OllyDBG

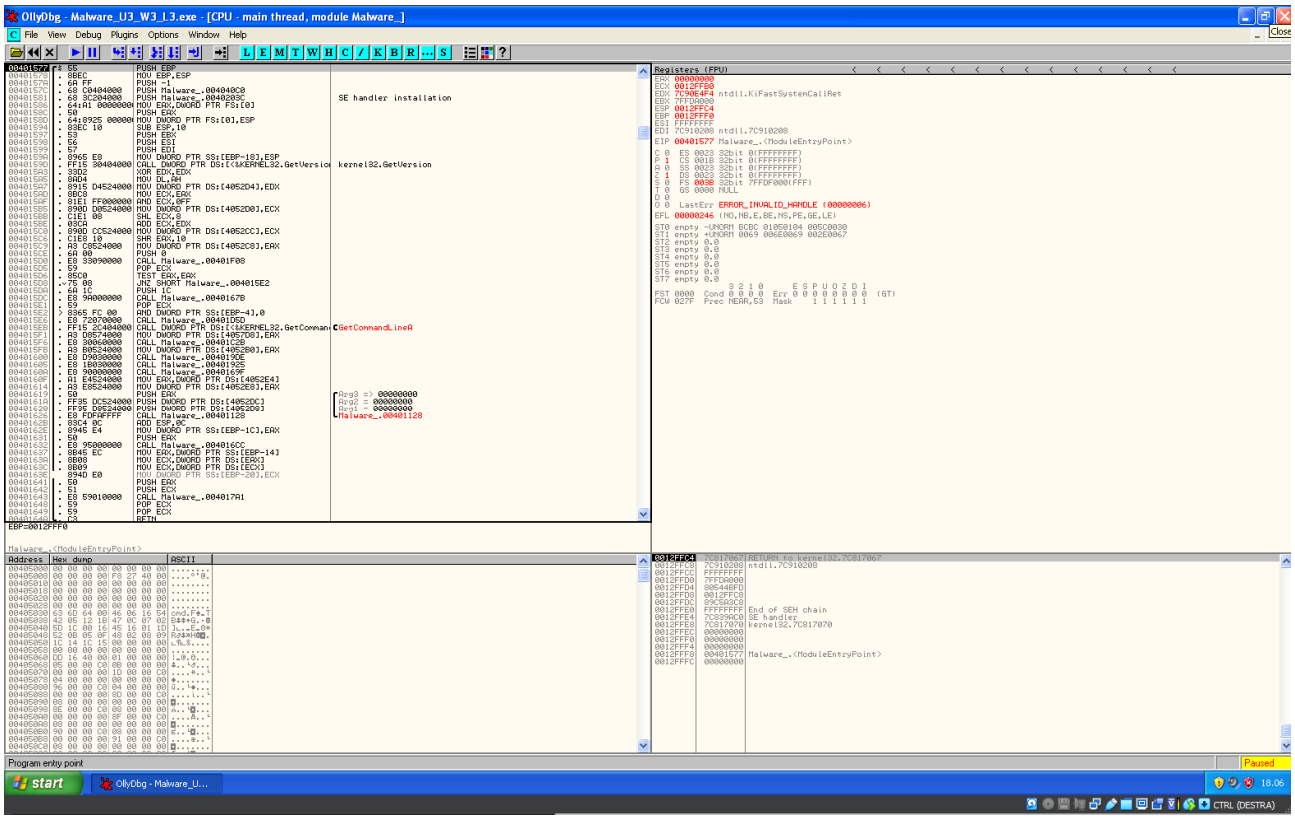
- **All’indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione “CreateProcess”. Quel è il valore del parametro “CommandLine” che viene passato sullo stack ?**

