

The background is a dark blue gradient with a subtle pattern of white dots. On the left side, there are several concentric circles and a large arc with a scale. The scale has numbers ranging from 140 to 260 in increments of 10. There are also some smaller circles and arrows scattered across the background.

# MALWARE ANALYSIS

ANALISI STATICA - IDA PRO

S11/L3

In 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).

- ❑ 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?

00401056	. 52	PUSH EDX	pProcessInfo
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	ModuleFileName = NULL
00401067	. 68 30504000	PUSH Malware_.00405030	CommandLine = "cmd"
0040106C	. 6A 00	PUSH 0	ModuleFileName = NULL
0040106E	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA	CreateProcessA
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	Timeout = INFINITE
00401077	. 6A FF	PUSH -1	hObject
00401079	. 8B4D F0	MOV ECX,DWORD PTR SS:[EBP-10]	WaitForSingleObject
0040107C	. 51	PUSH ECX	
0040107D	. FF15 00404000	CALL DWORD PTR DS:[<&KERNEL32.WaitForSingleObject	
00401083	. 33C0	XOR EAX,EAX	
00401085	. 8BE5	MOV ESP,EBP	
00401087	. 5D	POP EBP	
00401088	. C3	RETN	

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

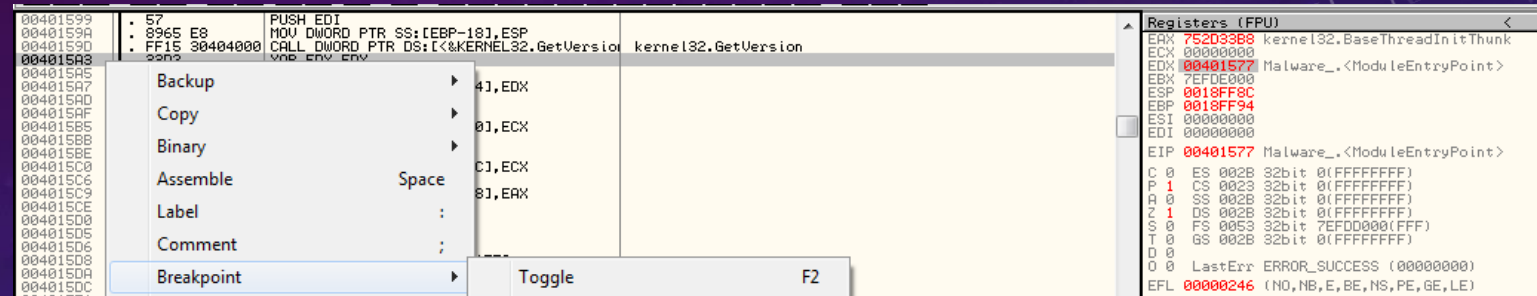


❑ Inserite un breakpoint software all'indirizzo 004015A3.

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. Che istruzione è stata eseguita?

Nella seconda parte dell'esercitazione, ci siamo spostati all'allocazione di memoria 004015A3 e abbiamo impostato un breakpoint su una specifica istruzione nel programma.

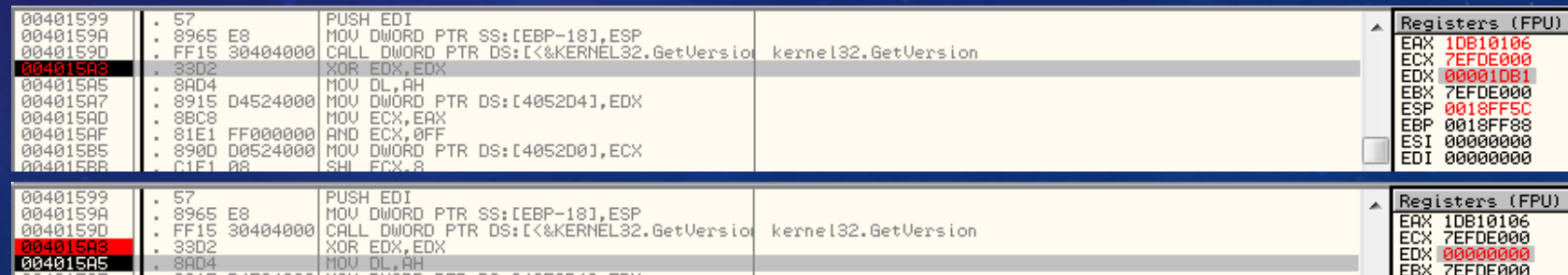


Dopo aver interrotto l'esecuzione del programma, abbiamo controllato il valore del registro EDX, che abbiamo trovato essere 00001DB1.

Successivamente, abbiamo riavviato l'esecuzione del programma cliccando sul tasto "play" nella barra degli strumenti. Attraverso la finestra "Registers FPU", abbiamo verificato che il valore nel registro EDX rimanesse lo stesso.

Successivamente, abbiamo utilizzato la funzione "Step-into" nella barra degli strumenti, che ci ha permesso di entrare nel codice della funzione in esame. Durante questo passaggio, abbiamo notato che il valore del registro EDX è cambiato in 00000000.

Questo cambiamento è dovuto all'operazione logica XOR nel codice, che restituisce sempre 0 quando applicata a due valori uguali. In questo caso, l'operazione XOR ha annullato il valore precedente di EDX, impostandolo a zero.



- ❑ 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

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
004015A5	33D2	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015A8	8BC8	MOV ECX,EAX	
004015AF	81E1 FF000000	AND ECX,0FF	
004015B5	890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	C1E1 08	SHL ECX,8	
004015BF	93C9	ADD ECX,EBX	

Registers (FPU)  
EAX 1DB10106  
ECX 7EFDE000  
EDX 00000000  
EBX 7EFDE000  
ESP 0018FF5C  
EBP 0018FF88  
ESI 00000000  
EDI 00000000  
EIP 004015A5 Malware\_.004015A5

Configuriamo il secondo breakpoint. Il valore del registro ECX è «1DB10106».

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
004015A5	33D2	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015A8	8BC8	MOV ECX,EAX	
004015AF	81E1 FF000000	AND ECX,0FF	
004015B5	890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	C1E1 08	SHL ECX,8	

Registers (FPU)  
EAX 1DB10106  
ECX 1DB10106  
EDX 00000001  
EBX 7EFDE000  
ESP 0018FF5C  
EBP 0018FF88  
ESI 00000000  
EDI 00000000  
EIP 004015AF Malware\_.004015AF

Dopo lo step-into il valore del registro ECX è stato modificato in «00000006» in quanto è stata eseguita l'istruzione AND ECX, FF. In questo caso abbiamo un operato logico AND il quale ricevendo in ingresso almeno due valori restituisce 1 solo se tutti i valori di ingresso hanno valore 1.

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
004015A5	33D2	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015A8	8BC8	MOV ECX,EAX	
004015AF	81E1 FF000000	AND ECX,0FF	
004015B5	890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	C1E1 08	SHL ECX,8	

Registers (FPU)  
EAX 1DB10106  
ECX 00000006  
EDX 00000001  
EBX 7EFDE000  
ESP 0018FF5C  
EBP 0018FF88  
ESI 00000000  
EDI 00000000  
EIP 004015B5 Malware\_.004015B5