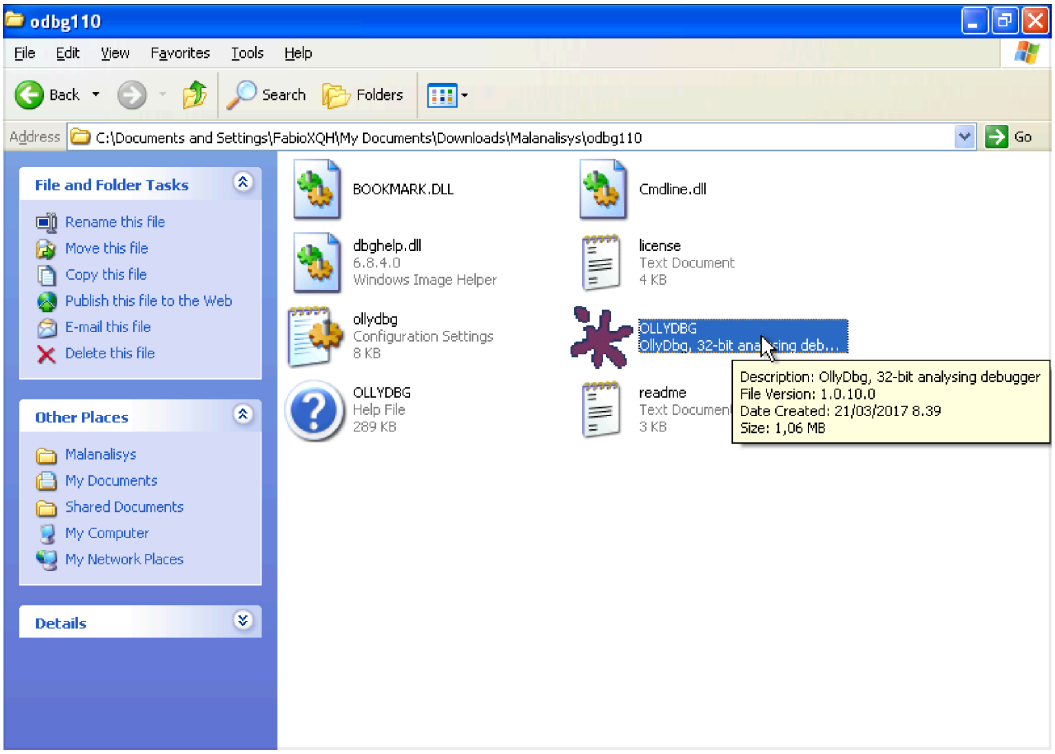
ANALISI DINAMICA AVANZATA CON OllyDGB

Traccia:

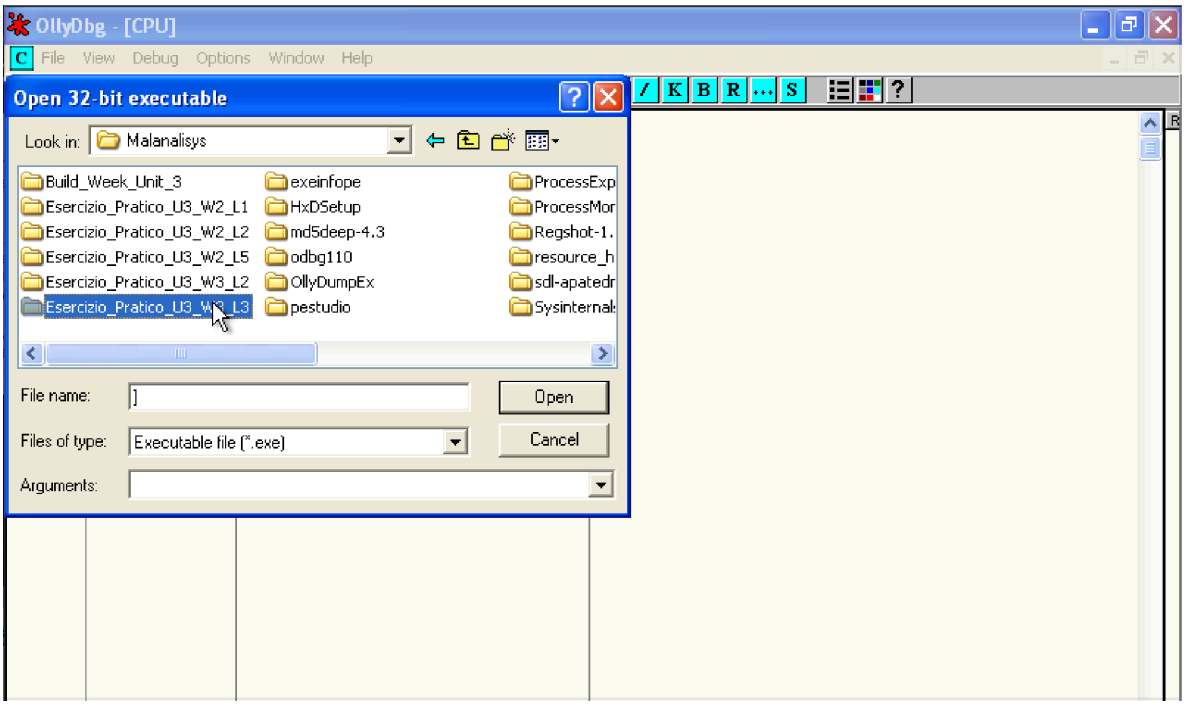
Fate riferimento al malware: **Malware_U3_W3_L3**, presente all'interno della cartella **Esercizio_Pratico_U3_W3_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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

