

# OllyDBG

Con riferimento al malware "Malware\_U3\_W3\_L3" presente all'interno della cartella "Esercizio\_Pratico\_U3\_W3\_L3" sul desktop della macchina virtuale Windows XP dedicata all'analisi dei malware, rispondere ai seguenti quesiti utilizzando OllyDBG:

- **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?;
- **2)** Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?. Eseguite a questo punto uno «step-into» e indicate qual'è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?;
- **3)** Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?. Eseguite poi uno step-into, qual'è ora il valore di ECX? Spiegate quale istruzione è stata eseguita

## SOLUZIONI:

Dopo aver preparato la macchina virtuale, disattivando le connessioni esterne ad internet ed ogni instradamento pericoloso verso la macchina host e dispositivi di archiviazione esterni, procedo con le soluzioni:

**1)**

00401020	51	PUSH EAX	
0040102C	E8 AF030000	CALL Malware_.004013E0	
00401031	83C4 0C	ADD ESP,0C	
00401034	C745 D4 010101	MOV DWORD PTR SS:[EBP-2C],101	
00401038	66:C745 D8 00	MOV WORD PTR SS:[EBP-28],0	
00401041	8B55 18	MOV EDI,DWORD PTR SS:[EBP+18]	
00401044	8B55 E0	MOV EDI,DWORD PTR SS:[EBP-20],EDI	
00401047	8B45 E0	MOV EAX,DWORD PTR SS:[EBP-20]	
0040104A	8B45 E8	MOV DWORD PTR SS:[EBP-18],EAX	
0040104D	8B4D E8	MOV ECX,DWORD PTR SS:[EBP-18]	
00401050	8B4D E4	MOV DWORD PTR SS:[EBP-1C],ECX	
00401053	8D55 F0	LEA EDI,DWORD PTR SS:[EBP-10]	
00401056	52	PUSH EDI	
00401057	8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]	
0040105A	50	PUSH EAX	
0040105B	6A 00	PUSH 0	
0040105D	6A 00	PUSH 0	
0040105F	6A 00	PUSH 0	
00401061	6A 01	PUSH 1	
00401063	6A 00	PUSH 0	
00401065	6A 00	PUSH 0	
00401067	68 30504000	PUSH Malware_.00405030	
0040106C	6A 00	PUSH 0	
0040106E	FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreateProcess	pProcessInfo pStartupInfo CurrentDir = NULL pEnvironment = NULL CreationFlags = 0 InheritHandles = TRUE pThreadSecurity = NULL pProcessSecurity = NULL CommandLine = "cmd" ModuleFileName = NULL CreateProcessA Timeout = INFINITE
00401074	8B45 EC	MOV DWORD PTR SS:[EBP-14],EAX	
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.WaitForSingle	hObject WaitForSingleObject

All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess», il valore del parametro «CommandLine» che viene passato sullo stack è "cmd" ovvero il comando per avviare il command prompt di Windows.

2)

PRIMA

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]			
File View Debug Options Window Help			
LEMTW H C / K B R ... S			
0040156F	EB 02	JMP SHORT Malware_.00401573	
00401571	8BC7	MOV EAX,EDI	
00401573	FC	CLD	
00401574	5F	POP EDI	
00401575	C9	LEAVE	
00401576	C3	RETN	
00401577	55	PUSH EBP	
00401578	8BEC	MOV EBP,ESP	
0040157A	6A FF	PUSH -1	
0040157C	68 04040000	PUSH Malware_.00404000	
00401581	68 3C204000	PUSH Malware_.0040203C	
00401586	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
0040158C	50	PUSH EAX	
0040158D	64:8925 000000	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	8B65 E8	MOV DWORD PTR SS:[EBP-18],ESP	
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]	kernel32.GetVersion
004015A0	30D2	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	8BC8	MOV ECX,EAX	
004015AF	81E1 FF000000	AND ECX,0FF	
004015B5	8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	C1E1 05	SHL ECX,5	
004015BE	03CA	ADD ECX,EDX	
004015C0	8900 CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	C1E8 10	SHR EAX,10	
004015C9	A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	6A 00	PUSH 0	
004015D0	E8 33090000	CALL 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 90000000	CALL Malware_.0040167B	
004015E1	59	POP ECX	
004015E2	8B65 FC 00	MOV DWORD PTR SS:[EBP-4],0	
004015E5	8B65 20200000	CALL Malware_.004016D0	

DOPO

OllyDbg - Malware\_U3\_W3\_L3.exe - [CPU - main thread, module Malware\_]

