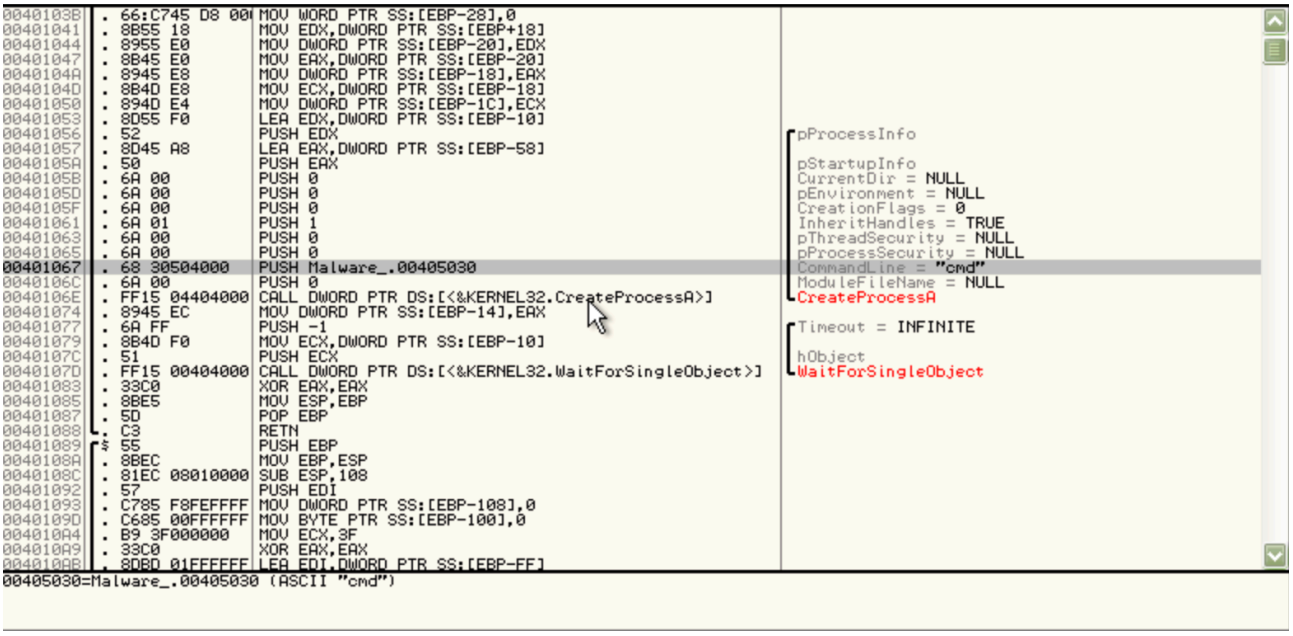
ANALISI MALWARE CON ONLYDBG

L'esercizio di oggi ci richiede di effettuare un analisi con il tool ONLYDBG

La prima parte consiste nel trovare il valore del parametro (commandLine) che viene passato sullo Stack.

