

# S11L3

OlllyDBG

*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 OlllyDBG.

- 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).

1)

00401065	: 64 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.CreatePro	CreateProcessA

Il valore del parametro «CommandLine» passato nello stack è "cmd"

2)

0040159D	: FF15 30404000	CALL DWORD PTR
004015A3	: 33D2	XOR EDX,EDX

inseriamo il breakpoint e avviamo l'esecuzione del programma tramite OlllyDBG

EDX	00000A28
-----	----------

al breakpoint questo è il valore del registro EDX

3)

EDX	00000000
-----	----------

eseguendo un step-into il registro cambia il suo valore a 00000000, (4,5) per via dello XOR effettuato all'interno dell'istruzione che avevamo bloccato.

6)

0040159D	: 0B00	MOV ECX,EAX
004015AF	: 81E1 FF000000	AND ECX,0FF
004015BE	: 0000 00000000	MOV EAX,0

al breakpoint questo è il valore del registro ECX

ECX	0A280105
-----	----------

7)



eseguendo un step-into il registro cambia il suo valore a 00000005 **(8)** per via dell'AND effettuato all'interno dell'istruzione che avevamo bloccato.

**(Bonus)**

**Ipotizziamo che il malware sia una backdoor, esso infatti crea un socket e aspetta una connessione in entrata**