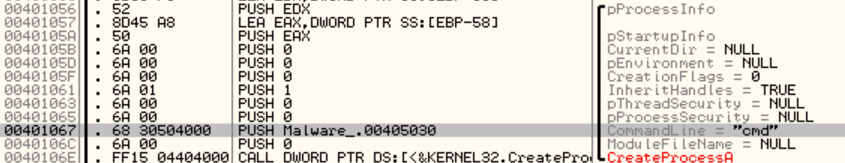
OllyDBG

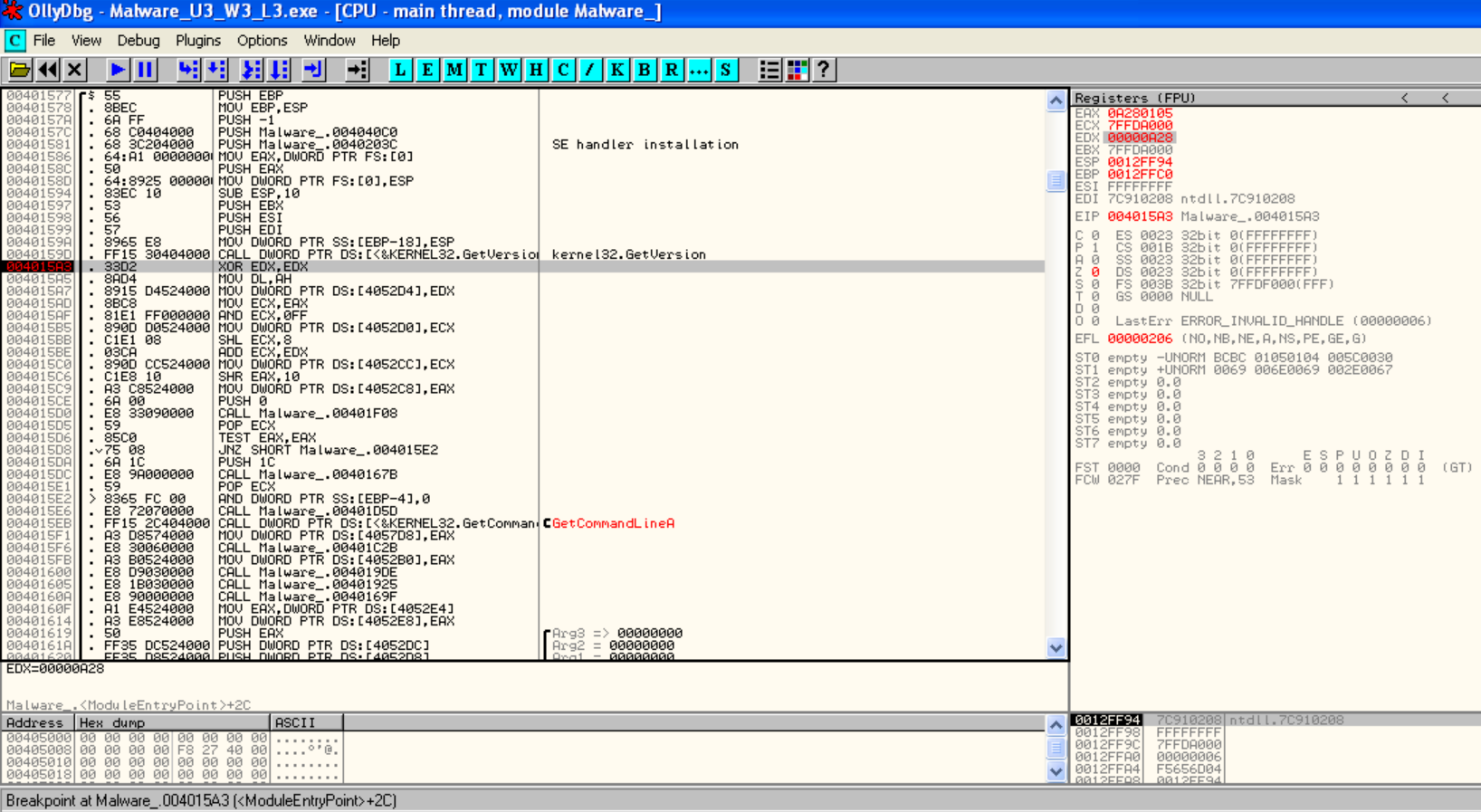
Nell’esercizio di oggi bisognava analizzare un malware con **OllyDBG** e rispondere a dei quesiti.

