

OLLY DBG

Tramite il tool OllyDBG, un debugger per sistemi Windows, che traccia registri, riconosce le funzioni e i parametri passati alle principali librerie standard, variabili, stringhe, eventuali salti condizionali ed altre componenti di codice, sarà possibile rispondere ai quesiti richiesti dalle task odierne.

1.

All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?

Dopo aver caricato il file d'interesse sul debugger, la schermata che si aprirà sarà la seguente

00401572 > 8B PUSH EBP
00401573 > 8B MOV EBP, ESP
00401574 > 6A FF PUSH -1
00401575 > 68 C0404000 PUSH Halware_..004040C0
00401581 > 69 3C204000 PUSH Halware_..0040203C
00401586 > 64H1 00000000 MOV EAX, DWORD PTR FS:[0]
0040158B > 8B MOV EBX, EDI
0040158D > 64I8925 000000 MOV DWORD PTR FS:[0], ESP
00401594 > 83EC 10 SUB ESP, 10
00401597 > 83 PUSH EBX
00401598 > 87 PUSH EDI
00401599 > 87 PUSH EDI
0040159A > 8965 E8 MOV DWORD PTR SS:[EBP-18], ESP
0040159B > 83E 30404000 CALL DWORD PTR DS:[<&Kernel32.GetVersion kernel32.GetVersion
0040159D > 83D2 XOR EDX, EDX
004015A0 > 8040 MOV DL, AH
004015A1 > 8115 04524000 MOV DWORD PTR DS:[4052D4], EDX
004015A4 > 8BC8 MOV ECX, EAX
004015A7 > 91E1 FF000000 AND ECX, 0FF
004015B0 > 83D0 D0524000 MOV DWORD PTR DS:[4052D0], ECX
004015B3 > C1E1 08 SHL ECX, 8
004015B4 > 83C4 MOV EAX, ECX
004015C0 > 83D0 C0524000 MOV DWORD PTR DS:[4052C0], ECX
004015C3 > C1E9 10 SHR EAX, 10
004015C5 > A3 C8524000 MOV DWORD PTR DS:[4052C8], EAX
004015C8 > 6A 00 PUSH 0
004015CB > C8H 33090000 CALL Halware_..00401F08
004015D0 > 59 POP ECX
004015D1 > 85C9 TEST EAX, EAX
004015D8 > 75 08 JNZ SHORT Halware_..004015E2
004015DA > 6A 1C PUSH 1C
004015DB > C8H 9A000000 CALL Halware_..00401678
004015DE > 59 POP ECX
004015E1 > 8965 FC 00 MOV DWORD PTR SS:[EBP-4], 0
004015E2 > E8 72070000 CALL Halware_..00401D5D
004015E5 > FF15 2C404000 CALL DWORD PTR DS:[<&Kernel32.GetCommand CGetCommandLineA
004015F0 > 8B D8740000 MOV DWORD PTR DS:[4057D0], EAX
004015F3 > C8 30B06000 CALL Halware_..00401C2E
004015F6 > A3 B0524000 MOV DWORD PTR DS:[4052D0], EAX
004015F9 > C8H D9090000 CALL Halware_..004019DE
00401600 > E8 1B0B0000 CALL Halware_..00401925
00401603 > E8 90090000 CALL Halware_..0040169F
00401606 > A1 E4524000 MOV EAX, DWORD PTR DS:[4052E4]
00401609 > C8H B8524000 MOV DWORD PTR DS:[4052E8], EAX
00401610 > 8B D8740000 MOV DWORD PTR DS:[4057D0], EAX
00401613 > FF35 D0524000 PUSH DWORD PTR DS:[4052D0]
00401616 > FF3E 00000000 PUSH DWORD PTR DS:[4052D0]
00401619 > E8 FDF0FFFF CALL Halware_..00401128
00401622 > 83C4 0C ADD ESP, 0C
00401625 > 9945 E4 MOV DWORD PTR SS:[EBP-1C], EAX
00401631 > 59 POP ECX
00401632 > C8H 95090000 CALL Halware_..004016CC
00401637 > 8B45 EC MOV EAX, DWORD PTR SS:[EBP-14]
0040163A > 8B08 MOV ECX, DWORD PTR DS:[EAX]
0040163D > 8B09 MOV EDI, DWORD PTR DS:[ECX]
0040163E > 8340 E0 MOV DWORD PTR SS:[EBP-20], ECX
00401641 > 8B MOV EAX, EDI
00401642 > 51 PUSH ECX
00401643 > E8 59010000 CALL Halware_..004017A1
00401648 > 59 POP ECX
00401649 > 59 POP ECX
0040164A > C3 RETN