- **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?**

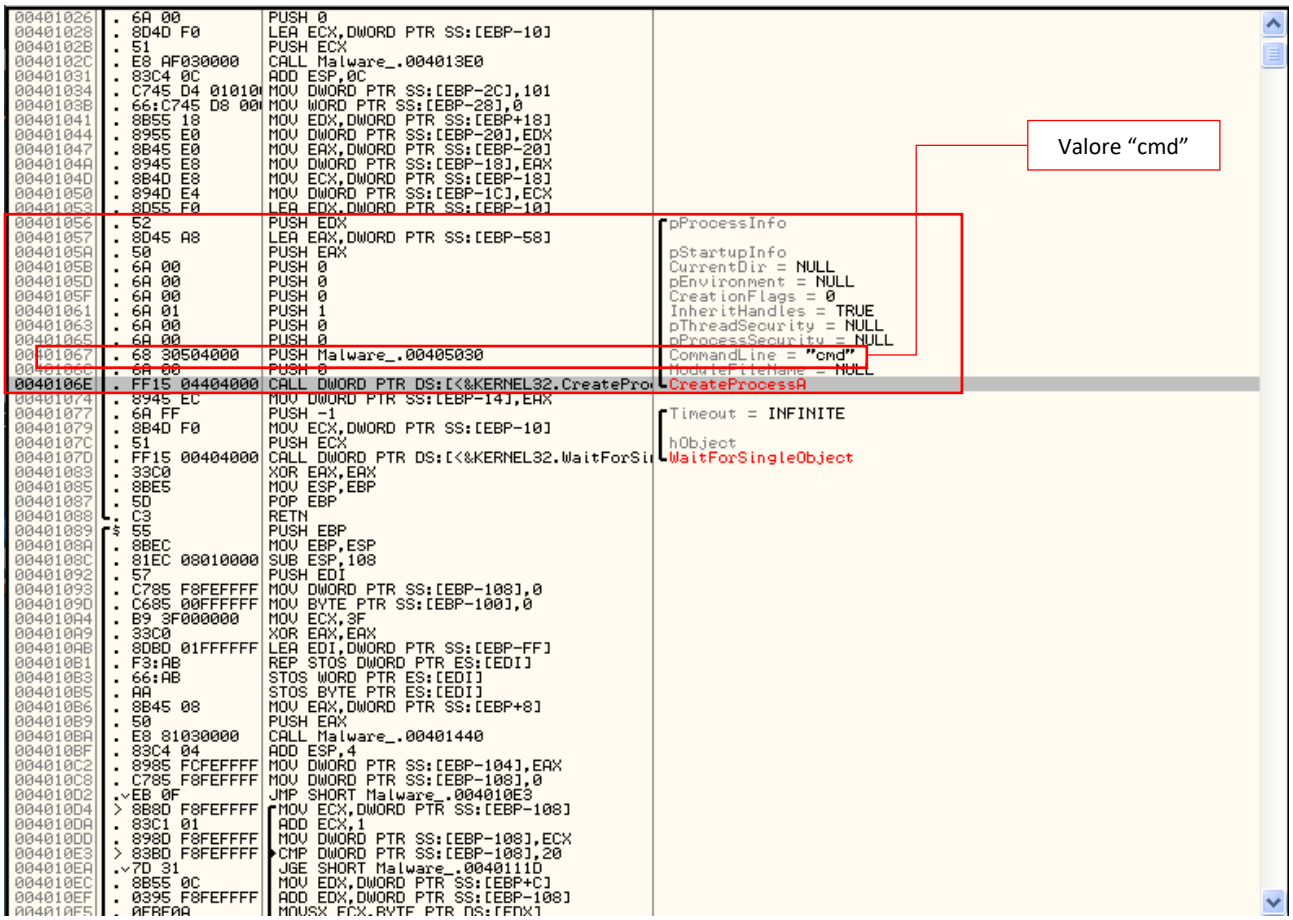
- **Inserite un secondo breakpoint all’indirizzo di memroia 004015AF. Qual è il valore del registro ECX? Eseguite uno “step-into”. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.**

All’indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione “CreateProcess”. Quel è il valore del parametro “CommandLine” che viene passato sullo stack ?

