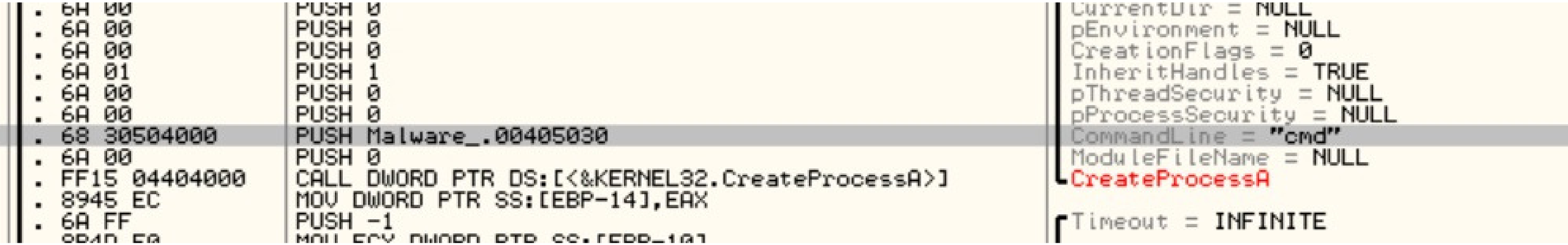
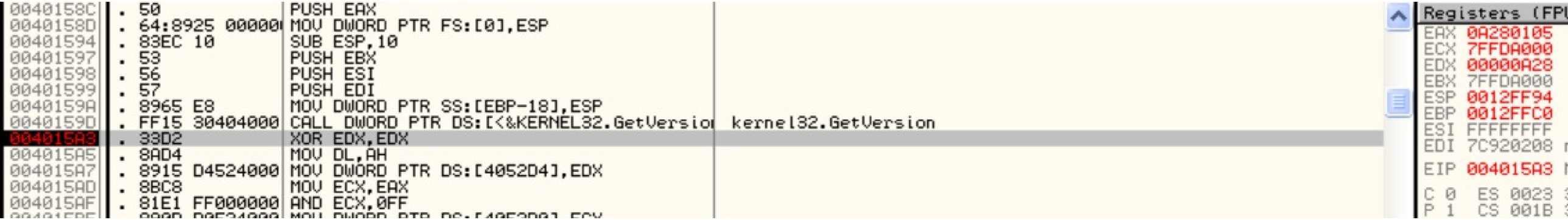
S11L3

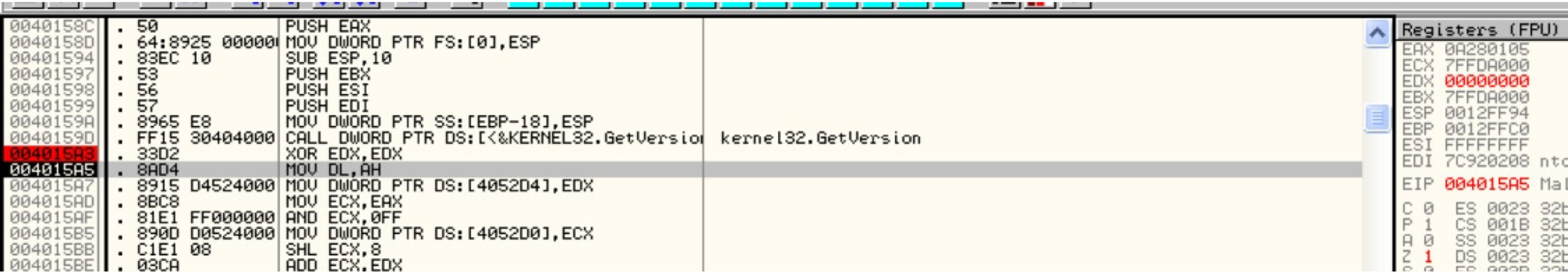
1 - Individuato l’indirizzo di memoria con la funzione CreateProcess e scoperto il valore Command Line ovvero “cmd”



Valore del registro EDX prima del BreakPoint

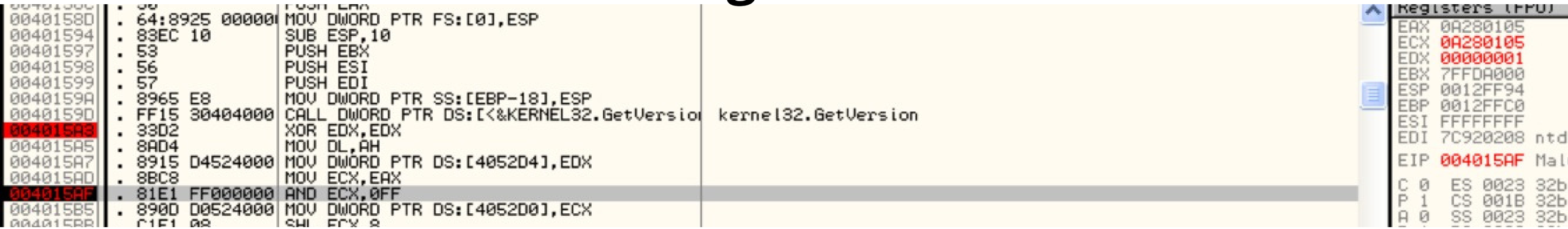


Valore del registro EDX dopo il BreakPoint

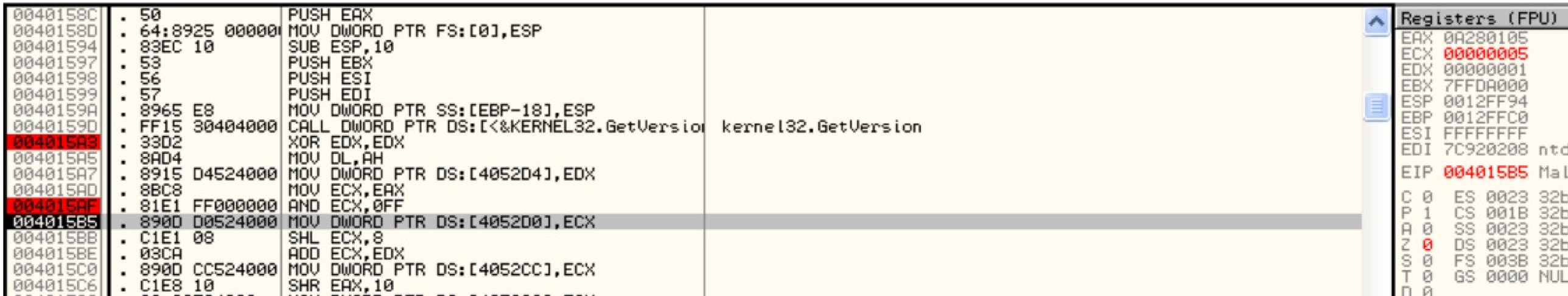


Notiamo che il valore del registro dopo il BP è 0. Questo perchè passa attraverso l’istruzione XOR EDX,EDX che restituisce 0 quando i due operandi sono uguali

Settato il BP all’indirizzo richiesto e individuato il valore del registro ECX



Eseguito lo step info e visualizzato il valore del registro ECX che risulta 05



Notiamo che il valore del registro ECX cambia in 5 che è il risultato dopo l’istruzione AND ECX, 0FFh che esegue un operazione trai due operandi

Bonus; Attraverso le funzioni WSASocket, Connect, HTONS, GETHOSTBYNAME,CLOSESOCKET si potrebbe pensare che la funzione del Malware è quella di connettersi ed aprire un socket che resti in ascolto