

## PRATICA S11L3

1) Come si vede dall'immagine, il valore del parametro passato sullo stack è cmd

00401055	. 0055 F0	LEA EAX,DWORD PTR SS:[EBP-10]	pProcessInfo
00401056	. 52	PUSH EDX	
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	InheritHandles = TRUE
00401061	. 6A 01	PUSH 1	pThreadSecurity = NULL
00401063	. 6A 00	PUSH 0	pProcessSecurity = NULL
00401065	. 6A 00	PUSH 0	ModuleFileName = NULL
00401067	. 68 30504000	PUSH Malware_.00405030	CommandLine = "cmd"
0040106C	. 6A 00	PUSH 0	
0040106E	. FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.CreateProcessA]	CreateProcessA

2) Come si vede dall'immagine sotto nel riquadro di destra il valore in questo punto dell'esecuzione del registro EDX è 00000A28

0040157A	. 6A FF	PUSH -1	
0040157C	. 68 C0404000	PUSH Malware_.004040C0	
00401581	. 68 3C204000	PUSH Malware_.0040203C	SE handler installation
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	. 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
004015A5	. 3302	XOR EDX,EDX	
004015A7	. 80D4	MOV DL,AH	
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	. 8BC3	MOV ECX,EDX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 89D0 D8524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	
004015BE	. 83CA	ADD ECX,EDX	
004015C0	. 89D0 CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	
004015C7	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	. 6A 00	PUSH 0	
004015D0	. E8 33090000	CALL Malware_.00401F08	
004015D5	. 59	POP ECX	
004015D6	. 85C9	TEST EAX,EAX	
004015D8	. J75 08	JNZ SHORT Malware_.004015E2	
004015DA	. 6A 1C	PUSH 1C	
004015DC	. E8 9A000000	CALL Malware_.0040167B	
004015E1	. 59	POP ECX	
004015E2	. > 8365 FC 00	AND DWORD PTR SS:[EBP-4],0	
004015E6	. E8 72070000	CALL Malware_.00401D5D	

Andiamo ad eseguire uno step into, eseguendo quindi l'istruzione xor EDX,EDX. Lo xor di un valore con sé stesso darà zero come risultato, e in effetti vediamo che il valore di EDX ora risulta 0

0040157A	. 6A FF	PUSH -1	
0040157C	. 68 C0404000	PUSH Malware_.004040C0	
00401581	. 68 3C204000	PUSH Malware_.0040203C	SE handler installation
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	. 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
004015A5	. 3302	XOR EDX,EDX	
004015A7	. 80D4	MOV DL,AH	
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	. 8BC3	MOV ECX,EDX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 89D0 D8524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	
004015BE	. 83CA	ADD ECX,EDX	
004015C0	. 89D0 CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	
004015C7	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	. 6A 00	PUSH 0	
004015D0	. E8 33090000	CALL Malware_.00401F08	
004015D5	. 59	POP ECX	
004015D6	. 85C9	TEST EAX,EAX	
004015D8	. J75 08	JNZ SHORT Malware_.004015E2	
004015DA	. 6A 1C	PUSH 1C	
004015DC	. E8 9A000000	CALL Malware_.0040167B	
004015E1	. 59	POP ECX	
004015E2	. > 8365 FC 00	AND DWORD PTR SS:[EBP-4],0	
004015E6	. E8 72070000	CALL Malware_.00401D5D	
004015E8	. FF15 2C404000	CALL DWORD PTR DS:[&KERNEL32.GetCommand	GetCommandLineA

3) In modo simile al caso sopra, andiamo ad inserire un break point all'istruzione and ecx,off. Vediamo che prima di questa esecuzione il registro ecx vale 0A280105

0040157A	. 6A FF	PUSH -1	
0040157C	. 68 C0404000	PUSH Malware_.004040C0	
00401581	. 68 3C204000	PUSH Malware_.0040203C	SE handler installation
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	. 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
004015A5	. 3302	XOR EDX,EDX	
004015A7	. 80D4	MOV DL,AH	
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	. 8BC3	MOV ECX,EDX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 89D0 D8524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	
004015BE	. 83CA	ADD ECX,EDX	
004015C0	. 89D0 CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	
004015C7	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	. 6A 00	PUSH 0	
004015D0	. E8 33090000	CALL Malware_.00401F08	
004015D5	. 59	POP ECX	
004015D6	. 85C9	TEST EAX,EAX	
004015D8	. J75 08	JNZ SHORT Malware_.004015E2	
004015DA	. 6A 1C	PUSH 1C	
004015DC	. E8 9A000000	CALL Malware_.0040167B	
004015E1	. 59	POP ECX	
004015E2	. > 8365 FC 00	AND DWORD PTR SS:[EBP-4],0	
004015E6	. E8 72070000	CALL Malware_.00401D5D	
004015E8	. FF15 2C404000	CALL DWORD PTR DS:[&KERNEL32.GetCommand	GetCommandLineA

eseguiamo uno step into andando ad eseguire l'istruzione. Notiamo che ora il registro ecx vale 00000005. Questo è il risultato dell'AND logico a livello di bit fra i due registri ecx e l'esadecimale 000000FF.

The screenshot shows a debugger window with the following components:

- Assembly View:** Displays a list of instructions with their addresses and hex values. The instruction at address 00401585 is highlighted in red: `00401585 . 8B 15 MOV ECX, DS:[4052D4]`. Other instructions include `PUSH -1`, `PUSH Malware_.004040C0`, `MOV EAX, DWORD PTR FS:[0]`, `PUSH EAX`, `MOV DWORD PTR FS:[0], ESP`, `SUB ESP, 10`, `PUSH EBX`, `PUSH ESI`, `PUSH EDI`, `MOV DWORD PTR SS:[EBP-10], ESP`, `CALL DWORD PTR DS:[4052D4], EDX`, `MOV ECX, EAX`, `AND ECX, 0FF`, `MOV DWORD PTR DS:[4052D0], ECX`, `SHL ECX, 8`, `ADD ECX, EDX`, `MOV DWORD PTR DS:[4052CC], ECX`, `SHR EAX, 10`, `MOV DWORD PTR DS:[4052C8], EAX`, `PUSH 0`, `CALL Malware_.00401F08`, `POP ECX`, `TEST EAX, EAX`, `JNZ SHORT Malware_.004015E2`, `PUSH 1C`, `CALL Malware_.00401678`, `POP ECX`, `AND DWORD PTR SS:[EBP-4], 0`, and `CALL Malware_.00401D5D`.
- Registers (FPU) View:** Shows the current state of the registers. The `ECX` register is highlighted in red and contains the value `00000005`. Other registers include `EAX: 0A280185`, `EDX: 00000001`, `EBX: 7FFDF000`, `ESP: 0012FF94`, `EBP: 0012FFD0`, `ESI: FFFFFFFF`, `EDI: 7C920208`, and `EIP: 00401585`. The `CS` register is `001B`, `DS` is `0023`, `SS` is `0023`, `FS` is `003B`, and `GS` is `0000`. The `LastError` field shows `ERROR_INVALID_HANDLE (00000006)`.