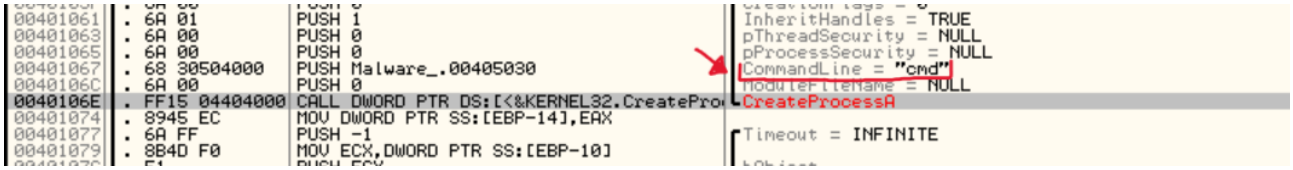
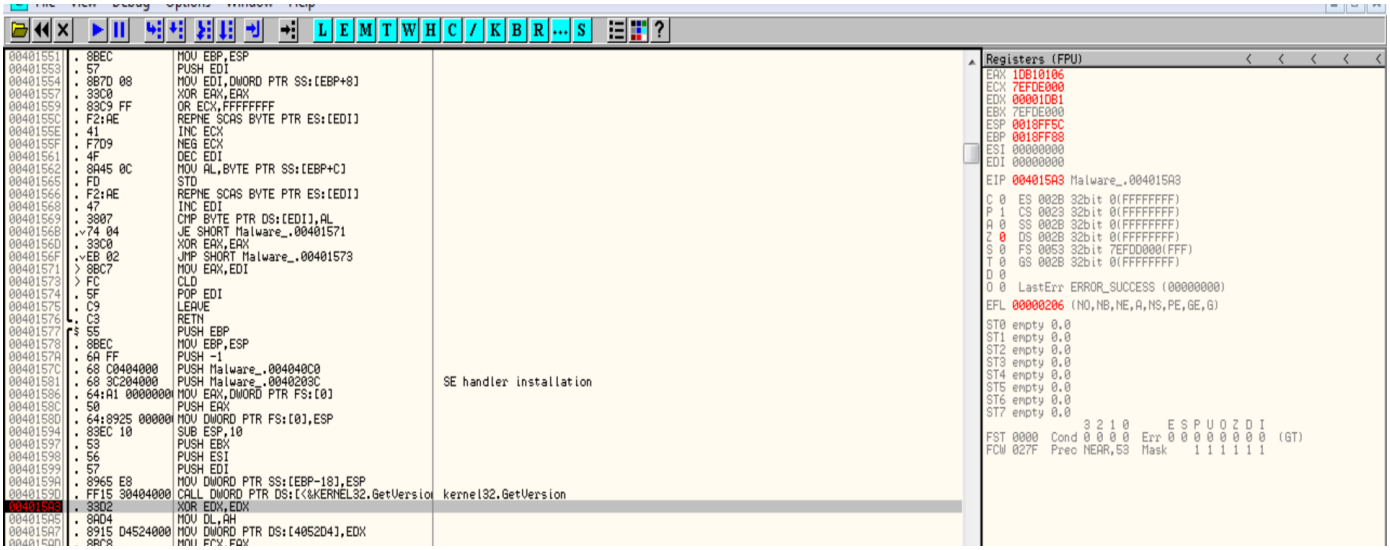
Facendo riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3 sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

• All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?

