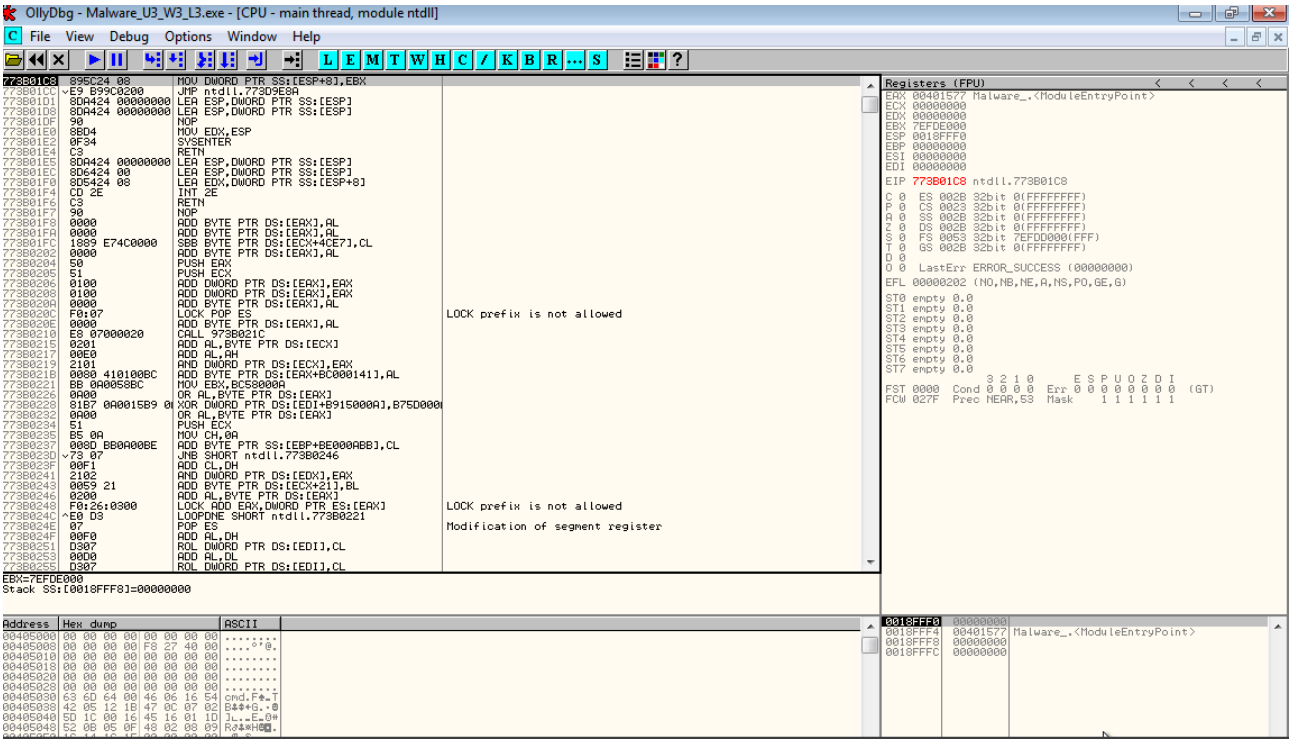
Amarfii Adrian 18/01/2023
Report
Task

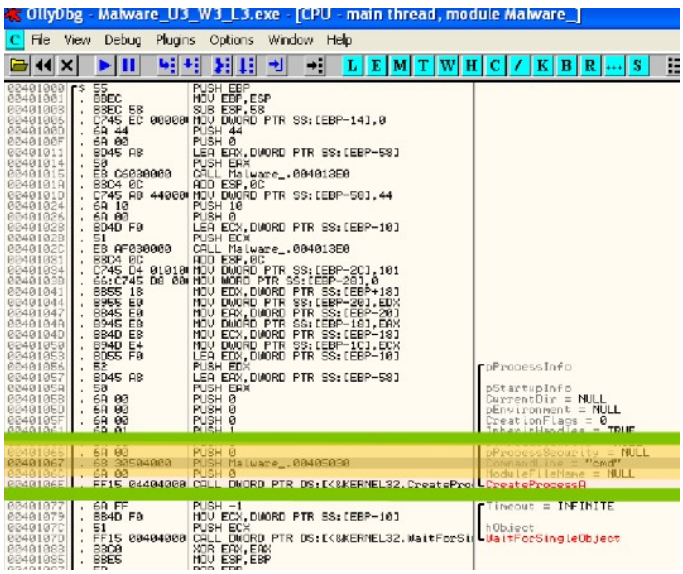
Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3 sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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?
- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?
- Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

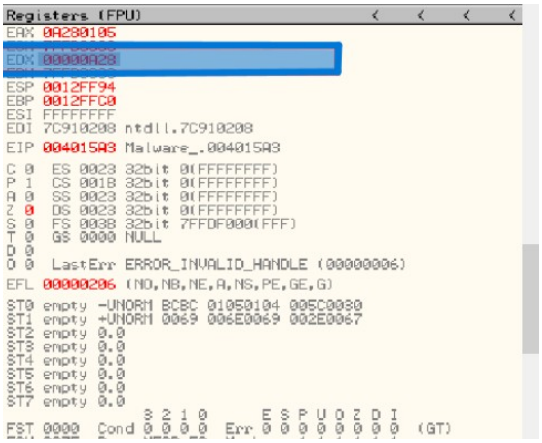
Andiamo sulla nostra machina e andiamo ad aprire OllyDBG e selezioneamo il file richiesto.



Andiamo all'indirizzo che ci da la traccia 0040106E e notiamo che nel Command Line viene fatto un push e il valore è Malware_00405030.



Andiamo al indirizzo 004015A3 e mettiamo un breakpoint e vediamo il comportamento del registro EDX prima e dopo .Prima il valore di EDX è uguale a 00000A28. Dopo aver fatto un step into notiamo che il registro EDX viene inizializzato a 0.



Come abbiamo fatto sopra andiamo al indirizzo 004015AF e faciamo lo stesso procedimento che abbiamo fatto sopra .Inizialmente il valore del registro ECX è 0A280105 dopo il step-into il valore cambia in 00000005 .Viene prima processato l'operatore logico AND che prende i valori ECX e off.AND nasconde alcuni bit di un determinato dato e azzera questo a 0 che corrispondono a un dato valore .