Una volta aperto il nostro malware ci ritroveremo con una schermata di questo tipo

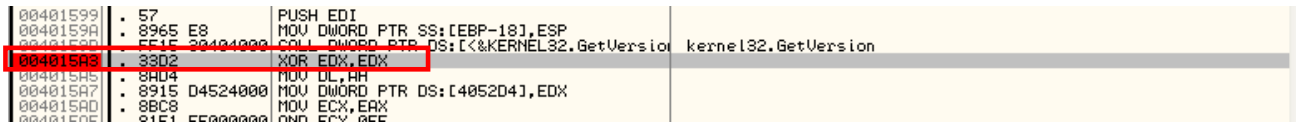


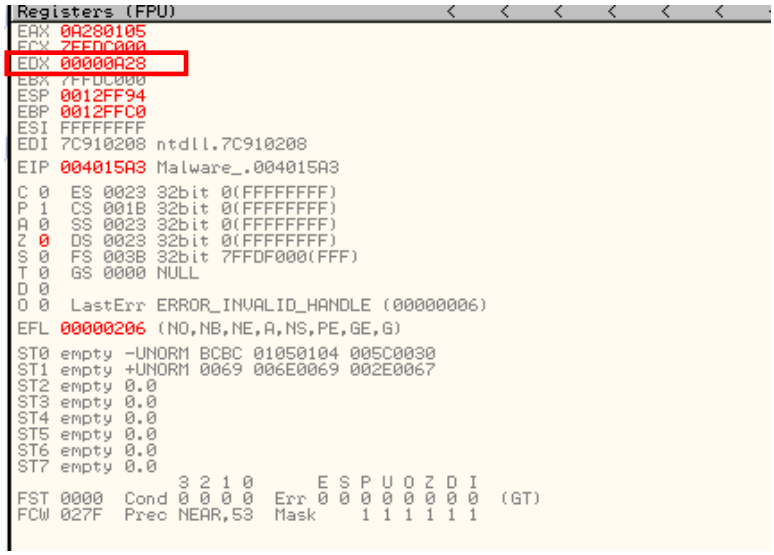
Ci rechiamo all'indirizzo di memoria richiesto **004015AF** dove possiamo vedere il valore del parametro "**CommandLine**"



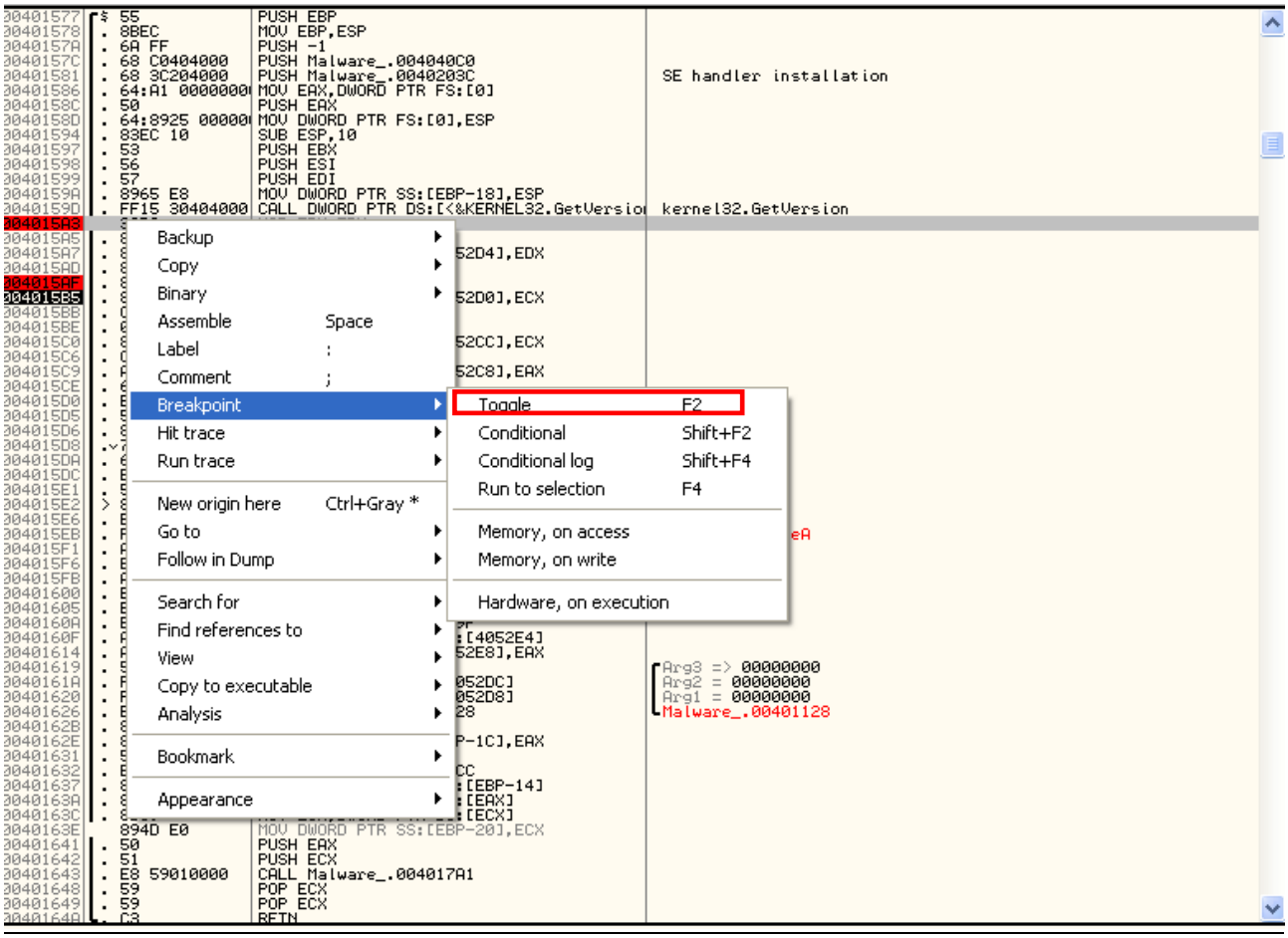
Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno "step-into". Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