1)

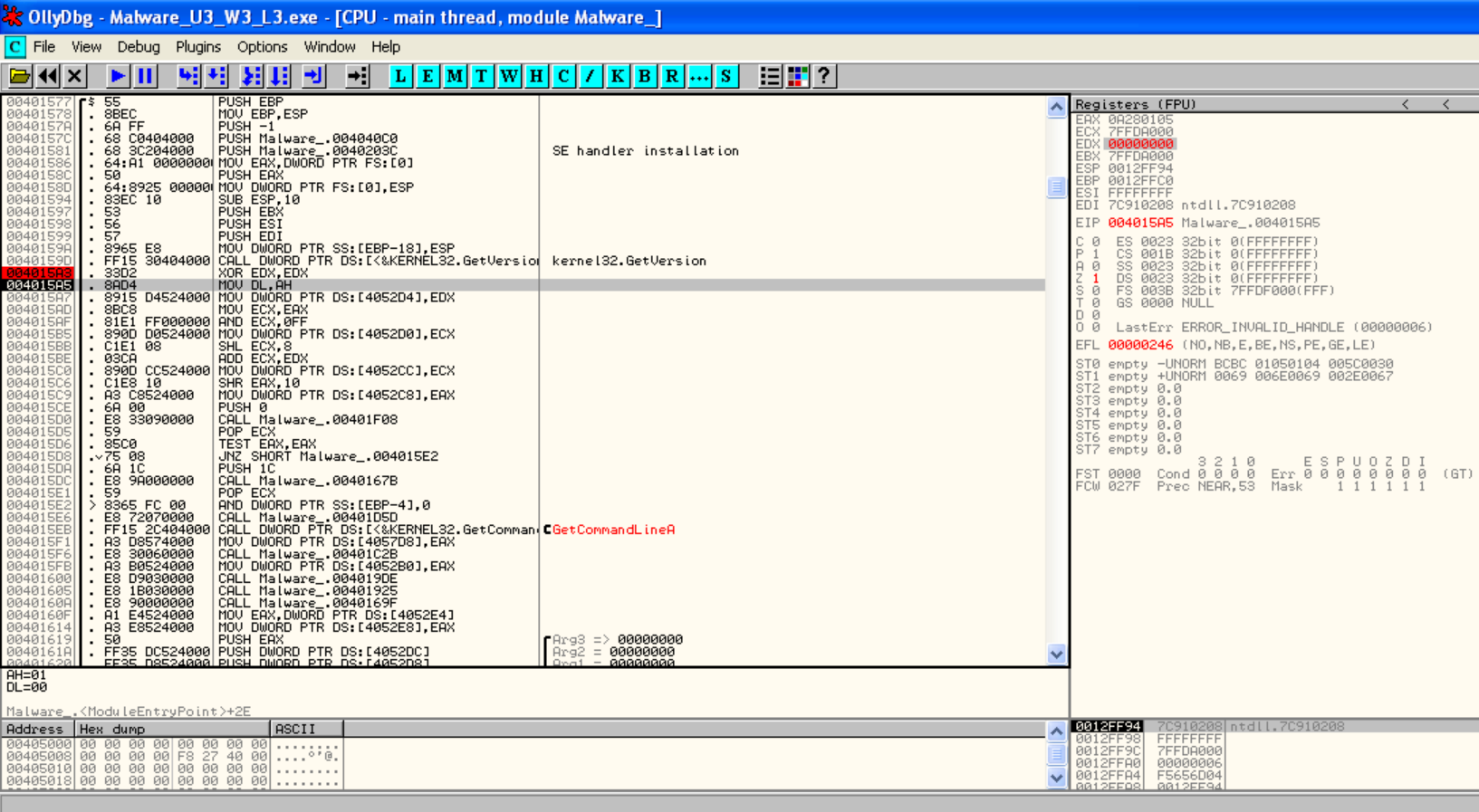


Nell’immagine si vede che la funzione **CreateProcess**, ha come parametro **CommandLine**, il cui valore passato sullo stack è “**cmd**”.

