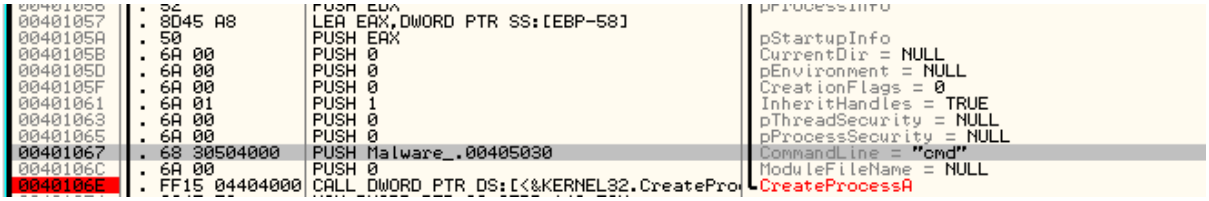
# S11L3

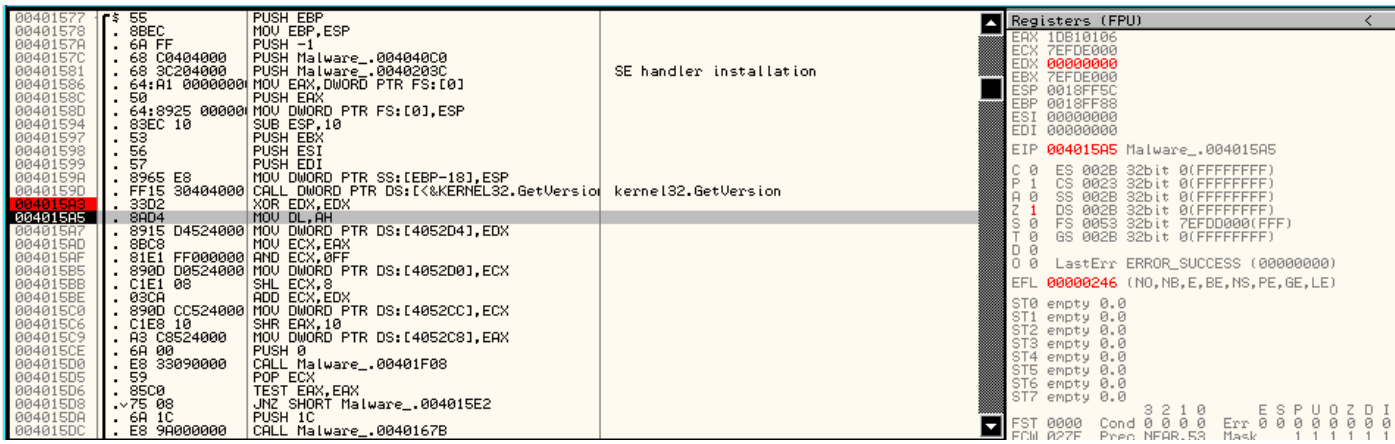
**Traccia:**All'indirizzo 0040106E il Malware Effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «Command Line» che viene passato sullo stack?




Sullo stack viene passato Commandline="cmd".

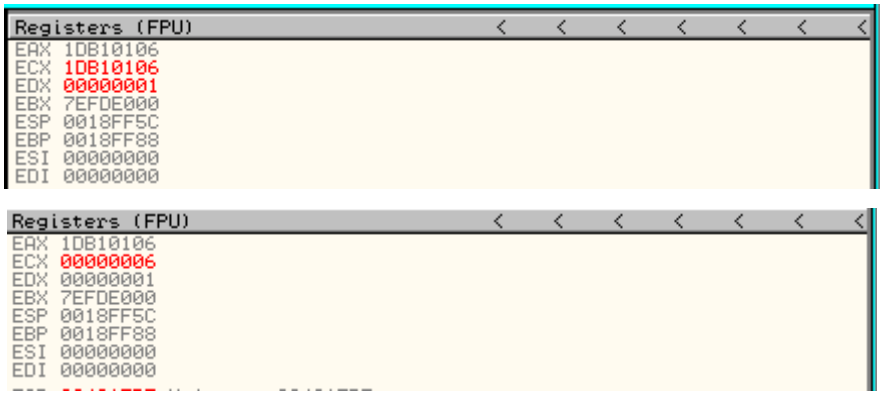
**Traccia:**Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta . Che istruzione è stata eseguita?


All'indirizzo 004015A3,EDX=00001DB1.




Ora EDX viene azzerato,perchè viene eseguito XOR EDX,EDX il quale va ad azzerare EDX.

**Traccia:**Inserite un secondo breakpoint all'indirizzo di memoria 004015 AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7)Spiegate quale istruzione è stata eseguita (8).




Il valore di ECX ora è 00000006,questo perchè è stata eseguita l’istruzione AND ECX,OFF.