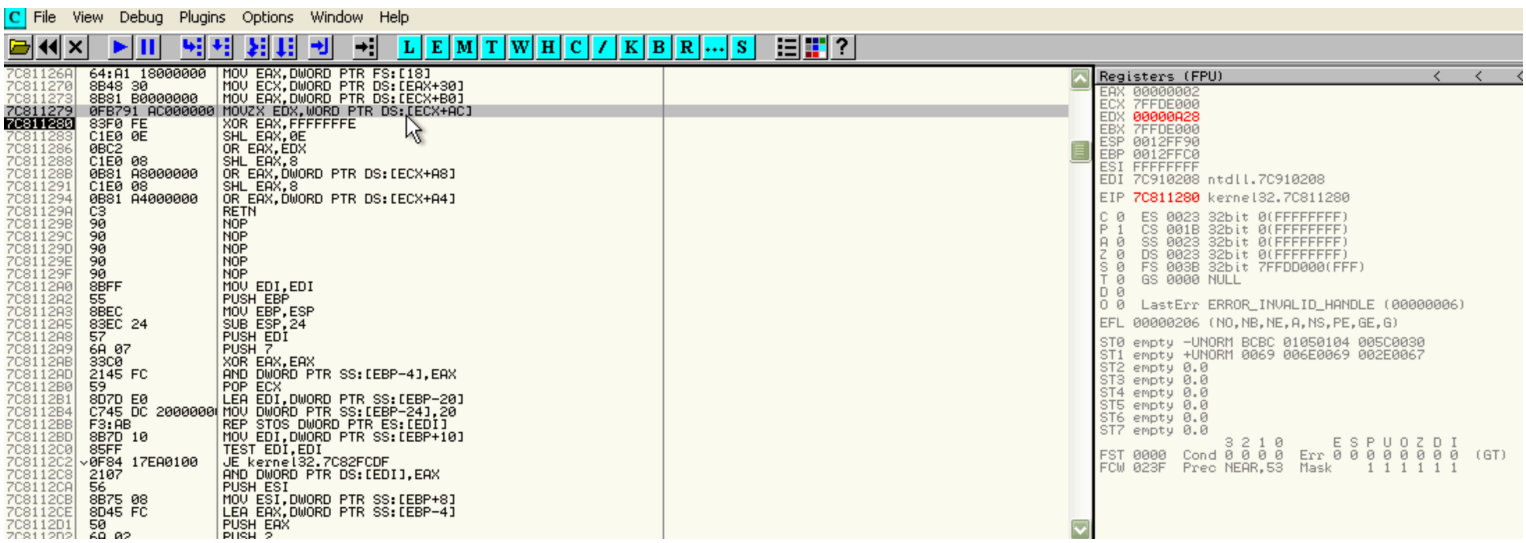
Il parametro passato è: MALWARE_.00405030 come si può notare dalla foto sotto



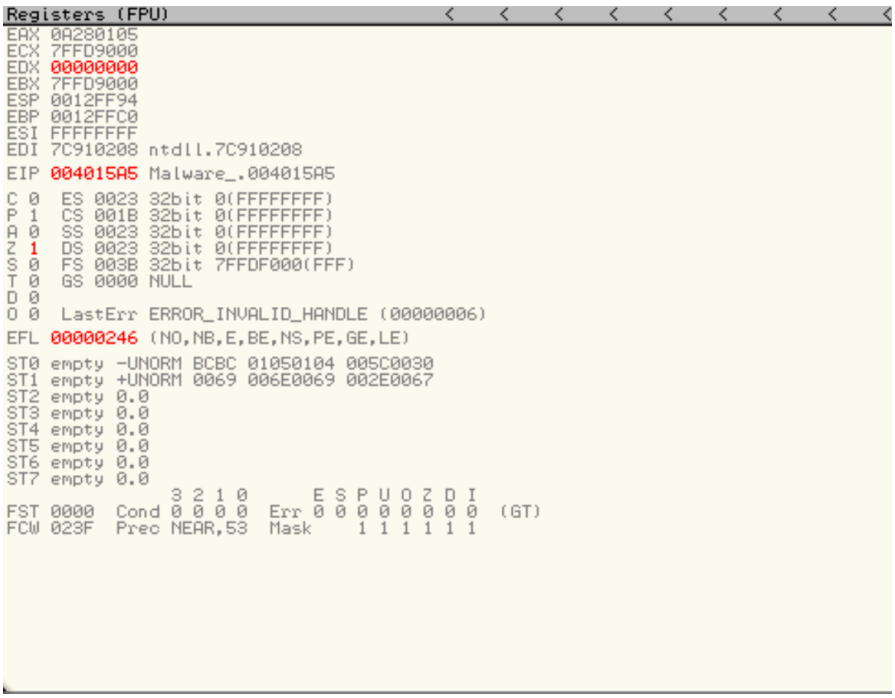
Il secondo punto dell'esercizio invece ci chiede di inserire un breakpoint software all'indirizzo 004015A3.