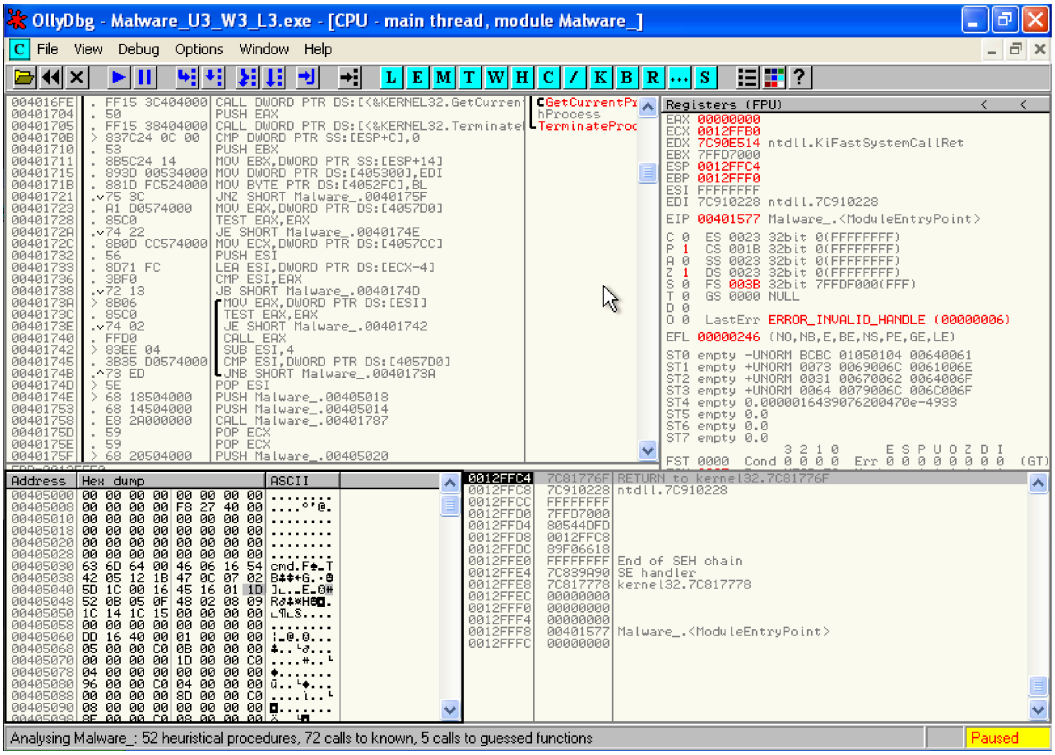
Per prima cosa andiamo ad aprire il programma "OLLYDBG" contenuto nella nostra macchina virtuale.



