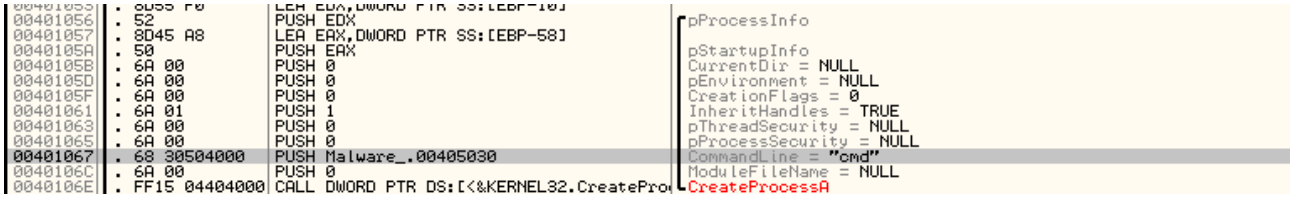
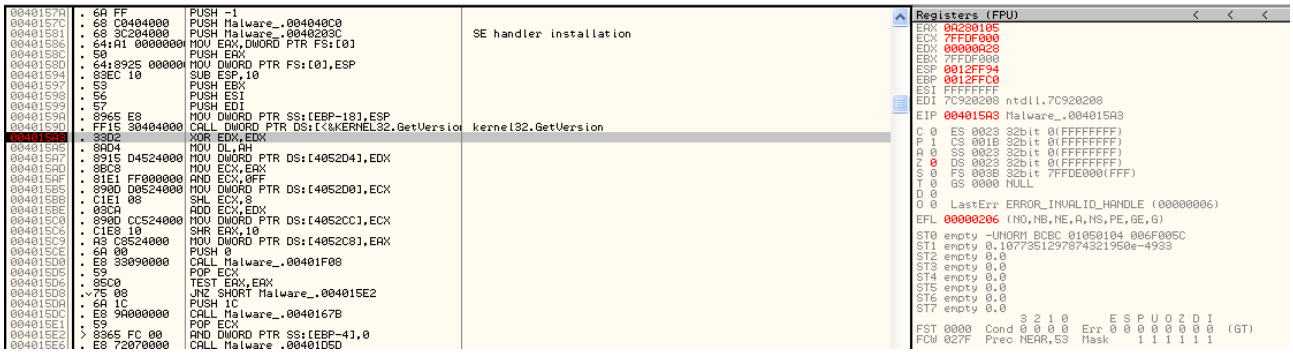
PRATICA S11L3

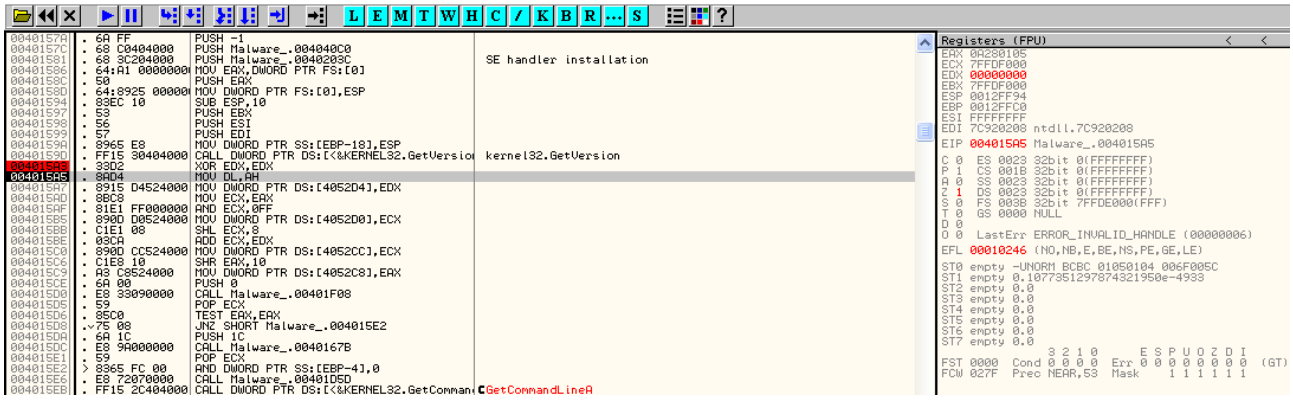
1) Come si vede dall'immagine, il valore del parametro passato sullo stack è cmd



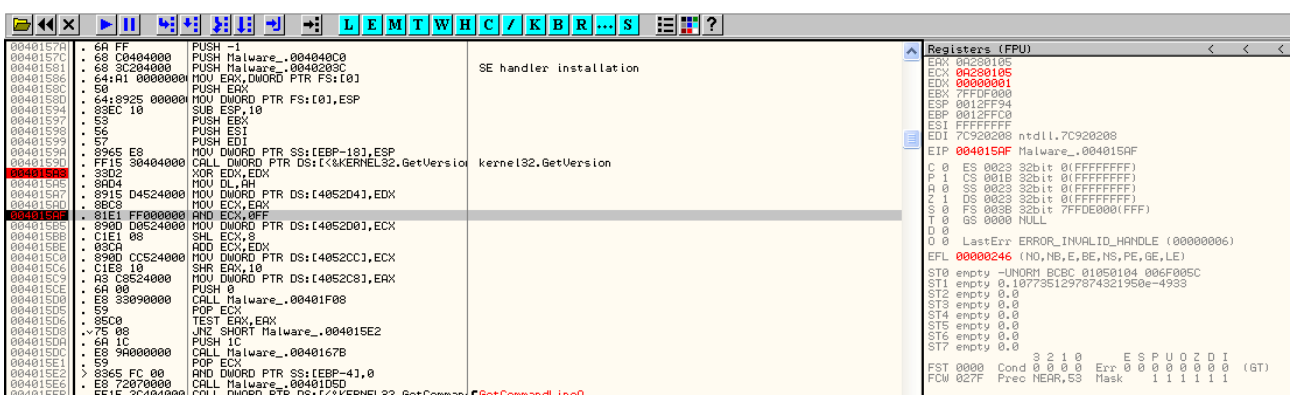
2) Come si vede dall'immagine sotto nel riquadro di destra il valore in questo punto dell'esecuzione del registro EDX è 00000A28



Andiamo ad eseguire uno step into, eseguendo quindi l'istruzione xor EDX,EDX. Lo xor di un valore con sé stesso darà zero come risultato, e in effetti vediamo che il valore di EDX ora risulta 0



3) In modo similare al caso sopra, andiamo ad inserire un break point all'istruzione and ecx,off. Vediamo che prima di questa esecuzione il registro ecx vale 0A280105



eseguiamo uno step into andando ad eseguire l'istruzione. Notiamo che ora il registro ecx vale 00000005. Questo è il risultato dell'AND logico a livello di bit fra i due registri ecx e l'esadecimale 000000FF.