Assembly window (addresses 0040156F to 00401F08):

```

0040156F JEB 02 JMP SHORT Malware_.00401573
00401571 JBC 7 MOV EAX, EDI
00401573 JFC 5 CLD
00401574 JF 5F POP EDI
00401575 JC 9 LEAVE
00401576 C9 RETN
00401577 55 PUSH EBP
00401578 8BEC MOV EBP, ESP
0040157A 6A FF PUSH -1
0040157C 68 C0404000 PUSH Malware_.004040C0
00401581 68 3C204000 PUSH Malware_.0040203C
00401586 64:01 00000000 MOV EAX, DWORD PTR FS:[0]
0040158C 50 PUSH EAX
00401590 64:9225 000000 MOV DWORD PTR FS:[0], ESP
00401594 83EC 10 SUB ESP, 10
00401597 53 PUSH EBX
00401599 57 PUSH ESI
0040159A 57 PUSH EDI
0040159B 8965 E8 MOV DWORD PTR SS:[EBP-18], ESP
0040159D FF15 30404000 CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]
004015A3 33D2 XOR EDX, EDX
004015A5 80D4 MOV DL, AH
004015A7 9115 D4524000 MOV DWORD PTR DS:[4052D4], EDX
004015AD 8BC8 MOV ECX, EAX
004015AF 9115 FF000000 MOV ECX, DWORD PTR FS:[0]
004015B5 99D0 D0524000 MOV DWORD PTR DS:[4052D0], ECX
004015BB C1E1 08 SHL ECX, 8
004015BE ADD ECX, EDX
004015C0 99D0 CC524000 MOV DWORD PTR DS:[4052CC], ECX
004015C6 C1E8 10 SHR EAX, 10
004015C9 A3 C8524000 MOV DWORD PTR DS:[4052C8], EAX
004015CE 6A 00 PUSH 0
004015D0 E8 33090000 CALL Malware_.00401F08
  
```

Registers (FPU) window:

```

EAX 0A280105
ECX 7FFD4000
EDI 00000000
EBX 7FFD4000
ESP 0012FF94
ESI FFFFFFFF
EDI 7C920208 ntdll.7C920208
EIP 004015A3 Malware_.004015A3
C 0 ES 0023 32bit 0 (FFFFFFFF)
P 1 CS 001B 32bit 0 (FFFFFFFF)
S 0 SS 0023 32bit 0 (FFFFFFFF)
D 0 DS 0023 32bit 0 (FFFFFFFF)
I 0 FS 003B 32bit 7FFDF000 (FFF)
T 0 GS 0000 NULL
D 0
0 0 LastErr ERROR_INVALID_HANDLE (00000000)
EFL 0000246 (NO, NB, E, BE, NS, PE, GE, LE)
ST0 empty -UNORM BCBC 01050104 006F005C
ST1 empty 0.1077351297874321950e-4933
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
FCW 027F Prec NEAR, 53 Mask 1 1 1 1 1 1
  
```

Inserito il breakpoint software all'indirizzo 004015A3, il valore del registro EDX è "00000A28". Eseguito uno «step-into», il valore del registro EDX diventa "00000000" poiché lo "XOR EDX, EDX" dello stesso registro (cioè con se stesso) inizializza a zero il suo valore, essendo che l'operazione XOR (exclusive OR) tra due bit restituisce 1 se i bit sono diversi e 0 se i bit sono uguali.

3)

PRIMA

OllyDbg - Malware\_U3\_W3\_L3.exe - [CPU - main thread, module Malware\_]

Assembly window (addresses 0040156F to 00401F08):

```

0040156F JEB 02 JMP SHORT Malware_.00401573
00401571 JBC 7 MOV EAX, EDI
00401573 JFC 5 CLD
00401574 JF 5F POP EDI
00401575 JC 9 LEAVE
00401576 C9 RETN
00401577 55 PUSH EBP
00401578 8BEC MOV EBP, ESP
0040157A 6A FF PUSH -1
0040157C 68 C0404000 PUSH Malware_.004040C0
00401581 68 3C204000 PUSH Malware_.0040203C
00401586 64:01 00000000 MOV EAX, DWORD PTR FS:[0]
0040158C 50 PUSH EAX
00401590 64:9225 000000 MOV DWORD PTR FS:[0], ESP
00401594 83EC 10 SUB ESP, 10
00401597 53 PUSH EBX
00401599 57 PUSH ESI
0040159A 57 PUSH EDI
0040159B 8965 E8 MOV DWORD PTR SS:[EBP-18], ESP
0040159D FF15 30404000 CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]
004015A3 33D2 XOR EDX, EDX
004015A5 80D4 MOV DL, AH
004015A7 9115 D4524000 MOV DWORD PTR DS:[4052D4], EDX
004015AD 8BC8 MOV ECX, EAX
004015AF 9115 FF000000 MOV ECX, DWORD PTR FS:[0]
004015B5 99D0 D0524000 MOV DWORD PTR DS:[4052D0], ECX
004015BB C1E1 08 SHL ECX, 8
004015BE ADD ECX, EDX
004015C0 99D0 CC524000 MOV DWORD PTR DS:[4052CC], ECX
004015C6 C1E8 10 SHR EAX, 10
004015C9 A3 C8524000 MOV DWORD PTR DS:[4052C8], EAX
004015CE 6A 00 PUSH 0
004015D0 E8 33090000 CALL Malware_.00401F08
  
