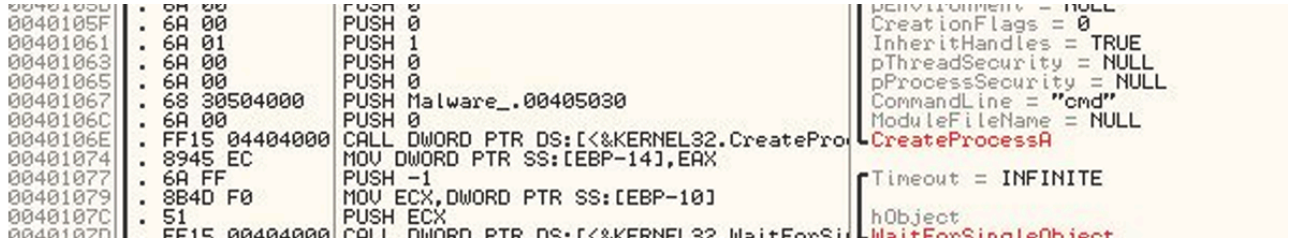
Pratica S11/L3

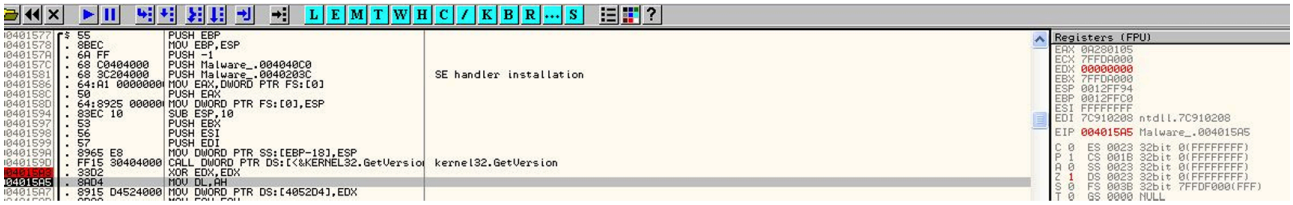
- All’indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?

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

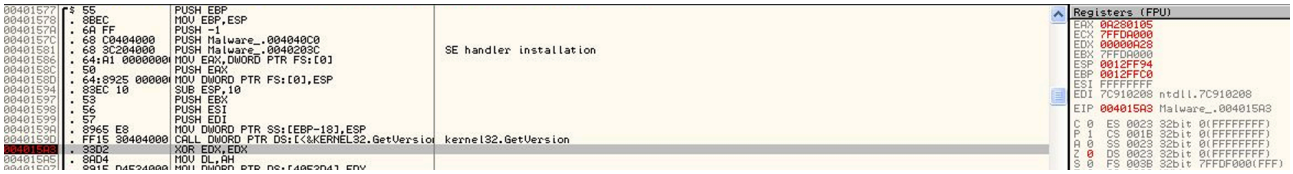


- Inserite un breakpointsoftware all’indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

Dopo aver impostato il breakpoint, faccio partire il programma. Si fermerà quando raggiunge l'istruzione XOR EDX, EDX. Prima dell'esecuzione di questa istruzione, **il valore di EDX è "00000A28".**

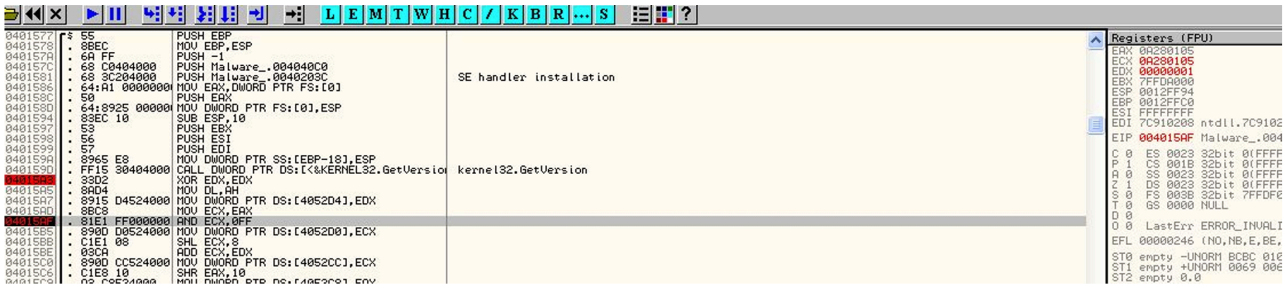


Dopo aver eseguito lo step-into, **l'istruzione XOR EDX, EDX** azzera il valore di EDX, che

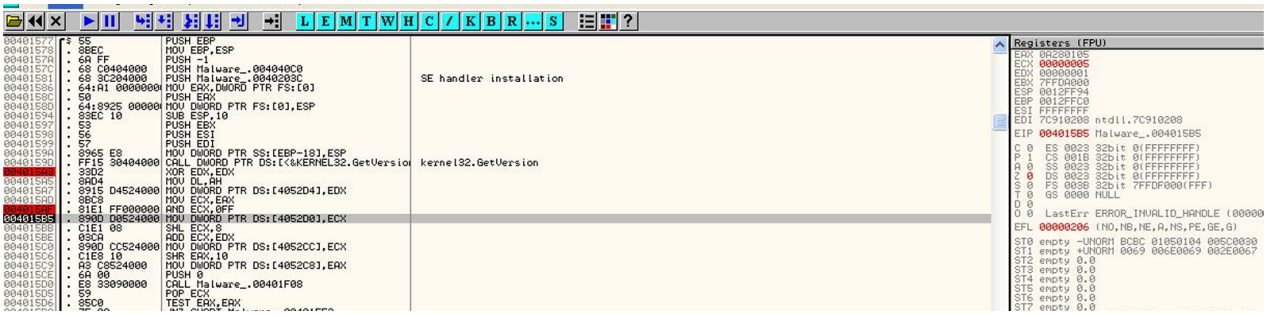


diventa quindi 0.

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



Il valore del registro ECX è «0A280105»,
Dopo aver eseguito lo step-into, il valore del registro ECX è cambiato in "00000005" perché è stata eseguita l'**istruzione AND ECX, FF**, la quale effettua un'operazione logica



tra il valore corrente di ECX e "FF".