Ci spostiamo all'indirizzo **004015A3** e leggiamo sulla destra il valore del registro EDX

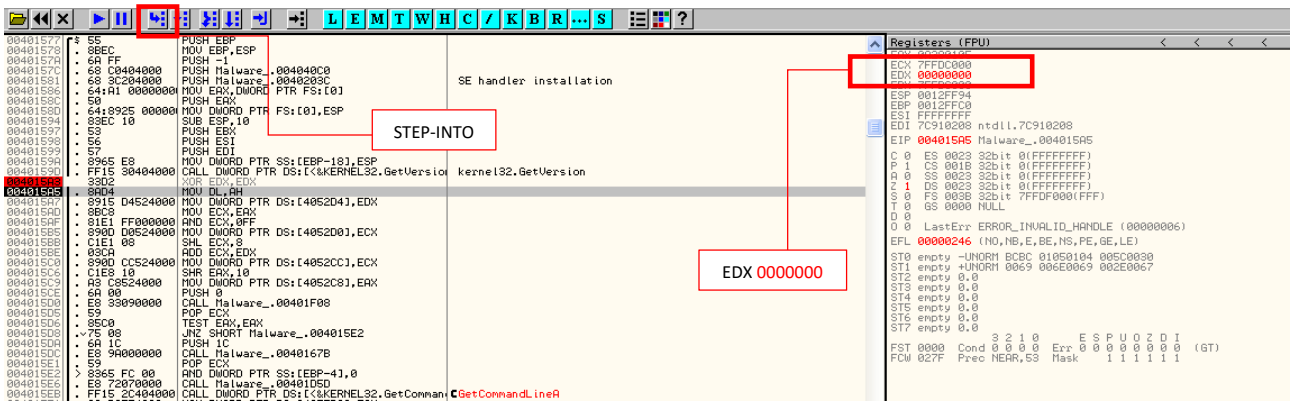




Inseriamo un **breakpoint** all'indirizzo, cliccando con il tasto destro >> Breakpoint >> Toggle

