

# Esercizio Epicode 06.12.2023

## Ollydbg

Con riferimento al Malware\_U3\_W3\_L3, presente all'interno della cartella Esercizio\_Pratico\_U3\_W3\_L3. Rispondere 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?

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

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	CommandLine = "cmd"
00401067	68 30504000	PUSH Malware_.00405030	ModuleFileName = NULL
0040106C	6A 00	PUSH 0	CreateProcessA
0040106E	FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreatePro	
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	
00401085	8BE5	MOV ESP,EBP	
00401087	5D	POP EBP	

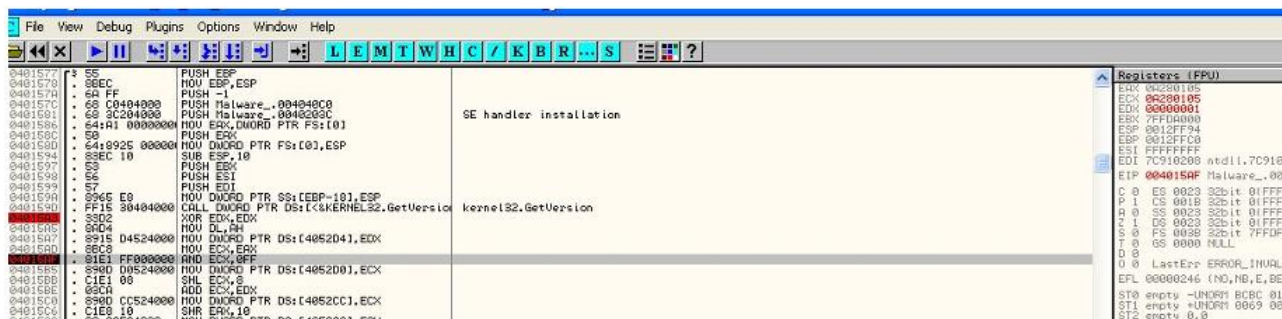
Inserire un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguire uno «step-into». Indicare qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

Una volta configurato il breakpoint, clicchiamo su «play», il programma si fermerà all'istruzione XOR EDX,EDX. Prima che l'istruzione venga eseguita il valore del registro è «00000A28». Dopo lo step-into, viene eseguita l'istruzione XOR EDX,EDX che di fatto equivale ad inizializzare a zero una variabile. Quindi, dopo lo step-into il valore di EDX sarà 0.

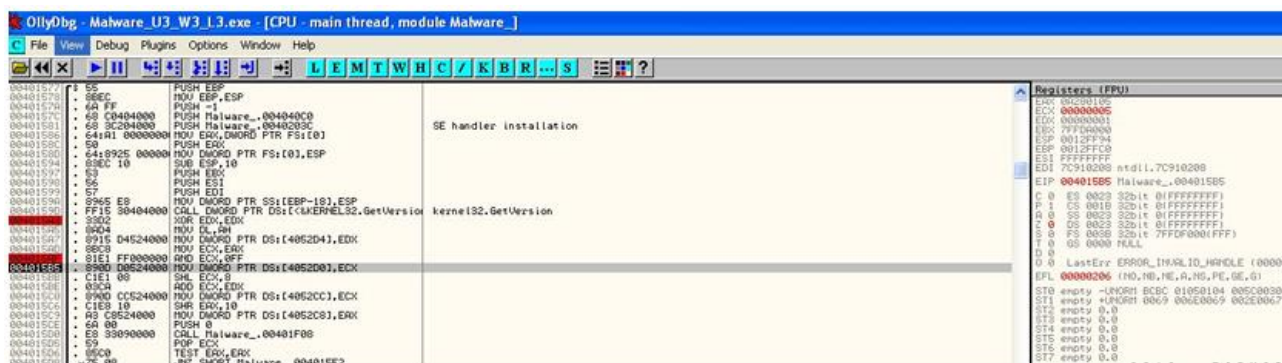


Inserire un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguire uno step-into. Qual è ora il valore di ECX? Spiegare quale istruzione è stata eseguita.

Configuriamo il secondo breakpoint. Il valore del registro ECX è «0A280105».



dopo lo step-into il valore del registro ECX è stato modificato in «00000005» in quanto è stata eseguita l'istruzione AND ECX, FF



Nel dettaglio, l'istruzione esegue l'AND logico sui bit di EAX e del valore esadecimale FF. Per prima cosa portiamo 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

0000 0000 0000 0000 0000 0000 0000 0101

**Che in Esadecimale è 00000005**

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