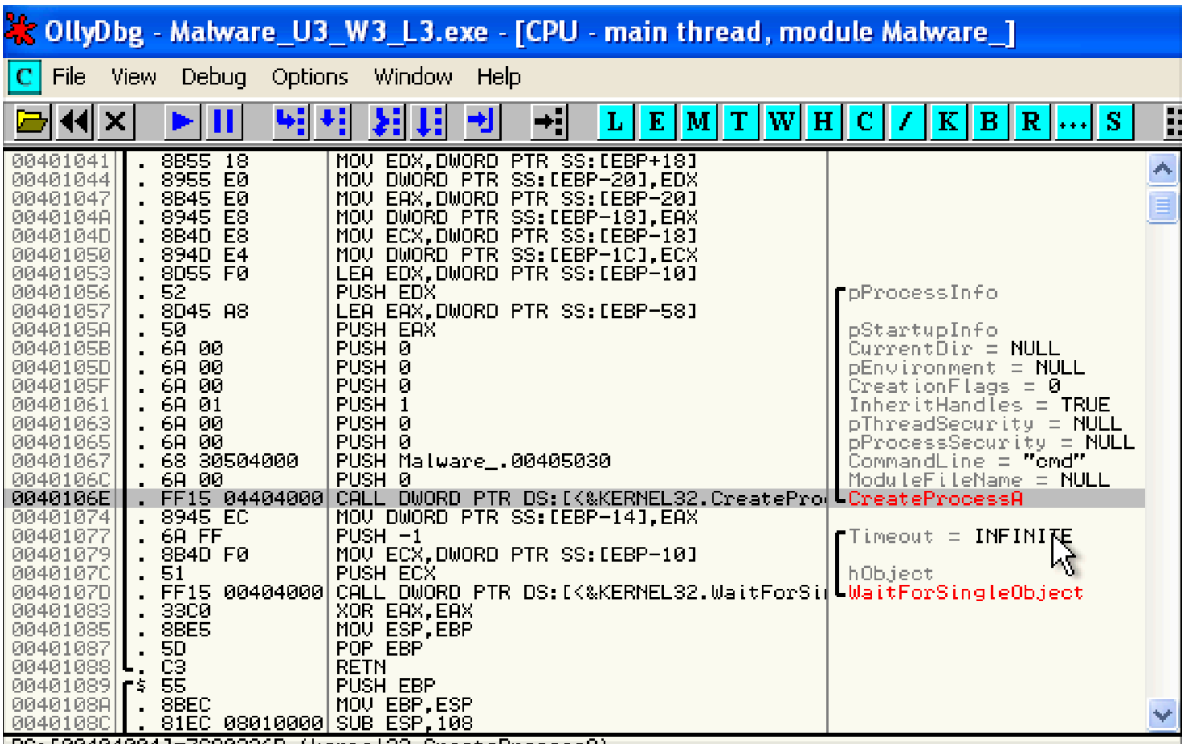
Una volta all'interno del programma andiamo a prelevare il file che vogliamo analizzare cliccando sull'icona Open new executable in alto a sinistra.



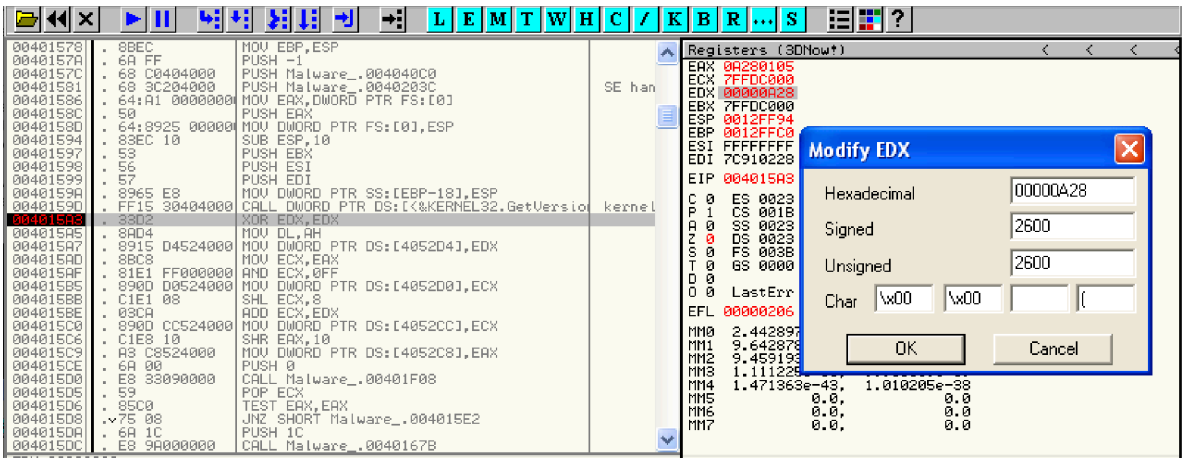
Selezionato il file ci ritroveremo questa schermata dove sono indicati i diversi indirizzi di memoria, registri e processi che il malware andrà ad eseguire.



