


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

1. 

Il valore del parametro di CommandLine è “cmd” cioè il command prompt di windows

2. 

Il valore del registro di EDI è 1, dopo aver fatto un breakpoint andiamo ad eseguire uno step-into, dato che lo step-into ci permette di iniziare il codice da dove è inserito, il valore del registro diventa 0 perchè è la prima riga ad essere eseguita.

3. 

Dopo aver eseguito un secondo breakpoint nell'indirizzo di memoria 004015AF il valore del registro ECX è “0A280105”. Ora eseguiamo lo step-into sul registro ECX ed il valore di ECX diventa “00000005” data l'esecuzione di AND ECX, FF.