Il valore di partenza di EDX è di 7c90e4f4 in esadecimale mentre in decimale è 208987050

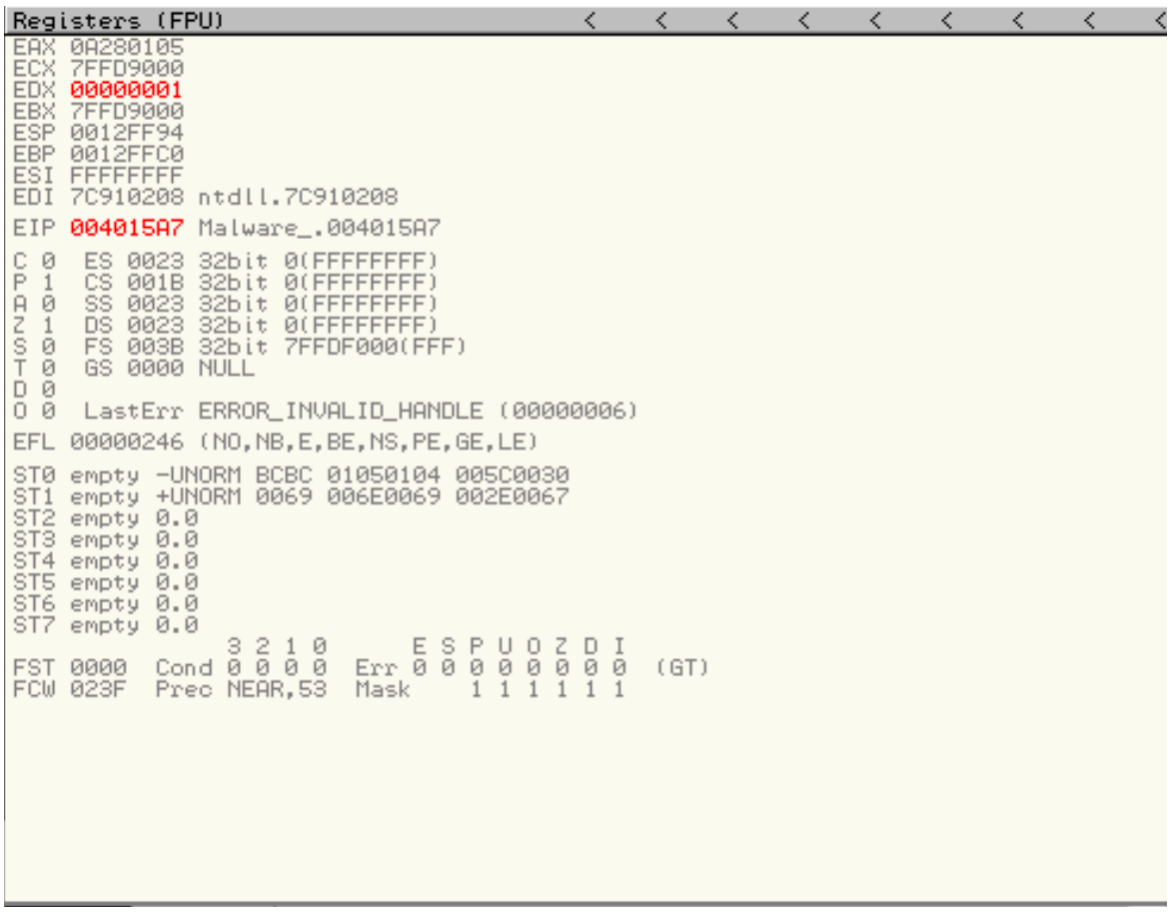
Dopo di che facendo step-into ad un certo punto ci porta dentro la funzione dove il valore di EDX cambia nuovo è diventa in esadecimale 00000a28 in decimale 2600 come possiamo vedere dalla foto qui sotto