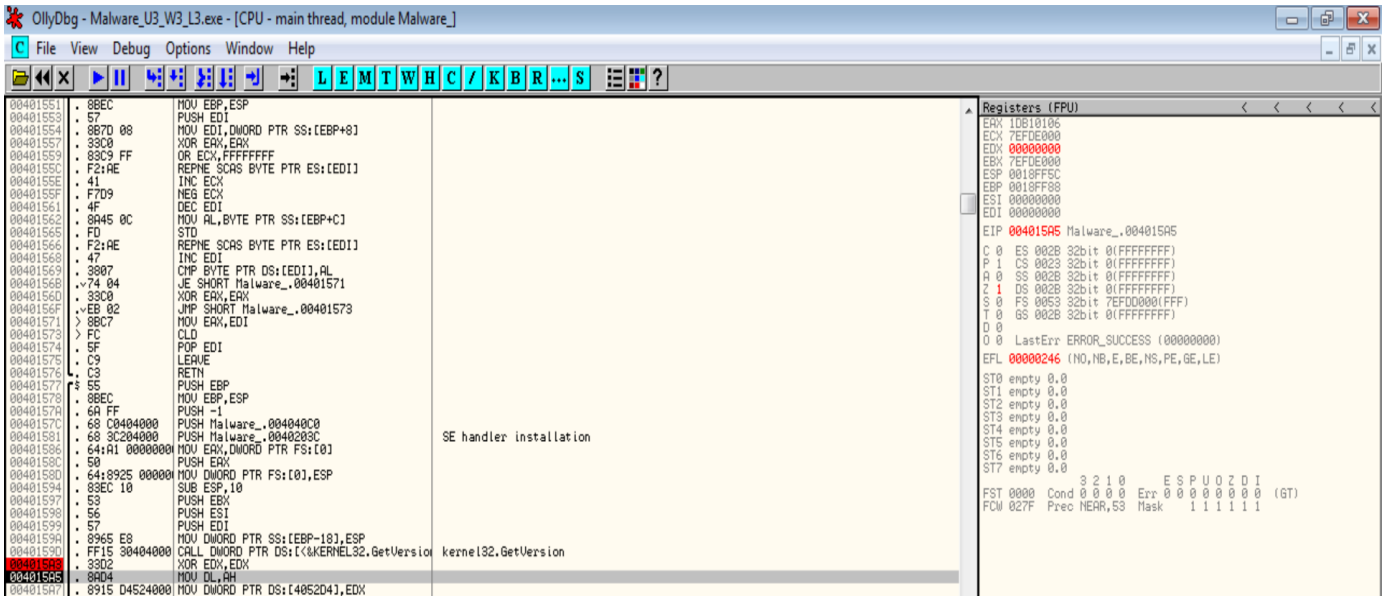


Il valore del parametro è "CMD", ovvero il command prompt di Windows.

• Inserite un breakpointsoftware all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