2)

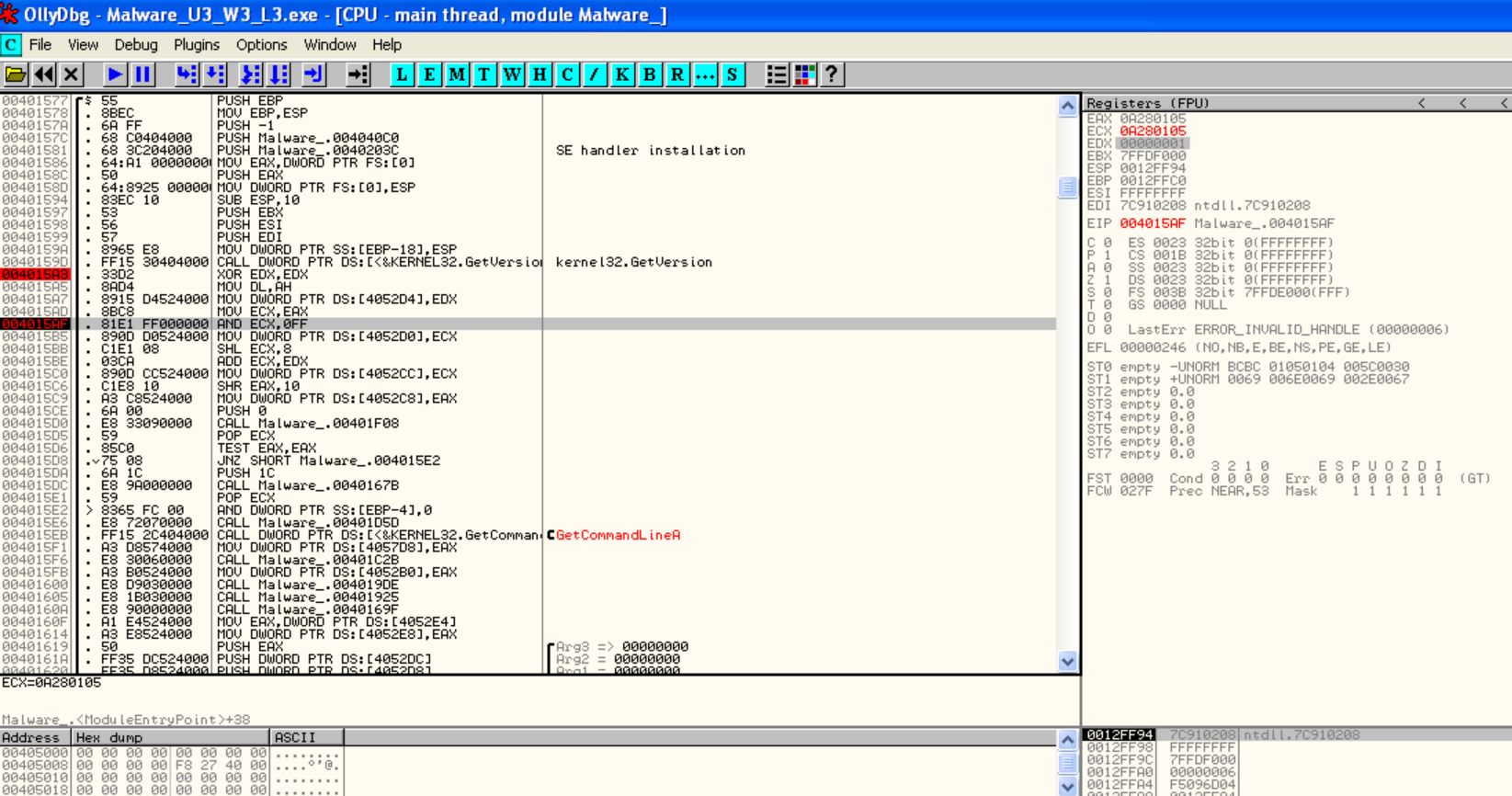


Qui vediamo che il valore di EDX prima dell’istruzione in esadecimale è 00000A28.