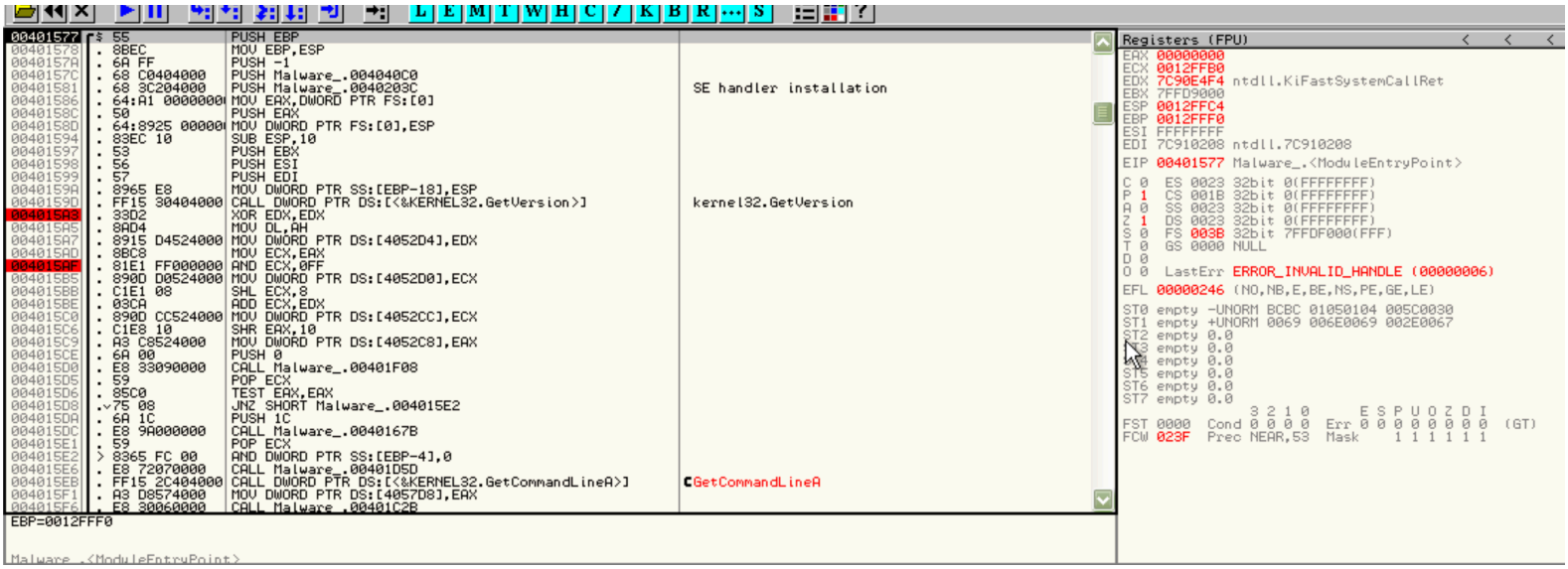
Dopo usciti dalla funzione possiamo notare come EDX cambia di nuovo di valore è diventa 0 perché xor dello stesso oggetto dà come risultato sempre 0



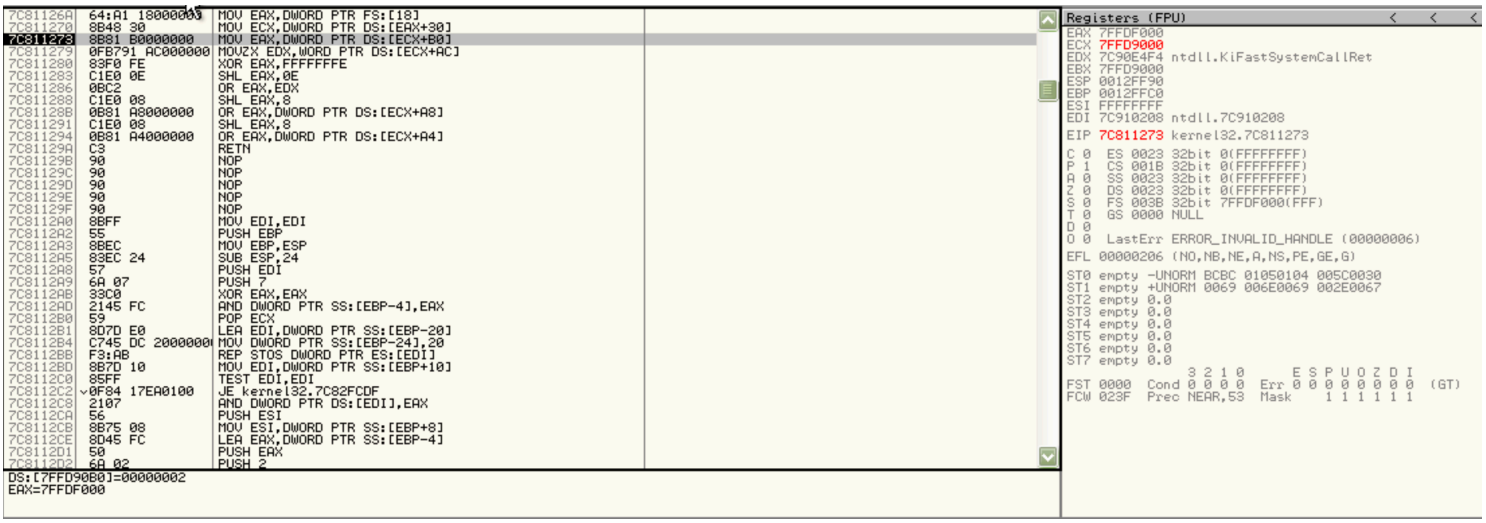
Successivamente il valore di EDX cambia di nuovo è diventa 1



