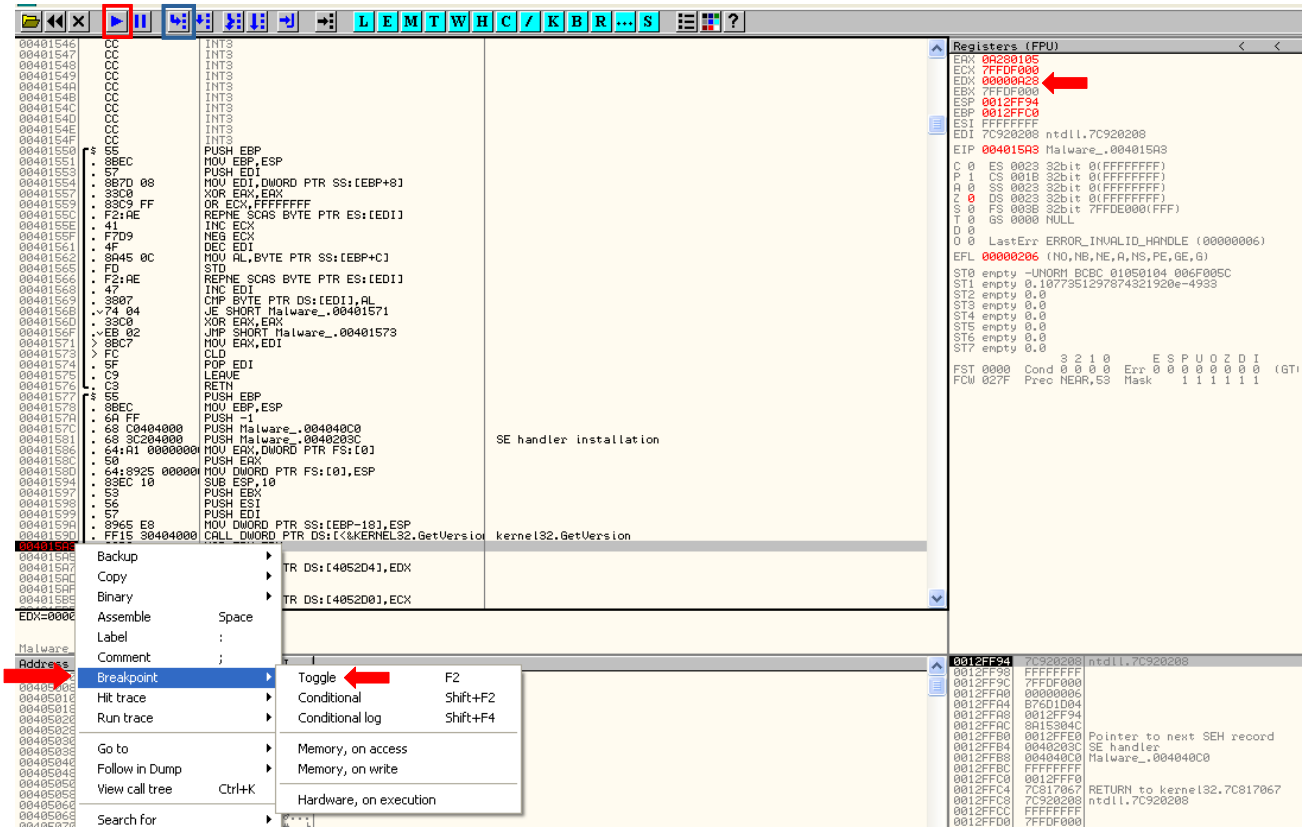
Analisi dinamica avanzata

1) Indicare qual'è il valore del parametro "Command Line" che viene passato sullo stack al indirizzo 0040106E.

Andiamo ad aprire OllyDBG ed una volta inserito il file, andando al indirizzo 0040106E possiamo notare che il valore del parametro **CommandLine** sia "**cmd**".

