

Facendo riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3 sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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?

00401061	6A 01	PUSH 1	InheritHandles = TRUE
00401063	6A 00	PUSH 0	pThreadSecurity = NULL
00401065	6A 00	PUSH 0	pProcessSecurity = NULL
00401067	68 30504000	PUSH Malware_.00405030	CommandLine = "cmd"
0040106C	6A 00	PUSH 0	ModuleFileName = NULL
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]	

Il valore del parametro è "CMD", ovvero il command prompt di Windows.

- 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?

00401551	8BEC	MOV EBP,ESP	
00401553	57	PUSH EDI	
00401554	8B7D 08	MOV EDI,DWORD PTR SS:[EBP+8]	
00401557	33C0	XOR EAX,EAX	
00401559	83C9 FF	OR ECX,FFFFFFFF	
0040155C	F2AE	REPNE SCAS BYTE PTR ES:[EDI]	
0040155E	41	INC ECX	
0040155F	F7D9	NEG ECX	
00401561	4F	DEC EDI	
00401562	8045 0C	MOV AL,BYTE PTR SS:[EBP+C]	
00401565	FD	STD	
00401566	F2AE	REPNE SCAS BYTE PTR ES:[EDI]	
00401568	47	INC EDI	
00401569	3B07	CMPL BYTE PTR DS:[EDI],AL	
0040156B	74 04	JE SHORT Malware_.00401571	
0040156D	33C0	XOR EAX,EAX	
0040156F	EB 02	JMP SHORT Malware_.00401573	
00401571	8BC7	MOV EAX,EDI	
00401573	FC	CWD	
00401574	5F	POP EDI	
00401575	C9	LEAVE	
00401576	C3	RETN	
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 01 00000000	MOV EAX,DWORD PTR FS:[0]	
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 04404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion]	kernel32.GetVersion
004015A3	3302	XOR EDX,EDX	
004015A5	80D4	MOV DL,AH	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D41],EDX	
004015A9	8B7D	MOV EDI,DWORD PTR SS:[EBP+8]	

Dopo aver configurato il breakpoint, clicchiamo "play". Il programma si ferma dunque all'istruzione XOR EDX,EDX. In questo caso il valore del registro EDX è "00001DB1".

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Options Window Help

Assembly window (disassembled code):

```

00401551 . 8BEC    MOV EBP,ESP
00401553 . 57      PUSH EDI
00401554 . 8B7D 08 MOV EDI,DWORD PTR SS:[EBP+8]
00401557 . 33C0    XOR EAX,EAX
00401559 . 8BC9 FF OR ECX,FFFFFFFF
0040155C . F2:RE   REPNE SCAS BYTE PTR ES:[EDI]
0040155E . 41      INC ECX
0040155F . F7D9    NEG ECX
00401561 . 4F      DEC EDI
00401562 . 8A45 0C MOV AL,BYTE PTR SS:[EBP+C]
00401565 . FD      STD
00401566 . F2:RE   REPNE SCAS BYTE PTR ES:[EDI]
00401568 . 47      INC EDI
00401569 . 3B07    CMP BYTE PTR DS:[EDI],AL
0040156B . 74 04   JE SHORT Malware_.00401571
0040156D . 33C0    XOR EAX,EAX
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 C0404000 PUSH Malware_.004040C0
00401581 . 68 3C204000 PUSH Malware_.0040203C
00401586 . 64:R1 00000000 MOV EAX,DWORD PTR FS:[0]
0040158C . 50      PUSH EAX
00401590 . 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
004015A3 . 33D2    XOR EDX,EDX
004015A5 . 8AD4    MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
  
```

Registers (FPU) window:

```

EAX 1DB10106
ECX 7EFD0000
EDI 00000000
EBX 7EFD0000
ESP 0018FF5C
EBP 0018FF58
ESI 00000000
EDI 00000000
EIP 004015A5 Malware_.004015A5
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 0.0
ST1 empty 0.0
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 (GT)
FCW 027F Prec NEAR,S3 Mask 1 1 1 1 1 1
  
```

Dopo lo “step-into”, viene dunque eseguita l’istruzione “XOR EDX,EDX”, che inizializza a zero una variabile. Dunque ora il valore di EDX è “0”.

