

## 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).
- BONUS: spiegare a grandi linee il funzionamento del malware

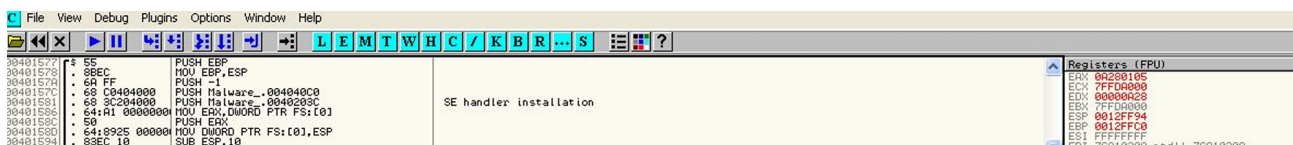
**All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?**

00401065	. 6A 00	PUSH 0	pProcessSecurity = NUL
00401067	. 68 30504000	PUSH Malware_.00405030	CommandLine = "cmd"
0040106C	. 6A 00	PUSH 0	ModuleFileName = NULL
0040106E	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreatePro	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.WaitForSi	WaitForSingleObject
00401083	. 33C0	XOR EAX,EAX	

Il valore che viene passato è cmd

**Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta (4). Che istruzione è stata eseguita?**

Prima il valore di edx è 00000A28



Dopo il valore sarà 0 perché viene eseguito `xor edx, edx`



**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.**

Prima il valore di ecx è 0A280105

00401570	8B4C	MOV ECX,ESP		ECX 0A280105
00401571	6A FF	PUSH -1		ECX 0A280105
00401572	68 004040C0	PUSH Malware_.004040C0		ECX 00000001
00401573	68 3C204000	PUSH Malware_.0040203C		ECX 7FFDA000
00401574	64:41 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation	ESP 0012FF94
00401575	50	PUSH EAX		EBP 0012FFC0
00401576	64:52 00000000	MOV DWORD PTR FS:[0],ESP		ESI FFFFFFFF
00401577	83EC 10	SUB ESP,10		EDI 7C910208

Dopo esser stata eseguita l'istruzione *and ecx, 0ff* il valore di ecx diventa 00000005