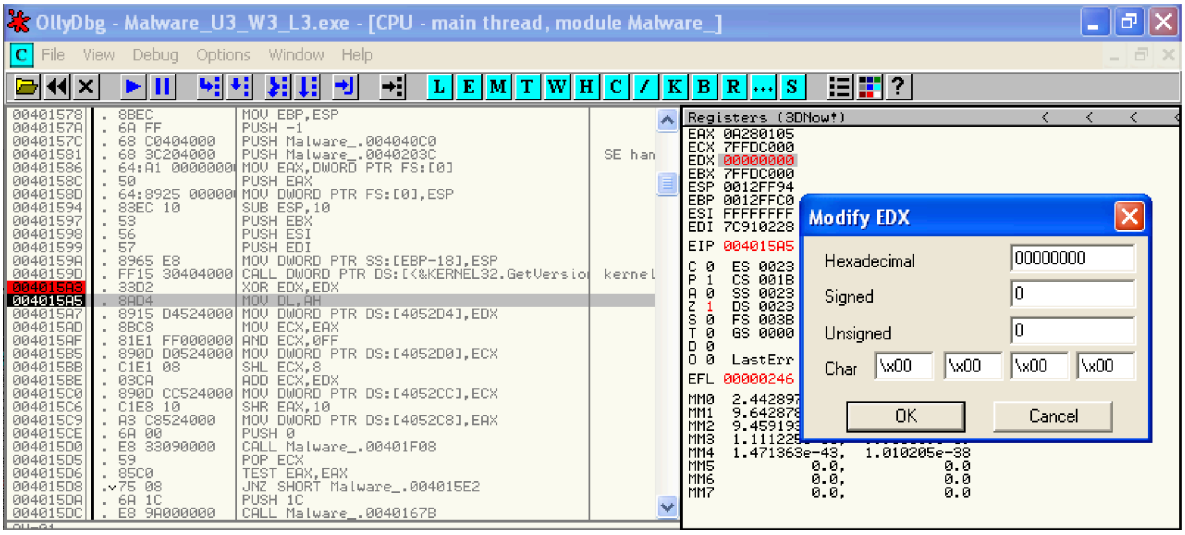
Come richiesto dal'esercizio, per prima cosa andiamo ad analizzare l'indirizzo "0040106E".
Come possiamo vedere il parametro Command line è dato come "cmd".