```

Registers (FPU) window:

```

EAX 0A280105
ECX 0A280105
EDI 00000001
EBX 7FFD4000
ESP 0012FF94
ESI FFFFFFFF
EDI 7C920208 ntdll.7C920208
EIP 004015AF Malware_.004015AF
C 0 ES 0023 32bit 0 (FFFFFFFF)
P 1 CS 001B 32bit 0 (FFFFFFFF)
S 0 SS 0023 32bit 0 (FFFFFFFF)
D 0 DS 0023 32bit 0 (FFFFFFFF)
I 0 FS 003B 32bit 7FFDF000 (FFF)
T 0 GS 0000 NULL
D 0
0 0 LastErr ERROR_INVALID_HANDLE (00000000)
EFL 0000246 (NO, NB, E, BE, NS, PE, GE, LE)
ST0 empty -UNORM BCBC 01050104 006F005C
ST1 empty 0.1077351297874321950e-4933
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
FCW 027F Prec NEAR, 53 Mask 1 1 1 1 1 1
  
```

DOPO

OllyDbg - Malware\_U3\_W3\_L3.exe - [CPU - main thread, module Malware\_]

Assembly window (addresses 0040156F to 00401F08):

```

0040156F JEB 02 JMP SHORT Malware_.00401573
00401571 JBC 7 MOV EAX, EDI
00401573 JFC 5 CLD
00401574 JF 5F POP EDI
00401575 JC 9 LEAVE
00401576 C9 RETN
00401577 55 PUSH EBP
00401578 8BEC MOV EBP, ESP
0040157A 6A FF PUSH -1
0040157C 68 C0404000 PUSH Malware_.004040C0
00401581 68 3C204000 PUSH Malware_.0040203C
00401586 64:01 00000000 MOV EAX, DWORD PTR FS:[0]
0040158C 50 PUSH EAX
00401590 64:9225 000000 MOV DWORD PTR FS:[0], ESP
00401594 83EC 10 SUB ESP, 10
00401597 53 PUSH EBX
00401599 57 PUSH ESI
0040159A 57 PUSH EDI
0040159B 8965 E8 MOV DWORD PTR SS:[EBP-18], ESP
0040159D FF15 30404000 CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]
004015A3 33D2 XOR EDX, EDX
004015A5 80D4 MOV DL, AH
004015A7 9115 D4524000 MOV DWORD PTR DS:[4052D4], EDX
004015AD 8BC8 MOV ECX, EAX
004015AF 9115 FF000000 MOV ECX, DWORD PTR FS:[0]
004015B5 99D0 D0524000 MOV DWORD PTR DS:[4052D0], ECX
004015BB C1E1 08 SHL ECX, 8
004015BE ADD ECX, EDX
004015C0 99D0 CC524000 MOV DWORD PTR DS:[4052CC], ECX
004015C6 C1E8 10 SHR EAX, 10
004015C9 A3 C8524000 MOV DWORD PTR DS:[4052C8], EAX
004015CE 6A 00 PUSH 0
004015D0 E8 33090000 CALL Malware_.00401F08
  
```

Registers (FPU) window:

```

EAX 0A280105
ECX 00000001
EDI 00000001
EBX 7FFD4000
ESP 0012FF94
ESI FFFFFFFF
EDI 7C920208 ntdll.7C920208
EIP 004015B5 Malware_.004015B5
C 0 ES 0023 32bit 0 (FFFFFFFF)
P 1 CS 001B 32bit 0 (FFFFFFFF)
S 0 SS 0023 32bit 0 (FFFFFFFF)
D 0 DS 0023 32bit 0 (FFFFFFFF)
I 0 FS 003B 32bit 7FFDF000 (FFF)
T 0 GS 0000 NULL
D 0
0 0 LastErr ERROR_INVALID_HANDLE (00000000)
EFL 0000206 (NO, NB, NE, A, NS, PE, GE, G)
ST0 empty -UNORM BCBC 01050104 006F005C
ST1 empty 0.1077351297874321950e-4933
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
FCW 027F Prec NEAR, 53 Mask 1 1 1 1 1 1
  
```

Inserito un secondo breakpoint all'indirizzo di memoria 004015AF, il valore del registro ECX è "0A280105". Eseguito poi uno step-into, il valore di ECX diventa "00000005", perchè è stata eseguita l'istruzione "AND ECX, 0xFF" che esegue un'operazione logica di AND bit a bit tra il registro ECX e il valore immediato 0xFF. L'operatore AND restituisce 1 solo se entrambi i bit corrispondenti sono 1, altrimenti restituisce 0. Quindi traducendo il valore esadecimale di ECX e di 0xFF in bit, ed operando l'AND tra i bit di entrambi, si ottiene appunto il valore di 00000005.