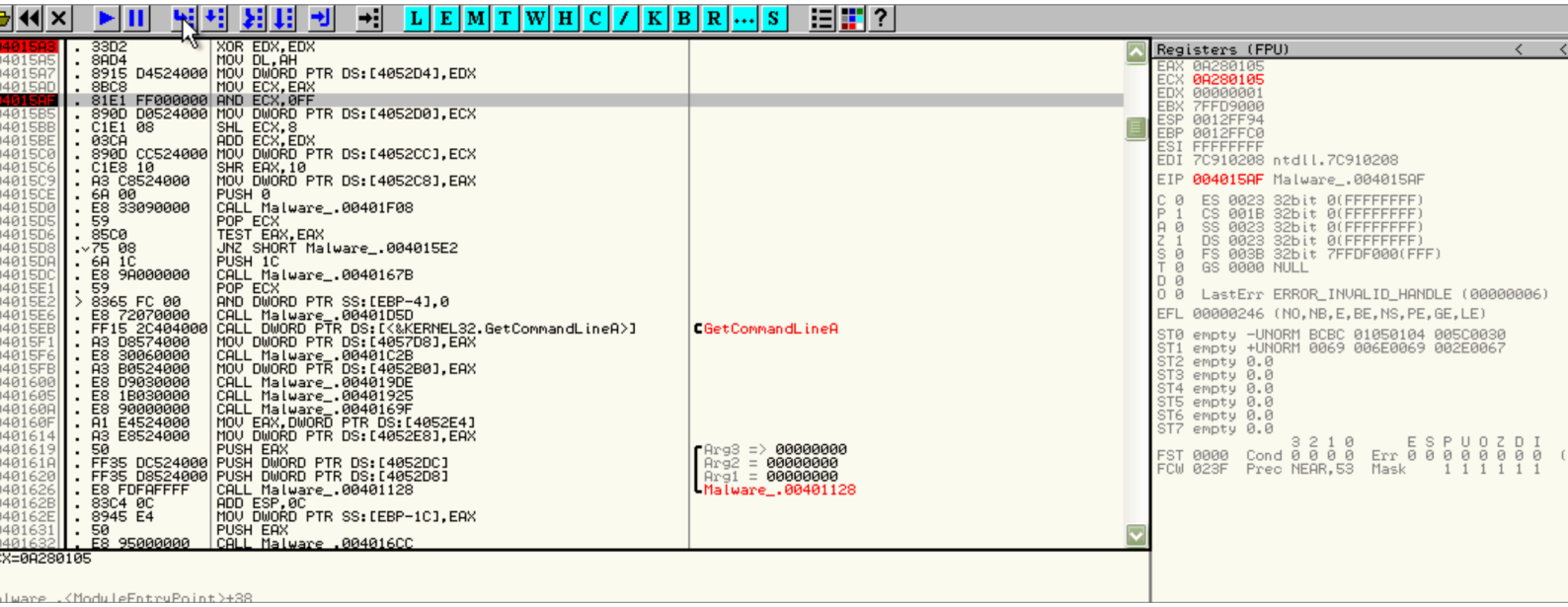
L’ultimo punto dell’esercizio ci richiede di mettere un secondo breakpoint all’indirizzo di memoria 004015AF e ci chiede di controllare il valore di ECX che in questo caso è in esadecimale 0012ffb0 in decimale è 1245104



