

ESERCIZIO 3 SETTIMANA 11

- 1) Il valore del parametro <Command Line> che viene passato sullo stack è 'cmd' ovvero il command prompt di Windows.

00401057	. 8045 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	InheritHandles = 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	ModuleFileName = NULL
0040106C	. 6A 00	PUSH 0	CreateProcessA
0040106E	. FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.CreatePro	
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	

- 2) Il valore del registro EDX è 00001DB1

Registers (FPU)	
EAX	1DB10106
ECX	7EFDE000
EDX	00001DB1
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000
EIP	004015A3 Malware_.004015A3

3/4) Il valore di EDX dopo step-into è 00000000 quindi 0. Ci aspettiamo che sia 0 poiché dopo lo step-into viene eseguita l'istruzione XOR EDX,EDX che equivale ad inizializzare a 0 una variabile.

Registers (FPU)	
EAX	1DB10106
ECX	7EFDE000
EDX	00000000
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000

5) l'istruzione eseguita è XOR EDX,EDX

0040159A	. 8965 E8	MOV DWORD PTR
0040159D	. FF15 30404000	CALL DWORD PTR
004015A3	. 33D2	XOR EDX,EDX
004015A5	. 8AD4	MOV DL,AH
004015A7	. 8915 04524000	MOV DWORD PTR
004015AD	. 8BC8	MOV ECX,EAX
004015B0	. 81F1 FF000000	AND ECX,0FF

6) Il valore del registro ECX è 1DB10106

Registers (FPU)	
EAX	1DB10106
ECX	1DB10106
EDX	00000001
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000

7) Il valore dopo lo step into è 00000006

Registers (FPU)	
EAX	1DB10106
ECX	00000006
EDX	00000001
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000

8) L'istruzione eseguita è ECX,OFF

004015A7	. 8915 D4524000	MOV DWORD PTR
004015AD	. 8BC8	MOV ECX,EAX
004015AF	. 81E1 FF000000	AND ECX,0FF
004015B5	. 890D D0524000	MOV DWORD PTR
004015BB	C1E1 08	SHI ECX,8