCP	54	[TCP dup Ack 3#1] cognex-insight > http [ACK] Seq=1 Ack=1 win=
5	0.00090900	10.0.2.15	192.168.122.1	HTTP	385	GET / HTTP/1.1
6	0.00104400	192.168.122.1	10.0.2.15	TCP	60	http > cognex-insight [ACK] Seq=1 Ack=332 win=65535 Len=0
7	0.00154200	192.168.122.1	10.0.2.15	TCP	1474	[TCP segment of a reassembled PDU]
8	0.00154800	192.168.122.1	10.0.2.15	TCP	1474	[TCP segment of a reassembled PDU]
9	0.00155700	10.0.2.15	192.168.122.1	TCP	54	cognex-insight > http [ACK] Seq=332 Ack=2841 win=65535 Len=0
10	0.00168200	192.168.122.1	10.0.2.15	TCP	1474	[TCP segment of a reassembled PDU]
11	0.00168600	192.168.122.1	10.0.2.15	TCP	1474	[TCP segment of a reassembled PDU]
12	0.00169000	192.168.122.1	10.0.2.15	HTTP	247	HTTP/1.1 403 Forbidden (text/html)
13	0.00169600	10.0.2.15	192.168.122.1	TCP	54	cognex-insight > http [ACK] Seq=332 Ack=5874 win=65535 Len=0

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0

Ethernet II, Src: CadmusCo_87:98:34 (08:00:27:87:98:34), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.168.122.1 (192.168.122.1)

Transmission Control Protocol, Src Port: cognex-insight (1069), Dst Port: http (80), Seq: 0, Len: 0

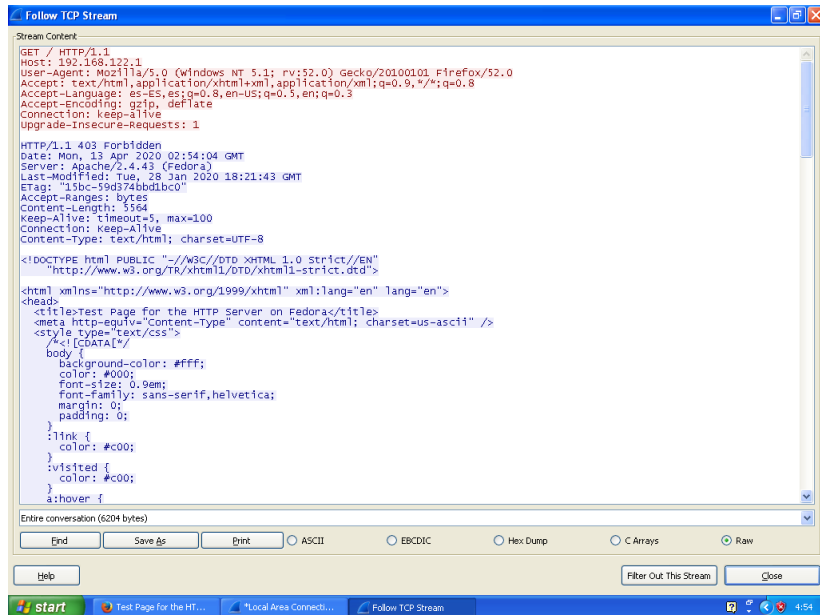
0000 52 54 00 12 35 02 08 00 27 87 98 34 08 00 45 00 RT..5...'.4..E.
0010 00 30 08 43 40 00 80 06 ab cc 0a 00 02 0f c0 a8 .0.C@... ..
0020 7a 01 04 2d 00 50 a4 7e b4 d3 00 00 00 70 02 Z...P~...p.
0030 fa f0 e3 a6 00 00 02 04 05 b4 01 01 04 02

File: C:\DOCUME~1\gustavo\LOCALS~1\Temp\... Packets: 13 · Displayed: 13 (100.0%) · Dropped: 0 (0.0%) Profile: Default

start Test Page for the HT... Local Area Connect...

4:54

Wireshark: diálogo Firefox <→> HTTPD



- ⊙ Simulador de los servicios más comunes de Internet.
- ⊙ Servicios emulados: DNS, FTP, HTTP, HTTPS, IRC, POP, POP₃, SMTP,...
- ⊙ Simular el comportamiento de los servidores reales para intentar mantener al malware funcionando.
- ⊙ Registra todas conexiones y peticiones entrantes.

1. Process Monitor
2. Process Explorer
3. Regshot
4. ApateDNS + nc/FakeNet/INetSim
5. Wireshark

... o todo a la vez desde una caja de arena...

1. Lab03-01.exe:

- 1.1 ¿Qué funciones importa? ¿Qué cadenas contiene?
- 1.2 ¿Deja señales en el anfitrión (*host-based indicators*)?
- 1.3 ¿Hay firmas de red? ¿Cuáles?

2. Lab03-02.dll:

- 2.1 ¿Puede conseguir que se instale?
- 2.2 ¿Cómo hacer que se ejecute?
- 2.3 ¿Cómo encontrar el proceso bajo el que se ejecuta?
- 2.4 ¿Qué filtros usaría en procmon para extraer información?
- 2.5 ¿Qué rastros deja en el anfitrión?
- 2.6 ¿Hay firmas de red?