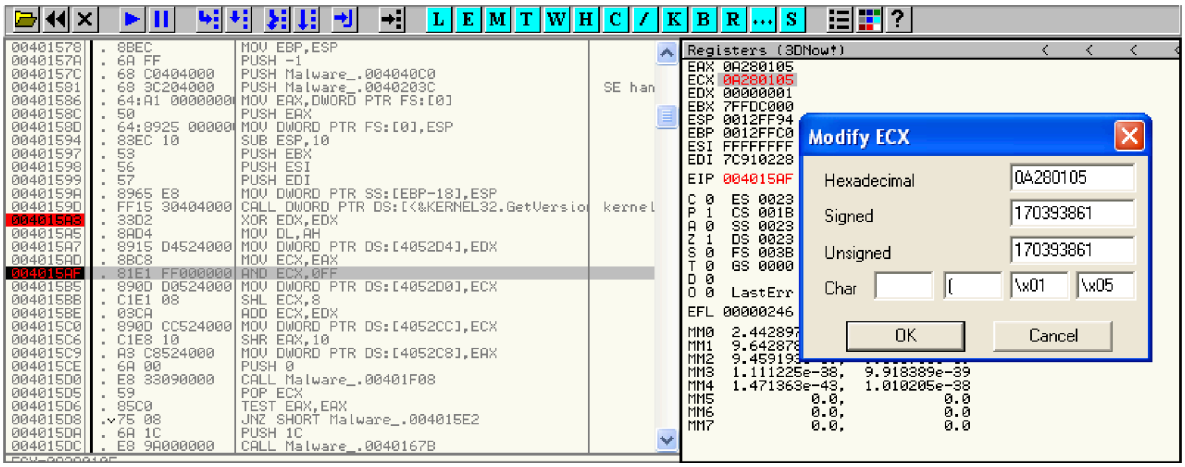
Ora andiamo come richiesto dall'esercizio andiamo a creare un breakpoint all'indirizzo 004015A3, ottenendo come risultato 2600.

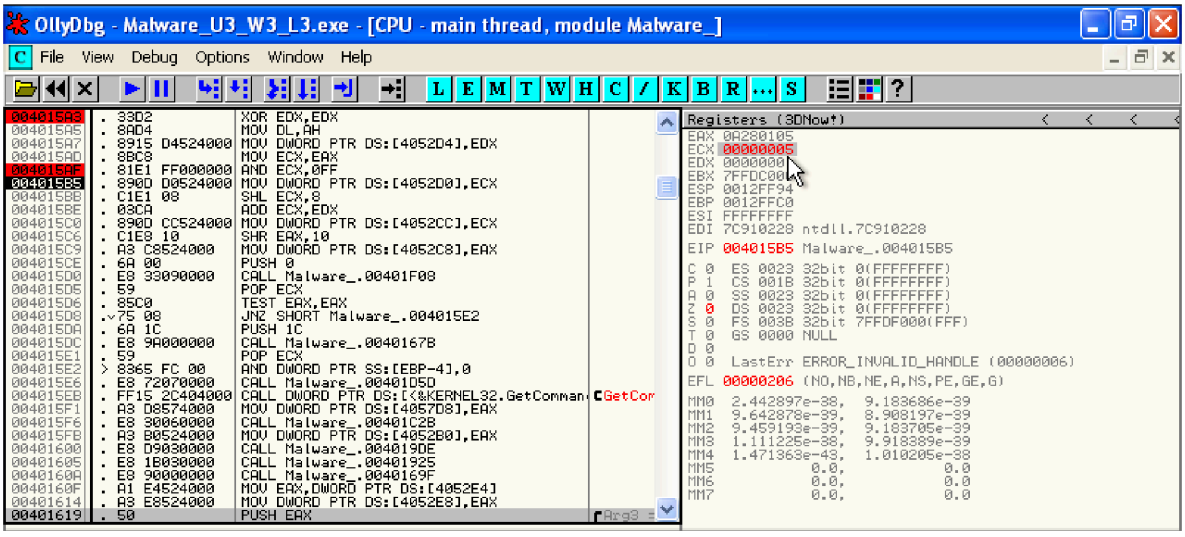


Ora andiamo ad effettuare uno "step into", e possiamo notare subito come il valore di (EDX) sia cambiato da 2600 a 0.
Questo è dovuto al fatto che l'operatore (XOR) finché avrà due operatori uguali darà come risultato 0.



Ora ripetiamo lo stesso procedimento però ad un indirizzo di memoria diverso ovvero il numero 004015AF.
Come richiesto dall'esercizio, creando un breakpoint otteniamo come valore "ECX" 170393861.
Successivamente effettuando uno "step into" possiamo covedere come "ECX" esso venga trasformato in valore decimale 00000005.





Oservando questi dati, si più presumere che questo Malware abbia la funzione di creare una backdoor per poter eseguire i codici in remoto.
Questa teoria viene presa in considerazione in quanto il Malware crea un Socket

andandosi a connettersi ad esso, e queste sono le stringhe di codice da cui abbiamo dedotto ciò.