

OlllyDBG

ESERCIZIO

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).

Parametro «CommandLine»

Il valore del parametro «CommandLine» che viene passato sullo stack è **“cmd”**

00401053	. 8B33 18	LEA EDI,DWORD PTR SS:[EBP-18]	pProcessInfo
00401056	. 52	PUSH EDI	pStartupInfo
00401057	. 8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]	CurrentDir = NULL
0040105A	. 50	PUSH EAX	pEnvironment = NULL
0040105B	. 6A 00	PUSH 0	CreationFlags = 0
0040105D	. 6A 00	PUSH 0	InheritHandles = TRUE
0040105F	. 6A 00	PUSH 0	pThreadSecurity = NULL
00401061	. 6A 01	PUSH 1	pProcessSecurity = NULL
00401063	. 6A 00	PUSH 0	CommandLine = "cmd"
00401065	. 6A 00	PUSH 0	ModuleFileName = NULL
00401067	. 68 30504000	PUSH Malware_.00405030	CreateProcessA
0040106C	. 6A 00	PUSH 0	
0040106E	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreatePro	
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	

Valore registro EDX

Cliccando col destro e scegliamo la voce Breakpoint sull'indirizzo 004015A3

0040159A	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
0040159D	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	. 33D2	XOR EDX,EDX	
004015A5	. 8AD4	MOV DL,AH	
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	. 8BC8	MOV ECX,EAX	

```
ECX 7FFD4000
EDX 00000A28
EBX 7FFD4000
ESP 00405504
```

Dopo lo step-in il valore del registro EDX è cambiato in:

```
ECX 7FFD4000
EDX 00000000
EBX 7FFD4000
ESP 00405504
```

poichè l'istruzione XOR EDX,EDX inizializza la variabile a 0

Valore registro ECX

Cliccando col destro e scegliamo la voce Breakpoint sull'indirizzo 004015AF

004015A5	• 3302	XOR EDX,EDX
004015A5	• 8AD4	MOV DL,AH
004015A7	• 8915 04524000	MOV DWORD PTR DS:[4052D4],EDX
004015AD	• 8BC8	MOV ECX,EAX
004015AF	• 81E1 FF000000	AND ECX,0FF
004015B5	• 890D 00524000	MOV DWORD PTR DS:[4052D0],ECX
004015B8	• C1E1 08	SHL ECX,8

EAX	0A280105
ECX	0A280105
EDX	00000001
EBX	75F04000

Dopo lo step-in il valore del registro ECX è cambiato in:

EAX	0A280105
ECX	00000005
EDX	00000001
EBX	75F04000

l'istruzione AND ECX, 0ff fa si che i bit in ECX vengano confrontati con 0ff, e se i bit in colonna sono entrambi 1 restituirà 1, altrimenti sarà 0. Dopo l'AND i bit vengono tradotti in esadecimale e il risultato sarà appunto 0000.0005