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

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Options Window Help

Assembly window (disassembled code):

```

00401551 . 8BEC    MOV EBP,ESP
00401553 . 57      PUSH EDI
00401554 . 8B7D 08 MOV EDI,DWORD PTR SS:[EBP+8]
00401557 . 33C0    XOR EAX,EAX
00401559 . 8BC9 FF OR ECX,FFFFFFFF
0040155C . F2:RE   REPNE SCAS BYTE PTR ES:[EDI]
0040155E . 41      INC ECX
0040155F . F7D9    NEG ECX
00401561 . 4F      DEC EDI
00401562 . 8A45 0C MOV AL,BYTE PTR SS:[EBP+C]
00401565 . FD      STD
00401566 . F2:RE   REPNE SCAS BYTE PTR ES:[EDI]
00401568 . 47      INC EDI
00401569 . 3B07    CMP BYTE PTR DS:[EDI],AL
0040156B . 74 04   JE SHORT Malware_.00401571
0040156D . 33C0    XOR EAX,EAX
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 C0404000 PUSH Malware_.004040C0
00401581 . 68 3C204000 PUSH Malware_.0040203C
00401586 . 64:R1 00000000 MOV EAX,DWORD PTR FS:[0]
0040158C . 50      PUSH EAX
00401590 . 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
004015A3 . 33D2    XOR EDX,EDX
004015A5 . 8AD4    MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015A9 . 8BC9    MOV ECX,ECX
004015AB . 81E1 FF000000 AND ECX,0FFF
004015B5 . 8900 D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015B6 . C1E1 08 SHL ECX,2...
  
```

Registers (FPU) window:

```

EAX 1DB10106
ECX 1DB10106
EDI 00000001
EBX 7EFD0000
ESP 0018FF5C
EBP 0018FF58
ESI 00000000
EDI 00000000
EIP 004015AF Malware_.004015AF
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 0.0
ST1 empty 0.0
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 (GT)
FCW 027F Prec NEAR,S3 Mask 1 1 1 1 1 1
  
```

Facendo un procedimento analogo a quello fatto prima, configuriamo il breakpoint e notiamo che il valore del registro ECX è “1DB10106”.

The screenshot shows the OllyDbg interface with the assembly window displaying the following code:

```
00401551 . 8BEC MOV EBP,ESP
00401553 . 57 PUSH EDI
00401554 . 8B7D 08 MOV EDI,DWORD PTR SS:[EBP+8]
00401557 . 33C8 XOR EAX,EAX
00401559 . 83C9 FF OR ECX,FFFFFFFF
0040155C . F2AE REPNE SCAS BYTE PTR ES:[EDI]
0040155E . 41 INC ECX
0040155F . F7D9 NEG ECX
00401561 . 4F DEC EDI
00401562 . 8A45 0C MOV AL,BYTE PTR SS:[EBP+C]
00401565 . FD STD
00401566 . F2AE REPNE SCAS BYTE PTR ES:[EDI]
00401568 . 47 INC EDI
00401569 . 3B07 CMP BYTE PTR DS:[EDI],AL
0040156B . 74 04 JE SHORT Malware_.00401571
0040156D . 33C8 XOR EAX,EAX
0040156F . EB 02 JMP SHORT Malware_.00401573
00401571 . 8EC7 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
00401579 . 6A FF PUSH -1
0040157C . 68 C0404000 PUSH Malware_.004040C0
00401581 . 68 3C204000 PUSH Malware_.0040203C
00401586 . 6A 01 00000000 MOV EAX,DWORD PTR FS:[0]
0040158C . 50 PUSH EAX
00401590 . 64 8925 00000000 MOV DWORD PTR FS:[0],ESP
00401594 . 33EC 18 SUB ESP,18
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]
004015A2 . 33D2 XOR EDX,EDX
004015A5 . 8A04 MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015AD . 8BC8 MOV ECX,EAX
004015B0 . 31E1 FF000000 AND ECX,0FF
004015B5 . 8900 D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015B8 . C1E1 08 SHL ECX,8
004015BE . 05CA ADD ECX,EDX
```

The registers window on the right shows the following values:

Register	Value
EAX	10B1B106
ECX	00000006
EDX	00000001
EBX	7FDE0000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000
EIP	004015B5 Malware_.004015B5
EAX	ES 002B 32bit 0xFFFFFFFF
ECX	CS 002B 32bit 0xFFFFFFFF
EDX	SS 002B 32bit 0xFFFFFFFF
EBX	DS 002B 32bit 0xFFFFFFFF
ESP	FS 0053 32bit 7FDD0000(FFF)
EBP	GS 002B 32bit 0xFFFFFFFF
ESI	0 0
EDI	0 0
EIP	LastErr ERROR_SUCCESS (00000000)
EFL	00000206 (NO,HB,NE,R,NS,PE,GE,G)
ST0	empty 0.0
ST1	empty 0.0
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

Dopo lo “step-into”, viene dunque eseguita l’istruzione “AND ECX, FF”. Ora il valore di EDX è “00000006”. Questo risultato è ottenuto perché l’istruzione esegue l’AND logico sui bit di EAX e FF (valore esadecimale).