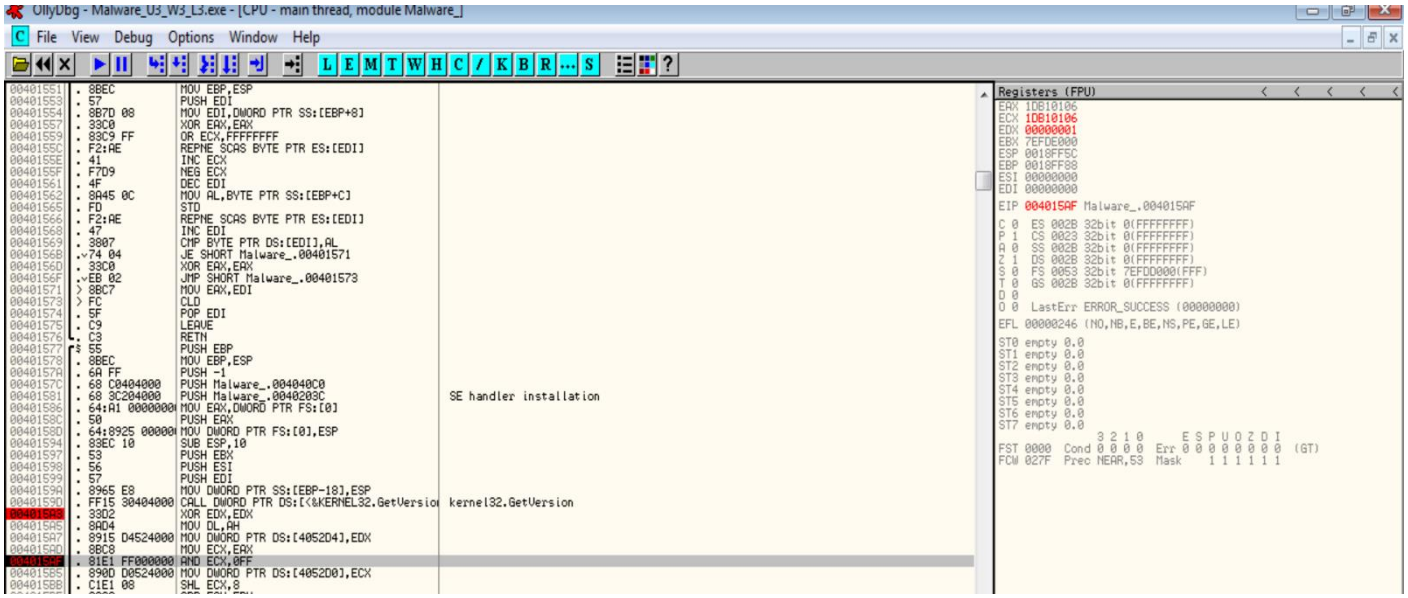


Dopo aver configurato il breakpoint, clicchiamo "play". Il programma si ferma dunque all'istruzione XOR EDX,EDX. In questo caso il valore del registro EDX è "00001DB1".

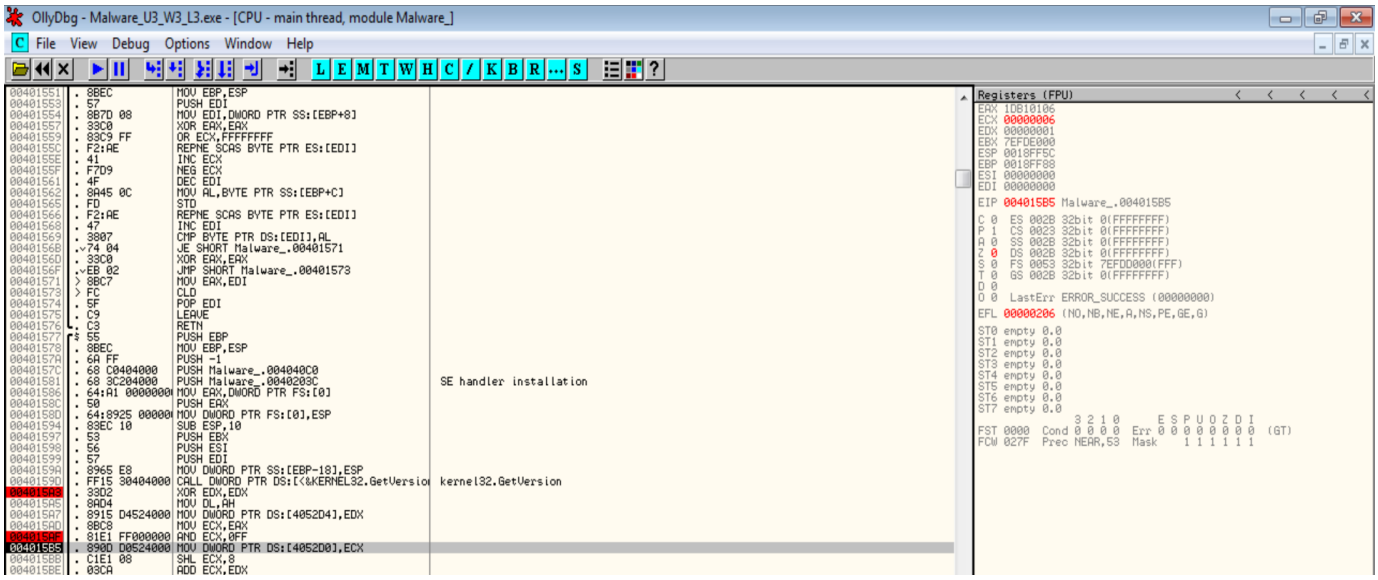


Dopo lo “step-into”, viene dunque eseguita l’istruzione “XOR EDX,EDX”, che inizializza a zero una variabile. Dunque ora il valore di EDX è “0”.

- ***Inserite un secondo breakpoint all’indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite uno step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.***



Facendo un procedimento analogo a quello fatto prima, configuriamo il breakpoint e notiamo che il valore del registro ECX è “1DB10106”.



Dopo lo “step-into”, viene dunque eseguita l’istruzione “AND ECX, FF”. Ora il valore di EDX è “00000006”. Questo risultato è ottenuto perché l’istruzione esegue l’AND logico sui bit di EAX e FF (valore esadecimale).