Registers (FPU)

EAX	00000000
ECX	0012FFB0
EDX	7C90E4F4 ntddi.KiFastSystemCallRet
EBX	7FFDF000
ESP	0012FFC4
EBP	0012FFFF
EIP	0012FFFF
EDI	7C910208 ntddi..7C910208
EIP	00401577 Halware_..<ModuleEntryPoint>
C 0	ES 0023 32bit 0 (FFFFFFFF)
P 1	CS 001B 32bit 0 (FFFFFFFF)
R 0	SS 0023 32bit 0 (FFFFFFFF)
Z 1	DS 0023 32bit 0 (FFFFFFFF)
F 0	FS 003B 32bit 7FDE000 (FFF)
D 0	GS 0000 NULL
I 0	0 LastErr ERROR_INVALID_HANDLE (00000006)
EPL	000000246 (NO, NB, E, BE, HS, PE, GE, LE)
ST0	empty -UNORM 010904 00500090
ST1	empty +UNORM 0069 006E0069 002E0069
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0
ST6	empty 0.0
ST7	empty 0.0
FST 0000	Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F	Prec NEAR, SS Mask 1 1 1 1 1 1

Disassembler Window

00401572 > 8B PUSH EBP
00401573 > 8B MOV EBP, ESP
00401574 > 6A FF PUSH -1
00401575 > 68 C0404000 PUSH Halware_..004040C0
00401581 > 69 3C204000 PUSH Halware_..0040203C
00401586 > 64H1 00000000 MOV EAX, DWORD PTR FS:[0]
0040158B > 8B MOV EBX, EDI
0040158D > 64I8925 000000 MOV DWORD PTR FS:[0], ESP
00401594 > 83EC 10 SUB ESP, 10
00401597 > 83 PUSH EBX
00401598 > 87 PUSH EDI
00401599 > 87 PUSH EDI
0040159A > 8965 E8 MOV DWORD PTR SS:[EBP-18], ESP
0040159B > 83E 30404000 CALL DWORD PTR DS:[<&Kernel32.GetVersion kernel32.GetVersion
0040159D > 83D2 XOR EDX, EDX
004015A0 > 8040 MOV DL, AH
004015A1 > 8115 04524000 MOV DWORD PTR DS:[4052D4], EDX
004015A4 > 8BC8 MOV ECX, EAX
004015A7 > 91E1 FF000000 AND ECX, 0FF
004015B0 > 83D0 D0524000 MOV DWORD PTR DS:[4052D0], ECX
004015B3 > C1E1 08 SHL ECX, 8
004015B4 > 83C4 MOV EAX, ECX
004015C0 > 83D0 C0524000 MOV DWORD PTR DS:[4052C0], ECX
004015C3 > C1E9 10 SHR EAX, 10
004015C5 > A3 C8524000 MOV DWORD PTR DS:[4052C8], EAX
004015C8 > 6A 00 PUSH 0
004015CB > C8H 33090000 CALL Halware_..00401F08
004015D0 > 59 POP ECX
004015D1 > 85C9 TEST EAX, EAX
004015D8 > 75 08 JNZ SHORT Halware_..004015E2
004015DA > 6A 1C PUSH 1C
004015DB > C8H 9A000000 CALL Halware_..00401678
004015DE > 59 POP ECX
004015E1 > 8965 FC 00 MOV DWORD PTR SS:[EBP-4], 0
004015E2 > E8 72070000 CALL Halware_..00401D5D
004015E5 > FF15 2C404000 CALL DWORD PTR DS:[<&Kernel32.GetCommand CGetCommandLineA
004015F0 > 8B D8740000 MOV DWORD PTR DS:[4057D0], EAX
004015F3 > C8 30B06000 CALL Halware_..00401C2E
004015F6 > A3 B0524000 MOV DWORD PTR DS:[4052D0], EAX
004015F9 > C8H D9090000 CALL Halware_..004019DE
00401600 > E8 1B0B0000 CALL Halware_..00401925
00401603 > E8 90090000 CALL Halware_..0040169F
00401606 > A1 E4

Per ritrovare informazioni circa le istruzioni eseguite dalla CPU, in questo caso specifico per capire il valore del parametro “Command Line” passato allo stack, sarà necessario analizzare attentamente la