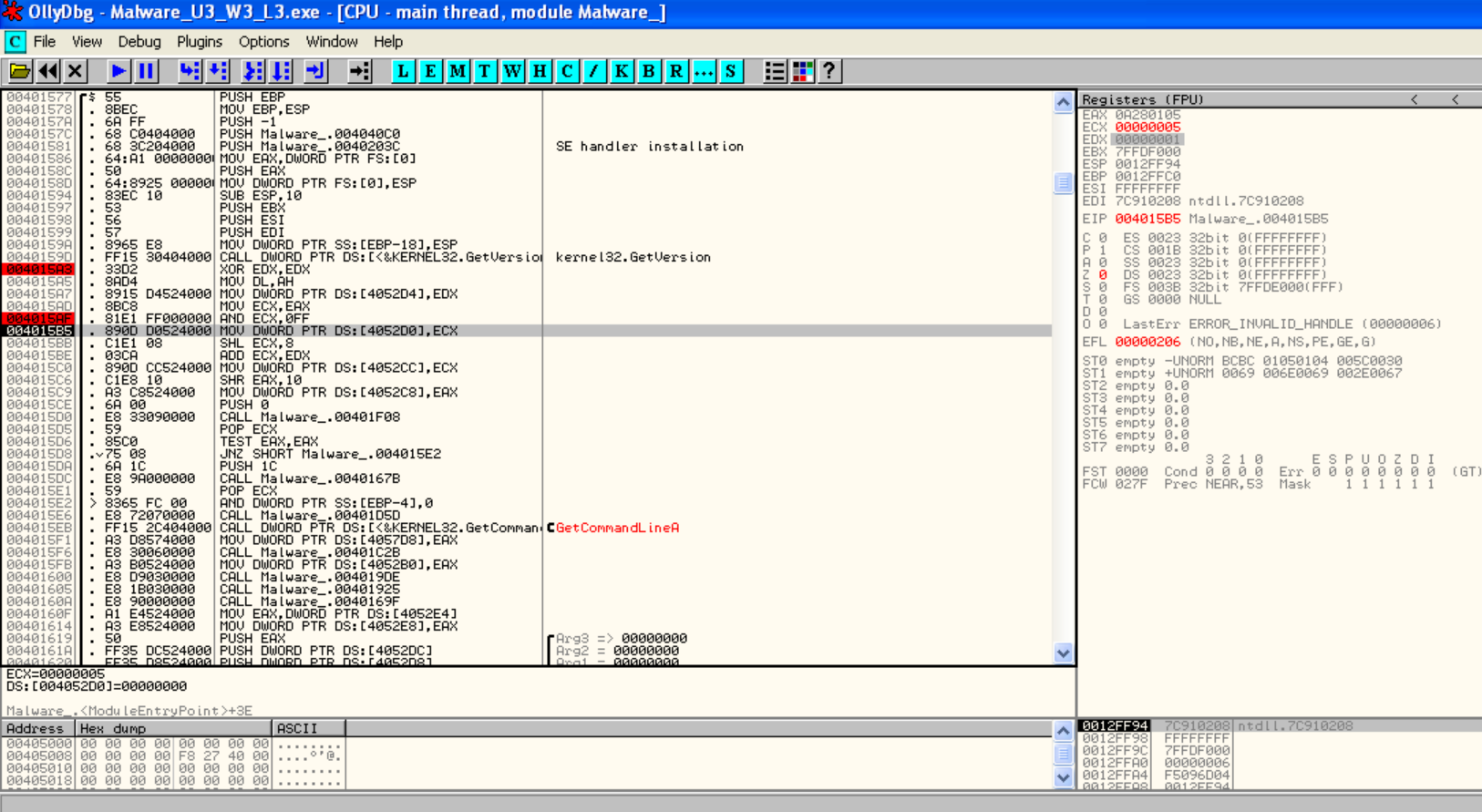


Mentre dopo aver seguito l’istruzione diventa 0, poiché l’XOR di se stessi è sempre 0.

3)



Il valore del registro ECX prima di eseguire l’istruzione è 0A280105.



Mentre dopo l’istruzione è 5 perché esegue un AND tra ECX e 0FF.