00401578	8B4C	MOV ECX,ESP		ECX 0A280105
00401579	6A FF	PUSH -1		ECX 00000005
0040157A	68 004040C0	PUSH Malware_.004040C0		ECX 00000001
0040157B	68 3C204000	PUSH Malware_.0040203C		ECX 7FFDA000
0040157C	64:41 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation	ESP 0012FF94
0040157D	50	PUSH EAX		EBP 0012FFC0
0040157E	64:52 00000000	MOV DWORD PTR FS:[0],ESP		ESI FFFFFFFF
0040157F	83EC 10	SUB ESP,10		EDI 7C910208
00401580	8B4C	MOV ECX,ESP		EIP 00401585 Malware_.00401585
00401581	6A FF	PUSH -1		C 0 ES 0023 32bit 0(FFFFFFF)
00401582	68 004040C0	PUSH Malware_.004040C0		P 1 CS 001E 32bit 0(FFFFFFF)
00401583	68 3C204000	PUSH Malware_.0040203C		Q 0 SS 0023 32bit 0(FFFFFFF)
00401584	64:41 00000000	MOV EAX,DWORD PTR FS:[0]	kernel32.GetVersion	Z 0 DS 0023 32bit 0(FFFFFFF)
00401585	50	PUSH EAX		S 0 FS 003B 32bit 7FFDF000
00401586	64:52 00000000	MOV DWORD PTR FS:[0],ESP		T 0 GS 0000 NULL
00401587	83EC 10	SUB ESP,10		D 0
00401588	8B4C	MOV ECX,ESP		0 0
00401589	6A FF	PUSH -1		0 0
0040158A	68 004040C0	PUSH Malware_.004040C0		0 0
0040158B	68 3C204000	PUSH Malware_.0040203C		0 0
0040158C	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
0040158D	50	PUSH EAX		0 0
0040158E	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
0040158F	83EC 10	SUB ESP,10		0 0
00401590	8B4C	MOV ECX,ESP		0 0
00401591	6A FF	PUSH -1		0 0
00401592	68 004040C0	PUSH Malware_.004040C0		0 0
00401593	68 3C204000	PUSH Malware_.0040203C		0 0
00401594	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
00401595	50	PUSH EAX		0 0
00401596	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
00401597	83EC 10	SUB ESP,10		0 0
00401598	8B4C	MOV ECX,ESP		0 0
00401599	6A FF	PUSH -1		0 0
0040159A	68 004040C0	PUSH Malware_.004040C0		0 0
0040159B	68 3C204000	PUSH Malware_.0040203C		0 0
0040159C	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
0040159D	50	PUSH EAX		0 0
0040159E	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
0040159F	83EC 10	SUB ESP,10		0 0
004015A0	8B4C	MOV ECX,ESP		0 0
004015A1	6A FF	PUSH -1		0 0
004015A2	68 004040C0	PUSH Malware_.004040C0		0 0
004015A3	68 3C204000	PUSH Malware_.0040203C		0 0
004015A4	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015A5	50	PUSH EAX		0 0
004015A6	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015A7	83EC 10	SUB ESP,10		0 0
004015A8	8B4C	MOV ECX,ESP		0 0
004015A9	6A FF	PUSH -1		0 0
004015AA	68 004040C0	PUSH Malware_.004040C0		0 0
004015AB	68 3C204000	PUSH Malware_.0040203C		0 0
004015AC	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015AD	50	PUSH EAX		0 0
004015AE	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015AF	83EC 10	SUB ESP,10		0 0
004015B0	8B4C	MOV ECX,ESP		0 0
004015B1	6A FF	PUSH -1		0 0
004015B2	68 004040C0	PUSH Malware_.004040C0		0 0
004015B3	68 3C204000	PUSH Malware_.0040203C		0 0
004015B4	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015B5	50	PUSH EAX		0 0
004015B6	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015B7	83EC 10	SUB ESP,10		0 0
004015B8	8B4C	MOV ECX,ESP		0 0
004015B9	6A FF	PUSH -1		0 0
004015BA	68 004040C0	PUSH Malware_.004040C0		0 0
004015BB	68 3C204000	PUSH Malware_.0040203C		0 0
004015BC	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015BD	50	PUSH EAX		0 0
004015BE	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015BF	83EC 10	SUB ESP,10		0 0
004015C0	8B4C	MOV ECX,ESP		0 0
004015C1	6A FF	PUSH -1		0 0
004015C2	68 004040C0	PUSH Malware_.004040C0		0 0
004015C3	68 3C204000	PUSH Malware_.0040203C		0 0
004015C4	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015C5	50	PUSH EAX		0 0
004015C6	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015C7	83EC 10	SUB ESP,10		0 0
004015C8	8B4C	MOV ECX,ESP		0 0
004015C9	6A FF	PUSH -1		0 0
004015CA	68 004040C0	PUSH Malware_.004040C0		0 0
004015CB	68 3C204000	PUSH Malware_.0040203C		0 0
004015CC	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015CD	50	PUSH EAX		0 0
004015CE	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015CF	83EC 10	SUB ESP,10		0 0
004015D0	8B4C	MOV ECX,ESP		0 0
004015D1	6A FF	PUSH -1		0 0
004015D2	68 004040C0	PUSH Malware_.004040C0		0 0
004015D3	68 3C204000	PUSH Malware_.0040203C		0 0
004015D4	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015D5	50	PUSH EAX		0 0
004015D6	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015D7	83EC 10	SUB ESP,10		0 0
004015D8	8B4C	MOV ECX,ESP		0 0
004015D9	6A FF	PUSH -1		0 0
004015DA	68 004040C0	PUSH Malware_.004040C0		0 0
004015DB	68 3C204000	PUSH Malware_.0040203C		0 0
004015DC	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015DD	50	PUSH EAX		0 0
004015DE	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015DF	83EC 10	SUB ESP,10		0 0
004015E0	8B4C	MOV ECX,ESP		0 0
004015E1	6A FF	PUSH -1		0 0
004015E2	68 004040C0	PUSH Malware_.004040C0		0 0
004015E3	68 3C204000	PUSH Malware_.0040203C		0 0
004015E4	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015E5	50	PUSH EAX		0 0
004015E6	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015E7	83EC 10	SUB ESP,10		0 0
004015E8	8B4C	MOV ECX,ESP		0 0
004015E9	6A FF	PUSH -1		0 0
004015EA	68 004040C0	PUSH Malware_.004040C0		0 0
004015EB	68 3C204000	PUSH Malware_.0040203C		0 0
004015EC	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015ED	50	PUSH EAX		0 0
004015EE	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015EF	83EC 10	SUB ESP,10		0 0
004015F0	8B4C	MOV ECX,ESP		0 0
004015F1	6A FF	PUSH -1		0 0
004015F2	68 004040C0	PUSH Malware_.004040C0		0 0
004015F3	68 3C204000	PUSH Malware_.0040203C		0 0
004015F4	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015F5	50	PUSH EAX		0 0
004015F6	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015F7	83EC 10	SUB ESP,10		0 0
004015F8	8B4C	MOV ECX,ESP		0 0
004015F9	6A FF	PUSH -1		0 0
004015FA	68 004040C0	PUSH Malware_.004040C0		0 0
004015FB	68 3C204000	PUSH Malware_.0040203C		0 0
004015FC	64:41 00000000	MOV EAX,DWORD PTR FS:[0]		0 0
004015FD	50	PUSH EAX		0 0
004015FE	64:52 00000000	MOV DWORD PTR FS:[0],ESP		0 0
004015FF	83EC 10	SUB ESP,10		0 0