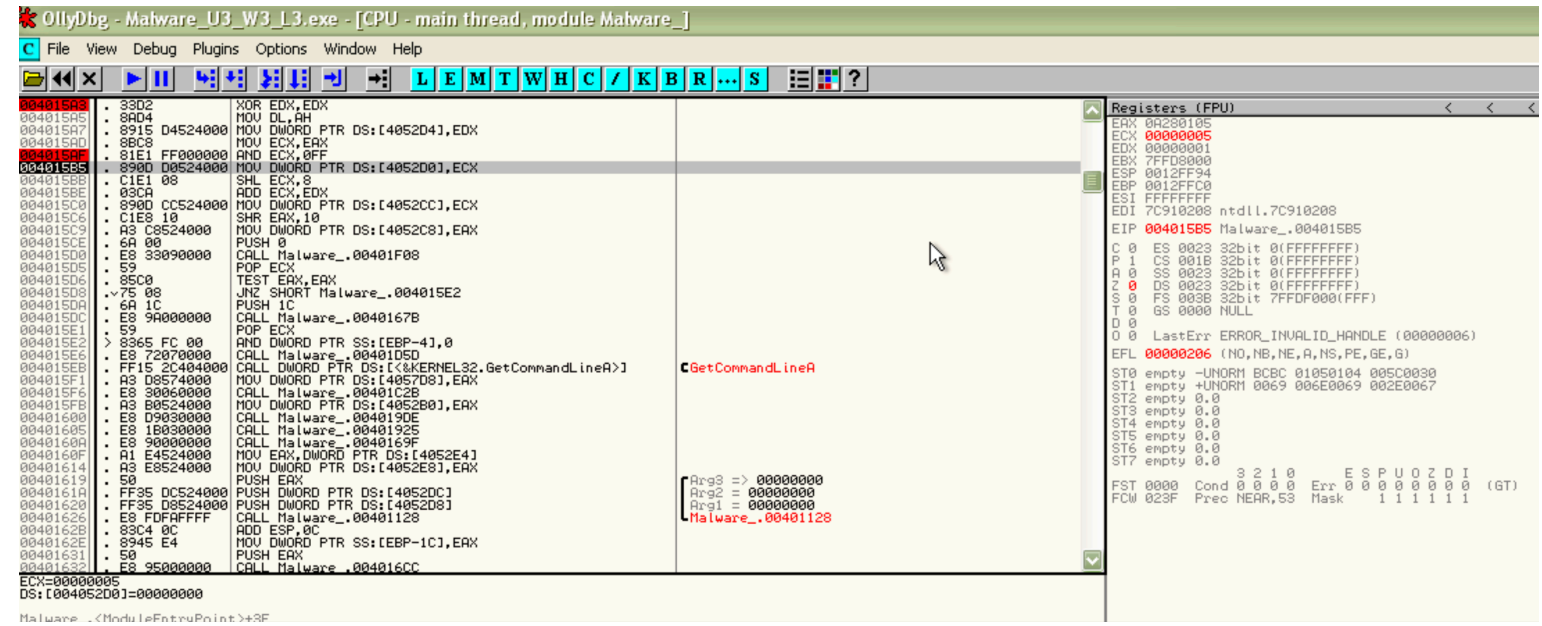
Possiamo vedere con all’ interno della funzione il valore di ECX cambia di nuovo diventando in esadecimale 7ffd9000 in decimale è 2147323904



Usciti dalla funzione il valore del registro ECX cambia nuovamente diventando in esadecimale 0a280105 in decimale 170393861



Possiamo notare come con l'istruzione and il valore di ECX cambia di nuovo in esadeciamle è 00000005 e in decimale 5



Infine possiamo vedere con l'istruzione adì come il valore di ECX cambia di nuovo è diventa in esadecimale 00000500 in decimale 1280 con l'istruzione add si va ad aggiungere il valore contenuto in EDX ad ECX e salva il risultato in ECX