

# CONSEGNA S11/L3

OllyDBG

## 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.

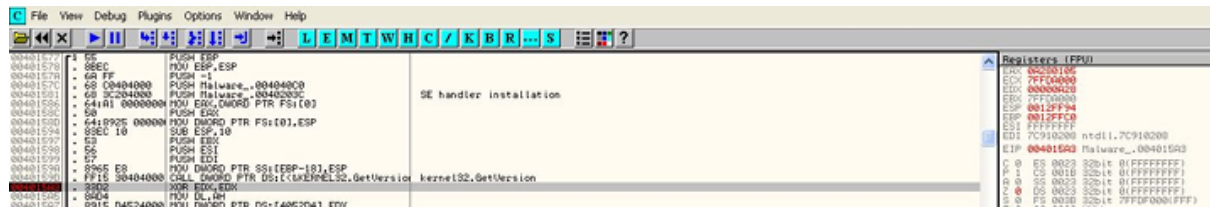
1. All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)
2. Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)
3. 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).
4. BONUS: Spiegare a grandi linee il funzionamento del malware

1 - Il valore del parametro è «**CMD**» ovvero il command prompt di Windows, come si nota nella figura sottostante all'indirizzo **00401067**

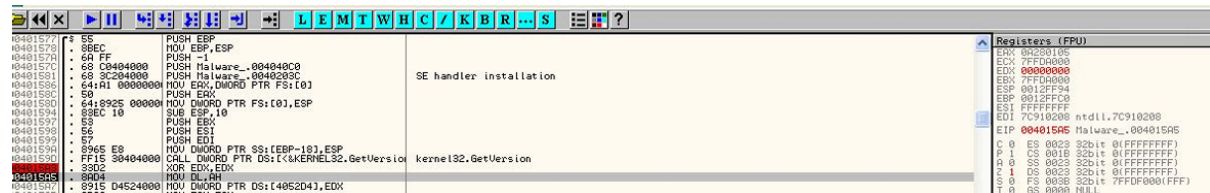
00401067	8D45 A8	LEA EAX, DWORD PTR SS:[EBP-58]	pStartupInfo
0040106A	50	PUSH EAX	CurrentDir = NULL
0040106B	6A 00	PUSH 0	pEnvironment = NULL
0040106D	6A 00	PUSH 0	CreationFlags = 0
0040106F	6A 00	PUSH 0	InheritHandles = TRUE
00401071	6A 01	PUSH 1	pThreadSecurity = NULL
00401073	6A 00	PUSH 0	pProcessSecurity = NULL
00401075	6A 00	PUSH 0	CommandLine = "cmd"
00401077	68 30504000	PUSH Malware_.00405030	ModuleFileName = NULL
00401079	6A 00	PUSH 0	
0040107B	FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.CreateProcessA]	CreateProcessA
0040107D	8945 EC	MOV DWORD PTR SS:[EBP-14], EAX	
0040107F	6A FF	PUSH -1	Timeout = INFINITE
00401081	8B4D F0	MOV ECX, DWORD PTR SS:[EBP-10]	hObject
00401083	51	PUSH ECX	WaitForSingleObject
00401085	FF15 00404000	CALL DWORD PTR DS:[&KERNEL32.WaitForSingleObject]	
00401087	33C0	XOR EAX, EAX	
00401089	8BE5	MOV ESP, EBP	
0040108B	5D	POP EBP	
0040108D	C3	RETN	

2 - Una volta settato il breakpoint andiamo a cliccare su "play", il programma si fermerà all'istruzione XOR EDX,EDX. Prima che l'istruzione venga eseguita il valore del registro è "00000A28". Successivamente allo step-into viene eseguita l'istruzione XOR EDX,EDX che di fatto equivale ad inizializzare a zero una variabile. Questo vuol dire che dopo lo step-into il valore di EDX sarà 0.

Prima:

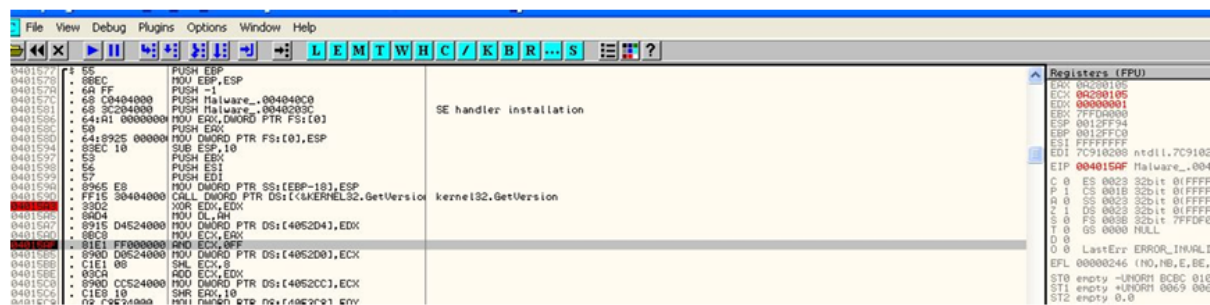


Dopo:



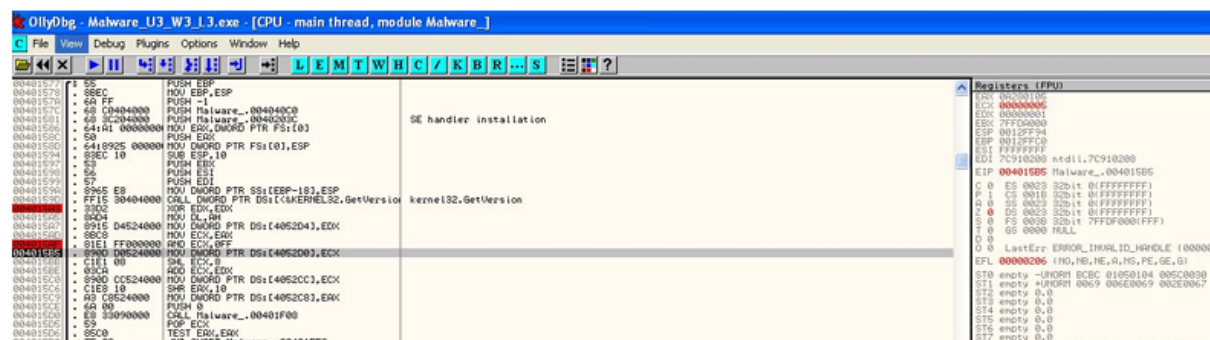
3 - Configuriamo il secondo breakpoint. Il valore del registro ECX è "0A280105".

Prima:



Dopo lo step-into il valore del registro ECX è stato modificato in "00000005" in quanto è stata eseguita l'istruzione AND ECX, FF.

Dopo:



L'istruzione esegue l'AND logico sui bit di EAX e del valore esadecimale FF. Per prima cosa riportiamo entrambi i valori in formato binario e poi eseguiamo l'AND logico tra i bit.

ESADECIMALE	BINARIO
0A280105	0000 1010 0010 1000 0000 0001 0000 0101
FF	0000 0000 0000 0000 0000 0000 1111 1111

Eseguendo l'AND logico tra i bit uno ad uno il risultato è:

**0000 0000 0000 0000 0000 0000 0000 0101**

Ecco spiegato il valore di ECX dopo l'istruzione AND ECX, 0FF.