## Traccia:

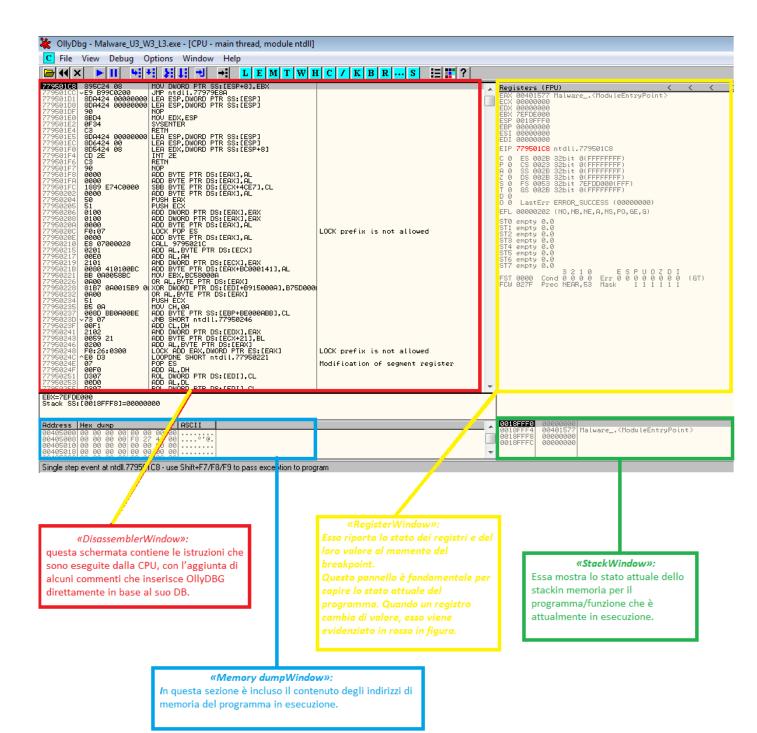
Fate riferimento al malware: Malware\_U3\_W3\_L3, presente all'interno della cartella Esercizio\_Pratico\_U3\_W3\_L3 sul desktop della macchina virtuale dedicata all'analisi dei malware.

Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 1. 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)
- 2. 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)
- 3. Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite uno step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).

**OllyDbg** è un debugger per il software di tipo reverse engineering, comunemente utilizzato per analizzare e modificare programmi binari eseguibili. È popolare tra gli sviluppatori di software, ricercatori di sicurezza e appassionati di hacking per esaminare il funzionamento interno di programmi e identificare vulnerabilità o comportamenti indesiderati.

Avviato il tool sulla nostra macchina virtuale ed aperto il malware da analizzare ci troveremo di fronte questa schermata:



Nella tabella di seguito trovate la funzione, una descrizione della funzione e la relativa icona mostrata da OllyDBG.

FUNZIONE	ICONA	DESCRIZIONE
Run / Play		Viene utilizzato per eseguire il programma che è stato precedentemente caricato in OllyDBG
Pausa	Ш	Viene utilizzato per stoppare un programma durante la sua esecuzione
Step-into	4	Utilizzato per esaminare righe di codice e a fronte di una chiamata di funzione accedere alla sua implementazione
Step-over	+:	Utilizzato per esaminare righe di codice singola. A fronte di una chiamata di una funzione permette di saltare l'implementazione della funzione

1. -----

All'indirizzo **0040106E** il Malware effettua una chiamata alla funzione "CreateProcess"; il valore del parametro "CommandLine" è visibile all'indirizzo **00401067**, ovvero CMD → command prompt di Windows:



2.-----

Andiamo ora all'indirizzo indicato in esercizio, ovvero **004015A3**, configuriamo un breackpoint ed eseguiamo premendo su play. Come possiamo vedere in figura il programma si fermerà all'istruzione *XOR EDX*, *EDX*. Prima che l'istruzione venga eseguita il valore del registro è **00401577**:

Ora clicchiamo sul tasto per eseguire lo *step-into*. Come si può vedere una volta eseguita la funzione *XOR EDX*, *EDX* il valore di **EDX** sarà **0**, in quanto eseguire lo step-into equivale ad inizializzare a zero la funzione:

3.-----

Facciamo un'altra prova, andiamo all'indirizzo **004015AF** come da istruzione, impostiamo un breackpoint, avviamo con play, notiamo che il valore di **ECX** è **1DB10106**.

In seguito allo step-into [ il valore di **ECX cambia in 0000006** in quanto viene eseguita l'istruzione AND ECX, FF:

