

## Esercizio G3

1. Il valore passato da CommandLine è 'cmd'.

00401053	. 8D55 F0	LEA EDX,DWORD PTR SS:[EBP-10]	
00401056	. 52	PUSH EDX	
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.CreatePro	pProcessInfo
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	pStartupInfo
00401077	. 6A FF	PUSH -1	CurrentDir = NULL
00401079	. 8B4D F0	MOV ECX,DWORD PTR SS:[EBP-10]	pEnvironment = NULL
0040107C	. 51	PUSH ECX	CreationFlags = 0
0040107D	. FF15 00404000	CALL DWORD PTR DS:[<&KERNEL32.WaitForSi	InheritHandles = TRUE
00401083	. 33C0	XOR EAX,EAX	pThreadSecurity = NULL
00401085	. 8BE5	MOV ESP,EBP	pProcessSecurity = NULL
00401087	. 5D	POP EBP	CommandLine = "cmd"
00401088	. C3	RETN	ModuleFileName = NULL
00401089	. 55	PUSH EBP	
0040108A	. 8BEC	MOV EBP,ESP	CreateProcessA
0040108C	. 81EC 00010000	SUB ESP,100	
00401092	. 57	PUSH EDI	Timeout = INFINITE
00401093	. C785 F8FEFFFF	MOV DWORD PTR SS:[EBP-100],0	hObject
0040109D	. C685 00FFFFFF	MOV BYTE PTR SS:[EBP-100],0	WaitForSingleObject
004010A4	. B9 3F000000	MOV ECX,3F	
004010A9	. 33C0	XOR EAX,EAX	
004010AB	. 8DBD 01FFFFFF	LEA EDI,DWORD PTR SS:[EBP-FF]	
004010B1	. F3:AB	REP STOS DWORD PTR ES:[EDI]	
004010B3	. 66:AB	STOS WORD PTR ES:[EDI]	
004010B5	. AA	STOS BYTE PTR ES:[EDI]	
004010B6	. 8B45 08	MOV EAX,DWORD PTR SS:[EBP+8]	
004010B9	. 50	PUSH EAX	
004010BA	. F8 81030000	CALL Malware_.00401440	

00405030=Malware\_.00405030 (ASCII "cmd")

2. Il valore di EDX è 00000A28 (2600).

00401577 <Modu	. 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:A1 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation	
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	
004015A3	. 33D2	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	. 89AD D4524000	MOV DWORD PTR DS:[4052D4],ECX		

Valore di EDX dopo Step-info è 0. Questo perché gli XOR dello stesso oggetto danno come risultato 0.

00401577 <Modu	. 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:A1 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation	
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	
004015A3	. 33D2	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	. 89AD D4524000	MOV DWORD PTR DS:[4052D4],ECX		

4. Il valore di registro di ECX è 0A280105 (170393861)

00401590	. FF15 30404000	CALL DWORD PTR DS:[&KERNEL32.GetVersion]	kernel32.GetVersion
004015A3	. 33D2	XOR EDX,EDX	
004015A5	. 8AD4	MOV DL,AH	
004015A7	. 8915 04524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	. 8BC8	MOV ECX,EAX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 890D 00524000	MOV DWORD PTR DS:[4052D0],ECX	
004015BB	. C1E1 08	SHL ECX,8	
004015BE	. 03CA	ADD ECX,EDX	
004015C0	. 890D CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	
004015C9	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
ECX=0A280105			

Valore di ECX dopo Step-info è 00000005 (5), l'istruzione utilizzata è AND.

00401590	. 0000	MOV ECX,EAX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 890D 00524000	MOV DWORD PTR DS:[4052D0],ECX	
004015BB	. C1E1 08	SHL ECX,8	
004015BE	. 03CA	ADD ECX,EDX	
004015C0	. 890D CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	
004015C9	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
ECX=00000005			
DS:[004052D0]=00000000			