



S11-L3

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



Dopo aver inserito un breakpoint toggle proseguiamo avviando l'esecuzione del programma, dirigendoci nuovamente dove abbiamo inserito il breakpoint, come possiamo notare ci verrà restituito il valore di "CommandLine"

00401061	. 6A 01	PUSH 1	InheritHandles = TRUE
00401063	. 6A 00	PUSH 0	pThreadSecurity = NULL
00401065	. 6A 00	PUSH 0	pProcessSecurity = 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	



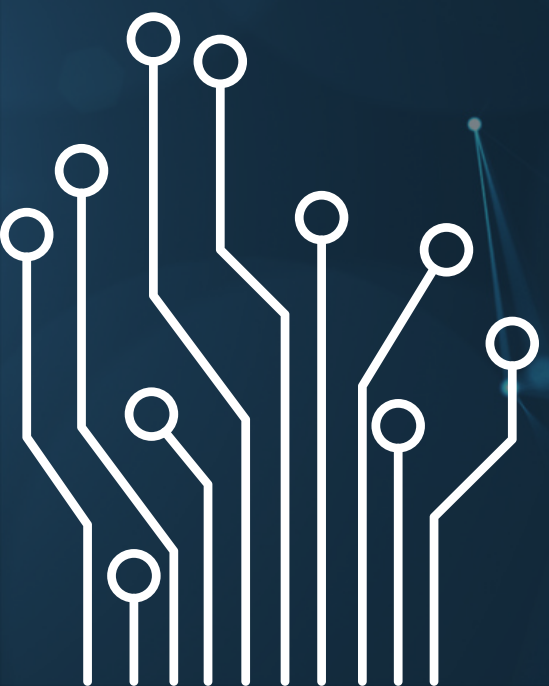


Anche in questo caso dopo aver inserito il breakpoint ed aver avviato l'esecuzione del programma, possiamo controllare i valori dei registri prima dell'istruzione

```
EAX 10B10106  
ECX 7EFDE000  
EDX 000010B1  
EBX 7EFDE000
```

a seguito di un'operazione XOR tra lo stesso registro (xor edx,edx), il risultato sarà sempre 0

```
EAX 10B10106  
ECX 7EFDE000  
EDX 00000000  
EBX 7EFDE000  
ESP 0018FF5C
```



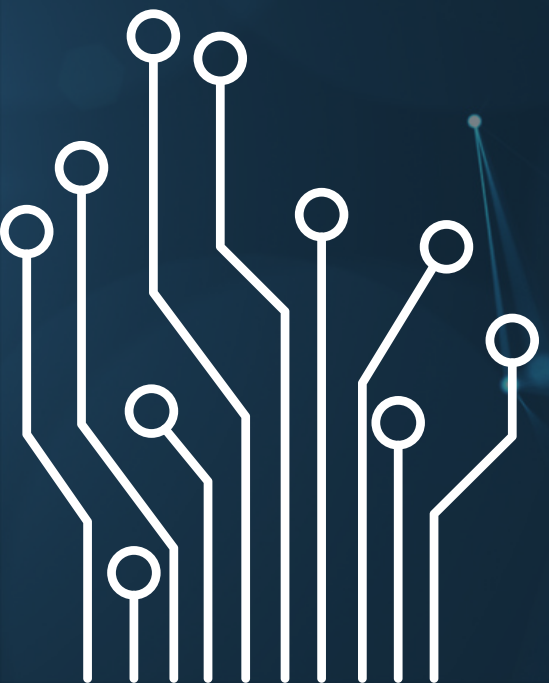


Il valore del registro ECX nell'indirizzo di memoria specificato risulta essere il seguente:

EAX	10B10106
ECX	10B10106
EDX	00000001

successivamente viene eseguita un'operazione logica AND bit a bit tra il registro ECX e il valore immediato 0xFF, l'operazione AND imposta a 1 solo i bit in ECX che corrispondono a 1 in 0xFF, mentre i restanti bit vengono impostati a 0.

EAX	10B10106
ECX	00000006
EDX	00000001





Il malware in questione potrebbe essere una backdoor, in quanto sono presenti molti elementi che riportano a questa tipologia di malware, sia direttamente all'interno del codice, sia attraverso le varie funzioni che vengono importate e utilizzate dallo stesso.

