Análisis de Malware

Comprensión y Análisis de Código Malicioso

Uso de herramientas, búsqueda en logs, funcionalidad y propósito del malware.

SECCION 2
Laboratorio de Análisis.

Clase 3
Herramientas de análisis.

.

Distros Forenses

OllyDbg

OllyDbg es un depurador a nivel de aplicación. La interfaz OllyDbg muestra el código ensamblador, volcado hexadecimal, la pila y registros de la CPU. OllyDbg también soporta rastreo, puntos de interrupción condicionales, visión de cabecera PE, edición hexadecimal.

IDA Pro

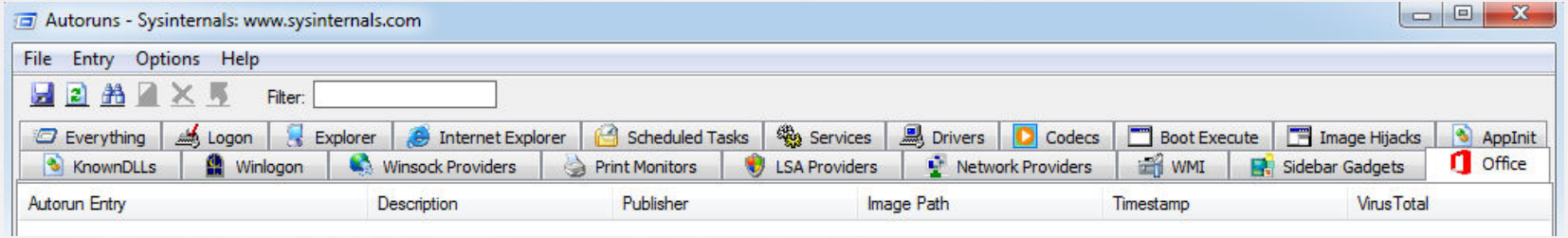
Al igual que OllyDbg, IDA Pro es un depurador / desensamblador a nivel de aplicación que nos ayudará enormemente en seguir la pista de la ejecución del programa. Cuenta con una versión de demo y una versión freeware más antigua, que es gratuita solo para uso no comercial.

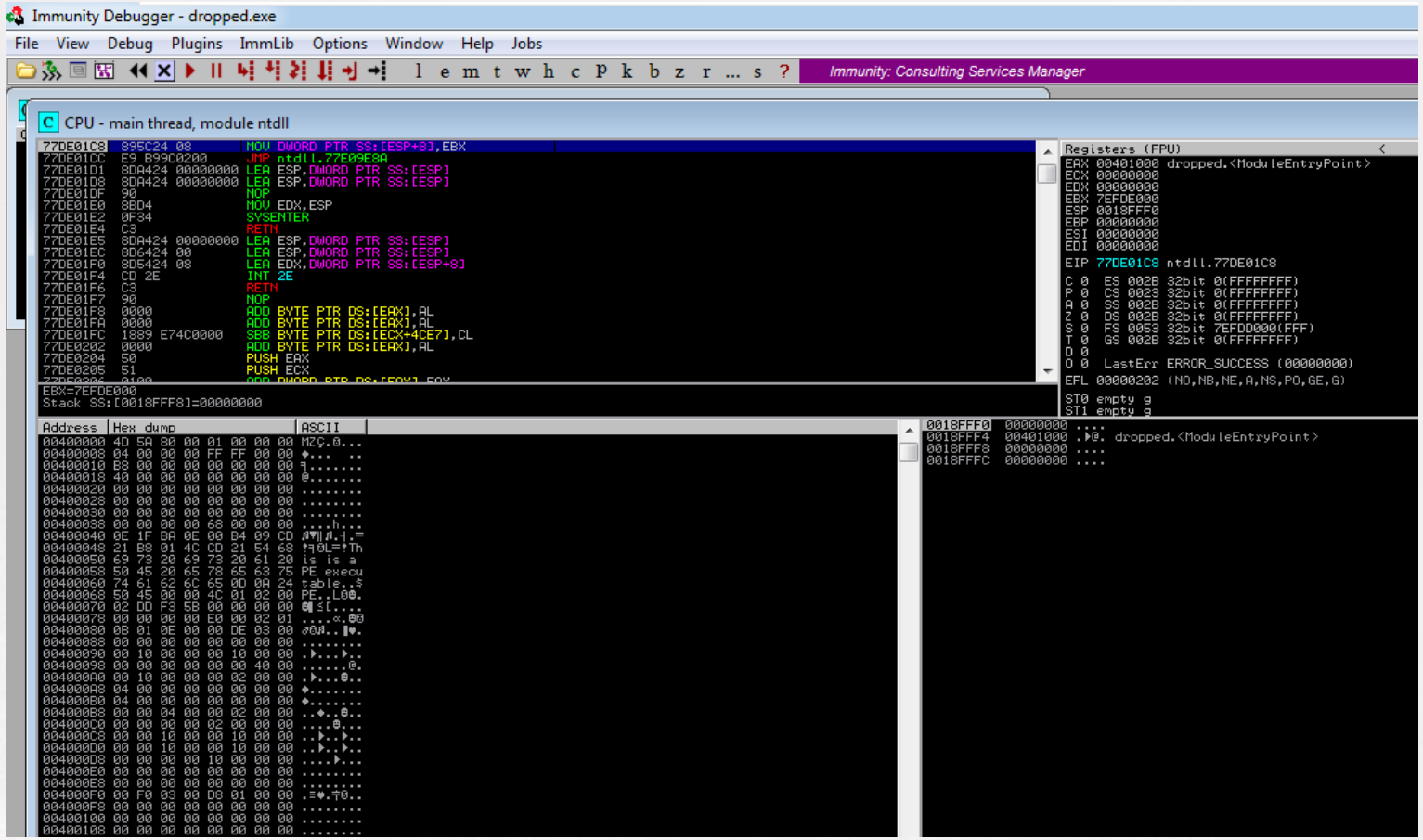
REGShot (Windows)

Comparativa de cambios en el sistema.

