



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.

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? (1)

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

Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3)

motivando la risposta (4). Che istruzione è stata eseguita? (5)

Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6)

Eseguite un step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8)

Svolgimento:

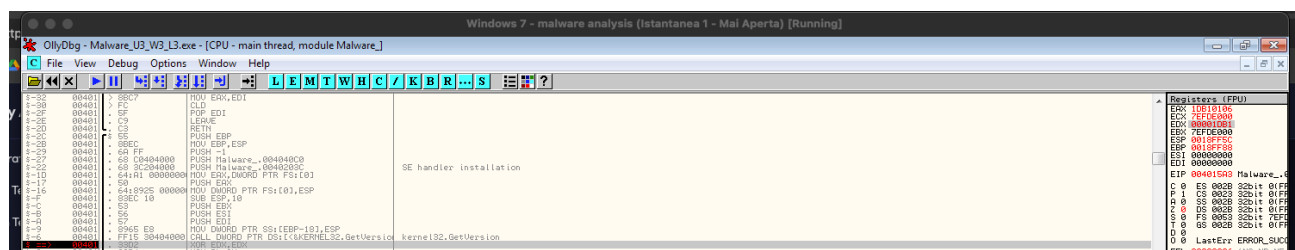
0040104D	. 8B4D E8	MOV ECX,DWORD PTR SS:[EBP-18]	
00401050	. 894D E4	MOV DWORD PTR SS:[EBP-1C],ECX	
00401053	. 8D55 F0	LEA EDX,DWORD PTR SS:[EBP-10]	
00401056	. 52	PUSH EDX	
00401057	. 8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]	
0040105A	. 50	PUSH EAX	
0040105B	. 6A 00	PUSH 0	
0040105D	. 6A 00	PUSH 0	
0040105F	. 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.CreateProcessA]	
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	

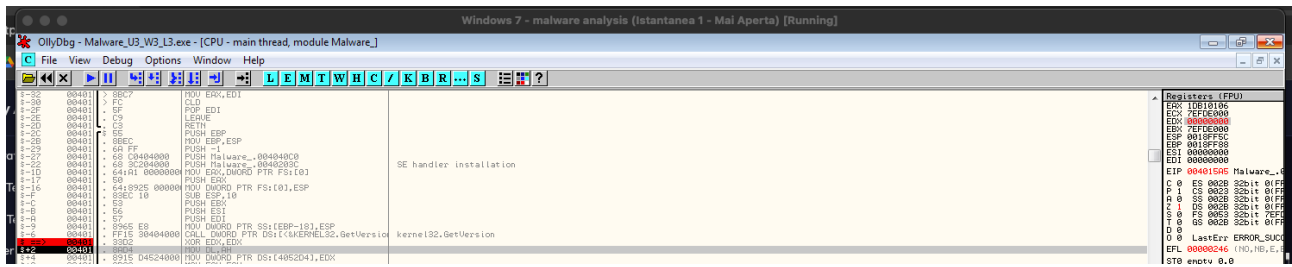
```

pProcessInfo
pStartupInfo
CurrentDir = NULL
pEnvironment = NULL
CreationFlags = 0
InheritHandles = TRUE
pThreadSecurity = NULL
pProcessSecurity = NULL
CommandLine = "cmd"
ModuleFileName = NULL
CreateProcessA

```

Il valore del parametro CommandLine è "cmd"

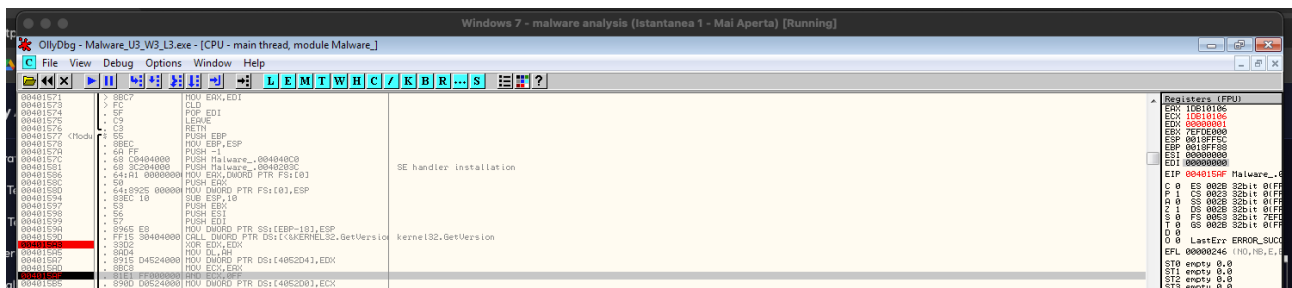




00401571	8BC7	MOV EAX, EDI	
00401572	75	JNZ 00401574	
00401573	5F	POP EDI	
00401574	5E	POP ESI	
00401575	5D	POP EBP	
00401576	5C	POP EBX	
00401577	5B	POP EAX	
00401578	5A	POP EAX	
00401579	59	POP EAX	
0040157A	58	POP EAX	
0040157B	57	POP EAX	
0040157C	56	POP EAX	
0040157D	55	POP EAX	
0040157E	54	POP EAX	
0040157F	53	POP EAX	
00401580	52	POP EAX	
00401581	51	POP EAX	
00401582	50	POP EAX	
00401583	4F	POP EAX	
00401584	4E	POP EAX	
00401585	4D	POP EAX	
00401586	4C	POP EAX	
00401587	4B	POP EAX	
00401588	4A	POP EAX	
00401589	49	POP EAX	
0040158A	48	POP EAX	
0040158B	47	POP EAX	
0040158C	46	POP EAX	
0040158D	45	POP EAX	
0040158E	44	POP EAX	
0040158F	43	POP EAX	
00401590	42	POP EAX	

Prima EDX valeva 1DB1, dopo valeva 0

E' stata eseguita XOR EDX,EDX che praticamente inizializza a zero il registro



00401571	8BC7	MOV EAX, EDI	
00401572	75	JNZ 00401574	
00401573	5F	POP EDI	
00401574	5E	POP ESI	
00401575	5D	POP EBP	
00401576	5C	POP EBX	
00401577	5B	POP EAX	
00401578	5A	POP EAX	
00401579	59	POP EAX	
0040157A	58	POP EAX	
0040157B	57	POP EAX	
0040157C	56	POP EAX	
0040157D	55	POP EAX	
0040157E	54	POP EAX	
0040157F	53	POP EAX	
00401580	52	POP EAX	
00401581	51	POP EAX	
00401582	50	POP EAX	
00401583	4F	POP EAX	
00401584	4E	POP EAX	
00401585	4D	POP EAX	
00401586	4C	POP EAX	
00401587	4B	POP EAX	
00401588	4A	POP EAX	
00401589	49	POP EAX	
0040158A	48	POP EAX	
0040158B	47	POP EAX	
0040158C	46	POP EAX	
0040158D	45	POP EAX	
0040158E	44	POP EAX	
0040158F	43	POP EAX	
00401590	42	POP EAX	

Prima ECX valeva 0001 poi viene fatta una AND e prende valore 0006 e dopo il suo contenuto viene spostato PTR DS: ecc...