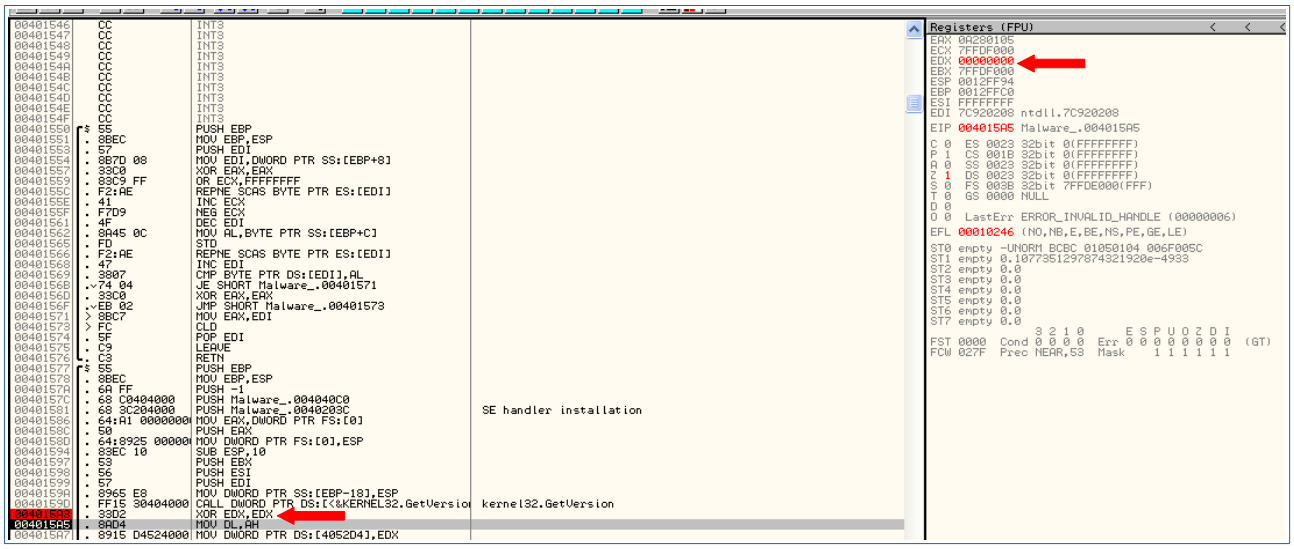
2) Inserire un software breakpoint all'indirizzo 004015A3 ed individuare il valore del registro EDX.

Andando al indirizzo **004015A3** ed inserendo un software breakpoint, con tasto destro sulla righa andando un breakpoint e poi sulla sezione **Toggle.**



Andiamo poi a eseguire il comando **Run programm** e potremmo poi vedere che il valore del registro EDX sarà: 00000A28.

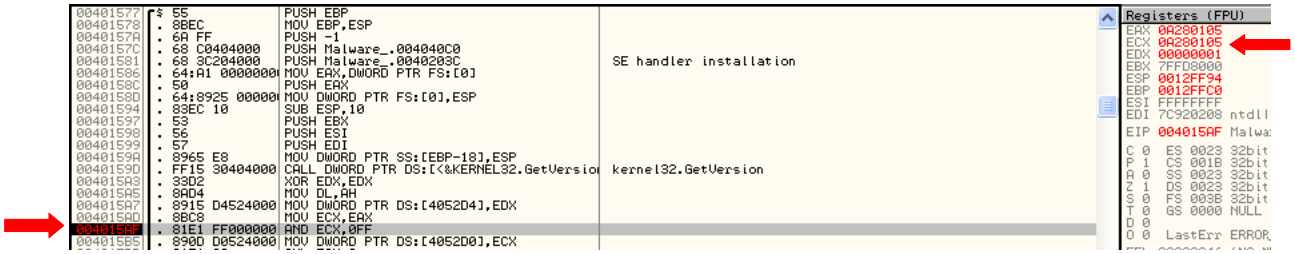
A questo punto eseguiamo uno **step-into** per controllare se il valore di EDX sia cambiato.



Come si può vedere il valore di EDX è cambiato in 0000000 questo dovuto al fatto che è stato usato l' operatore XOR tra EDX e se stesso che porterà come risultato a 0.

3) Inserire un secondo breakpoint nel indirizzo **004015AF** risalire al valore di ECX prima e dopo aver eseguito lo step-into.

Andiamo alla locazione di memoria **004015AF** inseriamo un breakpoint come possiamo vedere il valore di ECX in questo momento è **0A280105**.



Eseguiamo ora il comando **step-into** , come si può vedere il valore del registro adesso è 00000005. Questo risultato viene fuori perché la riga di comando **AND ECX,0FF** questo andrà a fare l' AND logico tra il registro ECX e il valore esadecimale 0FF ed il risultato sarà : **00000005.**