Disassembler window

00401056	52	PUSH EDX	pProcessInfo
00401057	8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]	pStartupInfo
0040105A	50	PUSH EAX	CurrentDir = NULL
0040105B	6A 00	PUSH 0	pEnvironment = NULL
0040105D	6A 00	PUSH 0	CreationFlags = 0
0040105F	6A 00	PUSH 0	InitialHandles = TRUE
00401061	6A 01	PUSH 1	pThreadSecurity = NULL
00401063	6A 00	PUSH 0	pProcessSecurity = NULL
00401065	6A 00	PUSH 0	CommandLine = "cmd"
00401067	68 30504000	PUSH Malware_.00405030	hObject
0040106C	6A 00	PUSH 0	WaitForSingleObject
0040106E	FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA	CreateProcessA
00401074	8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	Timeout = INFINITE
00401077	6A FF	PUSH -1	
00401079	8B4D F0	MOV ECX,DWORD PTR SS:[EBP-10]	
0040107C	51	PUSH ECX	
0040107D	FF15 00404000	CALL DWORD PTR DS:[<&KERNEL32.WaitForSingleObject	
00401083	33F0	XOR FAX,FAX	

Il valore del parametro <Command line> che viene passato sullo stack è <cmd> .

2. Cambiamento dei valori di registro EDX

Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

00401577	55	PUSH EBP	
00401578	8BEC	MOV EBP,ESP	
00401579	6A FF	PUSH -1	
0040157C	68 C0404000	PUSH Malware_.004040C0	
00401581	68 3C204000	PUSH Malware_.0040203C	
00401586	64:R1 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation
0040158C	50	PUSH EAX	
0040158D	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
00401594	8BEC 10	SUB ESP,10	
00401597	53	PUSH EBX	
00401598	56	PUSH ESI	
00401599	57	PUSH EDI	
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	33D2	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	8BDC	MOV ECX,EAX	
004015AF	81E1 FF000000	AND ECX,0FF	
004015B5	8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	C1E1 08	SHL ECX,8	
004015BE	03CA	ADD ECX,EDX	
004015C0	8900 CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C3	C1E3 10	SHR EAX,10	
004015C9	A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	6A 00	PUSH 0	
004015D0	68 33090000	PUSH Malware_.00401F08	
004015D5	59	POP ECX	
004015D6	85C0	TEST EAX,EAX	
004015D8	75 08	JNZ SHORT Malware_.004015E2	
004015DA	6A 1C	PUSH 1C	
004015DC	E8 9A000000	CALL Malware_.00401678	
004015E1	59	POP ECX	

Cerchiamo l'indirizzo assegnato, 004015A3, con tasto destro scorriamo nella finestra a cascata fino alla sezione "breakpoint" scegliendone uno software, ossia "toggle"

Il valore iniziale EDX sarà 7C90E4F4

Dopo aver inserito il breakpoint ed aver eseguito uno "step into" sarà possibile notare che alla "register window" è avvenuto un cambiamento nel valore del registro EDX

00401578	8BEC	MOV EBP,ESP	
00401579	6A FF	PUSH -1	
0040157C	68 C0404000	PUSH Malware_.004040C0	
00401581	68 3C204000	PUSH Malware_.0040203C	
00401586	64:R1 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation
0040158C	50	PUSH EAX	
0040158D	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
00401594	8BEC 10	SUB ESP,10	
00401597	53	PUSH EBX	
00401598	56	PUSH ESI	
00401599	57	PUSH EDI	
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	33D2	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	8BDC	MOV ECX,EAX	
004015AF	81E1 FF000000	AND ECX,0FF	
004015B5	8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	C1E1 08	SHL ECX,8	
004015BE	03CA	ADD ECX,EDX	
004015C0	8900 CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C3	C1E3 10	SHR EAX,10	
004015C9	A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	6A 00	PUSH 0	
004015D0	68 33090000	PUSH Malware_.00401F08	
004015D5	59	POP ECX	
004015D6	85C0	TEST EAX,EAX	
004015D8	75 08	JNZ SHORT Malware_.004015E2	
004015DA	6A 1C	PUSH 1C	
004015DC	E8 9A000000	CALL Malware_.00401678	
004015E1	59	POP ECX	
004015E2	8B45 F0	MOV ECX,DWORD PTR SS:[EBP-10]	
004015E3	E8 70090000	CALL Malware_.004016D0	
004015E8	FF15 2C404000	CALL DWORD PTR DS:[<&KERNEL32.GetCommandLineA	GetCommandLineA

Il valore del registro EDX è adesso 00000000

3. Cambiamenti dei valori di registro ECX

Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?
Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