AutoRuns (Windows)

Permite observar los ejecutables ACTIVOS en tiempo real y los programados




Immunity Debugger - dropped.exe
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
CPU - main thread, module ntdll
77DE01C8 895C24 08 MOV DWORD PTR SS:[ESP+8],EBX
77DE01CC E9 B99C0200 JMP ntdll.77E09E8A
77DE01D1 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
77DE01D8 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
77DE01DF 90 NOP
77DE01E0 8BD4 MOV EDX,ESP
77DE01E2 0F34 SYSENTER
77DE01E4 C3 RETN
77DE01E5 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
77DE01EC 8D6424 00 LEA ESP,DWORD PTR SS:[ESP]
77DE01F0 8D5424 08 LEA EDX,DWORD PTR SS:[ESP+8]
77DE01F4 CD 2E INT 2E
77DE01F6 C3 RETN
77DE01F7 90 NOP
77DE01F8 0000 ADD BYTE PTR DS:[EAX],AL
77DE01FA 0000 ADD BYTE PTR DS:[EAX],AL
77DE01FC 1889 E74C0000 SBB BYTE PTR DS:[ECX+4CE7],CL
77DE0202 0000 ADD BYTE PTR DS:[EAX],AL
77DE0204 50 PUSH EAX
77DE0205 51 PUSH ECX
EBX=7EFDE000
Stack SS:[0018FFF8]=00000000
Registers (FPU)
EAX 00401000 dropped.<ModuleEntryPoint>
ECX 00000000
EDX 00000000
EBX 7EFDE000
ESP 0018FFF0
EBP 00000000
ESI 00000000
EDI 00000000
EIP 77DE01C8 ntdll.77DE01C8
C 0 ES 002B 32bit 0(FFFFFFFF)
P 0 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFDD000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty g
ST1 empty g
Address Hex dump ASCII
00400000 4D 5A 80 00 01 00 00 00 MZÇ.☺...
00400008 04 00 00 00 FF FF 00 00 ♦... ..
00400010 B8 00 00 00 00 00 00 00 ¸.......
00400018 40 00 00 00 00 00 00 00 @.......
00400020 00 00 00 00 00 00 00 00 ....
00400028 00 00 00 00 00 00 00 00 ....
00400030 00 00 00 00 00 00 00 00 ....
00400038 00 00 00 00 68 00 00 00 ....h...
00400040 0E 1F BA 0E 00 B4 09 CD ♫▼||♫.┤.=
00400048 21 B8 01 4C CD 21 54 68 !¸☺L=!Th
00400050 69 73 20 69 73 20 61 20 is is a
00400058 50 45 20 65 78 65 63 75 PE execu
00400060 74 61 62 6C 65 0D 0A 24 table..$
00400068 50 45 00 00 4C 01 02 00 PE..L☻☻.
00400070 02 DD F8 5B 00 00 00 00 ☻▌°[....
00400078 00 00 00 00 E0 00 02 01 ....∝.☻☺
00400080 0B 01 0E 00 00 DE 03 00 ♂☺♫..▌♥.
00400088 00 00 00 00 00 00 00 00 ....
00400090 00 10 00 00 00 10 00 00 .►...►..
00400098 00 00 00 00 00 00 40 00 ......@.
004000A0 00 10 00 00 00 02 00 00 .►...☻..
004000A8 04 00 00 00 00 00 00 00 ♦.......
004000B0 04 00 00 00 00 00 00 00 ♦.......
004000B8 00 00 04 00 00 02 00 00 ..♦..☻..
004000C0 00 00 00 00 00 02 00 00 ....☻...
004000C8 00 00 10 00 00 10 00 00 ..►..►..
004000D0 00 00 10 00 00 10 00 00 ..►..►..
004000D8 00 00 00 00 10 00 00 00 ....►...
004000E0 00 00 00 00 00 00 00 00 ....
004000E8 00 00 00 00 00 00 00 00 ....
004000F0 00 F0 03 00 D8 01 00 00 .≡♥.╪☺..
004000F8 00 00 00 00 00 00 00 00 ....
00400100 00 00 00 00 00 00 00 00 ....
00400108 00 00 00 00 00 00 00 00 ....
0018FFF0 00000000 ....
0018FFF4 00401000 .►☺. dropped.<ModuleEntryPoint>
0018FFF8 00000000 ....
0018FFFC 00000000 ....


CRACKS
DATA VIRUS
MALICIOUS SOFTWARE
THEFT
SOCIAL MEDIA ATTACKS
CYBERWARFARE
VIRUS
SOFTWARE FAILURE
NETWORK SNIFFING
YOUR DATA SAFETY
SPYWARE
HUMAN ERROR
SOFTWARE ERROR
STOLEN INFORMATION
TROJAN
CYBER ATTACKS
PASSWORD CRACKING
HACKING
FRAUD
CYBERCRIMINALS
TROJAN
ADWARE
SYSTEM PENETRATION
CYBERSTALKING

¡Nos vemos en la siguiente Clase!