

S11/L3

Traccia: Fate 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.

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?

Vediamo che il parametro CommandLine è assegnato al valore "cmd" all'interno del programma, all'indirizzo 401067

0040105A	50	PUSH EAX	pStartupInfo
0040105B	6A 00	PUSH 0	CurrentDir = NULL
0040105D	6A 00	PUSH 0	pEnvironment = NULL
0040105F	6A 00	PUSH 0	CreationFlags = 0
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.C	CreateProcessA
00401074	8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	
00401077	6A FF	PUSH -1	Timeout = INFINITE
00401079	8B4D F0	MOV ECX,DWORD PTR SS:[EBP-10]	
0040107C	51	PUSH ECX	hObject
0040107D	FF15 00404000	CALL DWORD PTR DS:[<&KERNEL32.W	WaitForSingleObject
00401083	33C0	XOR EAX,EAX	
00401085	8BFC	MOV EBP,EBP	

2. Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?

Eseguite a questo punto uno «step-into».

00401577	55	PUSH EBP	
00401578	8BEC	MOV EBP,ESP	
00401579	6A FF	PUSH -1	
0040157C	68 C0404000	PUSH Malware_.004040C0	
00401581	68 30404000	PUSH Malware_.004030C0	
00401586	6441 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation
0040158C	50	PUSH EAX	
0040158D	6441 00000000	MOV EDI,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	
0040159C	FF15 00404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
0040159E	33D2	XOR EDX,EDX	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AC	8BCB	MOV ECX,EBX	
004015AF	01E1 FF000000	AND ECX,BF	
004015B5	01E0 D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	C1E1 00	SAL ECX,0	
004015BE	0BCA	ADD ECX,EDX	
004015C0	01E0 C0524000	MOV DWORD PTR DS:[4052C0],ECX	
004015C4	C1E1 10	SAR ECX,10	
004015C7	A3 C0524000	MOV DWORD PTR DS:[4052C0],EAX	
004015CC	6A 00	PUSH 0	
004015D0	E8 30090000	CALL Malware_.00401F08	
004015D5	59	POP ECX	
004015D8	0BCB	TEST ECX,ECX	
004015DB	75 08	JRC SHORT Malware_.004015E2	
004015DD	6A 1C	PUSH 1C	
004015E0	E8 74000000	CALL Malware_.00401678	
004015E1	59	POP ECX	
004015E2	8BFC 00	MOV EBP,ESP	

EAX	00401000
ECX	77F04000
EDX	00000000
EBX	77F04000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910200
EIP	004015A5 Malware_.004015A5
C 0	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
0 0	SS 0023 32bit 0(FFFFFFFF)
Z 1	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 002B 32bit 77F0000(FFF)
T 0	GS 0000 NULL
O 0	
D 0	LastErr ERROR_INVALID_HANDLE (00000006)
EFL	00000246 (NO,NO,E,OE,NS,PE,GE,LE)
ST0	empty +UNORM 8CB 01050104 005C0000
ST1	empty +UNORM 0069 006E0069 002E0067
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)
PCW	827F Prec NEAR,SS Rask 1 1 1 1 1 1

Il registro EDX contiene attualmente il valore 00000000, poiché è eseguita un'operazione XOR tra EDX e se stesso (EDX XOR EDX), il che restituisce sempre 0. Di conseguenza, il registro EDX viene inizializzato a zero

Indicate qual è ora il valore del registro EDX, motivando la risposta. Che istruzione è stata eseguita? 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:

The image displays two screenshots of a debugger window, likely OllyDbg, showing assembly code and the register window.

**Top Screenshot:**

- Assembly View:**
  - Address 00401577: 55 PUSH EBP
  - Address 00401578: 8BEC MOV EBP,ESP
  - Address 00401579: 6A FF PUSH -1
  - Address 0040157C: 68 C0404000 PUSH Malware\_..004040C0
  - Address 00401581: 68 3C204000 PUSH Malware\_..0040203C
  - Address 00401586: 64:41 00000000 MOV ECX,DMWORD PTR FS:[0]
  - Address 0040158C: 50 PUSH EAX
  - Address 00401590: 64:8925 00000000 MOV DMWORD PTR FS:[0],ESP
  - Address 00401594: 83EC 10 SUB ESP,10
  - Address 00401597: 53 PUSH EBX
  - Address 00401598: 56 PUSH ESI
  - Address 00401599: 57 PUSH EDI
  - Address 0040159A: 9965 E8 MOV DMWORD PTR SS:[EBP-10],ESP
  - Address 0040159B: FF15 30404000 CALL DMWORD PTR DS:[<&KERNEL32.GetVersion
  - Address 0040159C: 3302 XOR EDX,EDX
  - Address 0040159D: 9004 MOV DL,AH
  - Address 0040159E: 8915 04524000 MOV DMWORD PTR DS:[4052D4],EDX
  - Address 0040159F: 8B08 MOV ECX,EAX
  - Address 004015A0: 81E1 FF000000 AND ECX,0FF
  - Address 004015A1: 8900 D0524000 MOV DMWORD PTR DS:[4052D0],ECX
- Registers (FPU):**
  - EAX: 0A280105
  - ECX: 7FFDF000
  - EDX: 00000001
  - ESP: 0012FF94
  - EBP: 0012FFC0
  - ESI: FFFFFFFF
  - EDI: 7C910200
  - EIP: 004015A0

**Bottom Screenshot:**

- Assembly View:** (Same as top screenshot)
- Registers (FPU):**
  - EAX: 0A280105
  - ECX: 0A280105
  - EDX: 00000001
  - ESP: 0012FF94
  - EBP: 0012FFC0
  - ESI: FFFFFFFF
  - EDI: 7C910200
  - EIP: 004015AF

Il valore di ECX iniziale è 7FFDF000. Al secondo breakpoint, notiamo che il valore è 0A280105. Dalle istruzioni nel codice assembly, osserviamo che il contenuto di EAX viene trasferito in ECX e successivamente viene eseguita un'operazione AND tra ECX e 0FF. Se l'operazione restituisce un risultato vero, il valore di ECX viene modificato