00401577	55	PUSH EBP	
00401578	8BEC	MOV EBP,ESP	
00401579	6A FF	PUSH -1	
0040157C	68 C0404000	PUSH Malware_.004040C0	
00401581	68 3C204000	PUSH Malware_.0040203C	
00401586	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler: installation
0040158C	50	PUSH EAX	
0040158D	64:8925 000000	MOV DWORD PTR FS:[0],ESP	
00401594	83EC 10	SUB ESP,10	
00401597	53	PUSH EBX	
00401598	56	PUSH ESI	
00401599	57	PUSH EDI	
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A2	33D2	XOR EDX,EDX	
004015A3	8AD4	MOV DL,AH	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	8BC8	MOV ECX,EBX	
004015AE	81E1 FF000000	AND ECX,0FF	
004015B5	890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	91E1 80	CUI ERY 0	

Registers (FPU)
EAX 0A280105
ECX 0A280105
EDX 00000001
EBX 7FFD5000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C910208 ntdll.7C
EIP 004015AF Malware_
C 0 ES 0023 32bit 0:
P 1 CS 001B 32bit 0:
A 0 SS 0023 32bit 0:
Z 1 DS 0023 32bit 0:
S 0 FS 003B 32bit 7F
T 0 GS 0000 NULL
D 0
0 LastErr ERROR_INH
FFI 0000024C INN NR F

Valore iniziale all'indirizzo di memoria 004015AF è 0A280105

Dopo aver inserito un breakpoint Toggle all'indirizzo specificato, ed eseguito uno step into il valore di ECX sarà 000000005

CPU - main thread, module Malware_			
004015B3	33D2	XOR EDX,EDX	
004015B5	8AD4	MOV DL,AH	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	8BC8	MOV ECX,EBX	
004015AE	81E1 FF000000	AND ECX,0FF	
004015B5	890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	C1E1 08	SH ECX,8	
004015BE	8BC4	MOV ECX,EDX	
004015C0	890D CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	C1E8 10	SHR EAX,10	
004015C9	66 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	6A 00	PUSH 0	
004015D0	E9 30909000	CALL Malware_.00401F08	
004015D6	E9	POP ECX	
004015D8	85C9	TEST EAX,EAX	
004015D8	75 08	JNZ SHORT Malware_.004015E2	
004015D8	6A 1C	PUSH 1C	
004015D8	E8 30000000	CALL Malware_.00401578	
004015E1	59	POP ECX	
004015E2	8B65 FC 00	MOV DWORD PTR SS:[EBP-4],0	
004015E6	E8 72070000	CALL Malware_.00401D5D	
004015E9	FF15 2C404000	CALL DWORD PTR DS:[&KERNEL32.GetComm	CGetCommandLineA
004015F1	83 D8574000	MOV DWORD PTR DS:[4057D8],EAX	
004015F6	E8 30909000	CALL Malware_.00401C25	
004015FB	83 B8524000	MOV DWORD PTR DS:[4052B8],EAX	
00401600	E8 D9909000	CALL Malware_.0040190E	
00401605	E8 10930000	CALL Malware_.0040193E	
00401609	E8 90909000	CALL Malware_.00401699	
0040160F	A1 E4524000	MOV EAX,DWORD PTR DS:[4052E4]	
00401614	8B E8524000	MOV DWORD PTR DS:[4052E8],EAX	
00401619	59	PUSH EAX	
0040161A	FF35 DC524000	PUSH DWORD PTR DS:[4052DC]	
00401620	FF35 D8524000	PUSH DWORD PTR DS:[4052D8]	
00401626	E8 F0F0FFFF	CALL Malware_.00401128	
0040162B	83C4 0C	ADD ESP,0C	
0040162E	8945 E4	MOV DWORD PTR SS:[EBP-1C],EAX	
00401631	50	PUSH EAX	

Registers (FPU)
EAX 00000105
ECX 00000005
EDX 00000001
EBX 7FFD5000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C910208 Malware_.004015B5
EIP 004015B5
C 0 ES 0023 32bit 0:FFFFFFFF
P 1 CS 001B 32bit 0:FFFFFFFF
A 0 SS 0023 32bit 0:FFFFFFFF
Z 0 DS 0023 32bit 0:FFFFFFFF
S 0 FS 003B 32bit 7FFD5000
T 0 GS 0000 NULL
D 0
0 LastErr ERROR_INVALID_HRN
EFL 00000206 (NO,NS,NE,NA,NS,PE
ST0 empty +UNORM 0069 006E0069
ST1 empty +UNORM 0069 006E0069
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FPU 0000 Cond 0 0 0 0 Err 0
FCW 027F Prec NEAR,53 Mask

Index	Type	Access	Initial	Mapped as
0	Image	R	RWE	
1	Image	R	RWE	
2	Image	R	RWE	
3	Image	R	RWE	
4	Image	R	RWE	
5	Image	R	RWE	
6	Image	R	RWE	
7	Image	R	RWE	
8	Image	R	RWE	
9	Image	R	RWE	