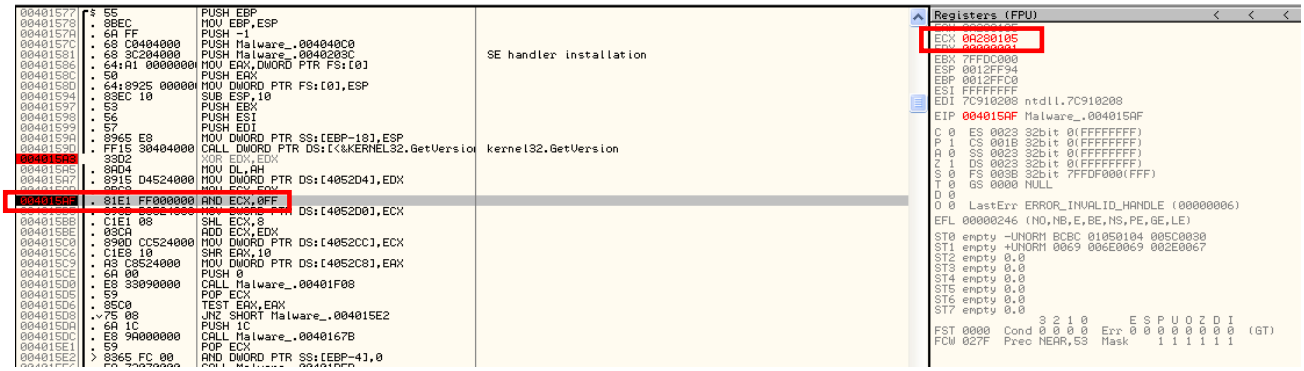


Inserito il **breakpoint** (lo notiamo dal colore rosso) eseguiamo uno **step-into** e notiamo come il valore di EDX si sia azzerato. Il risultato ottenuto è dovuto al fatto che la locazione di memoria precedente contiene un istruzione **XOR.** Operatore logico che mette a confronto destinatario e sorgente, e se i due valori sono identici l'istruzione darà come risultato **0**

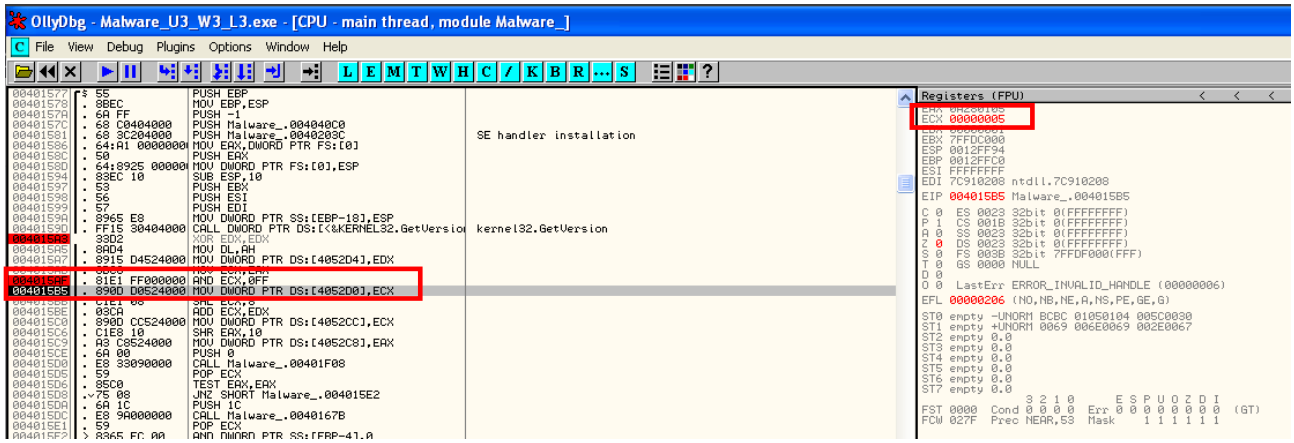


Inserite un secondo breakpoint all'indirizzo di memroia 004015AF. Qual è il valore del registro ECX? Eseguite uno "step-into". Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

Muoviamoci all'indirizzo di memoria **004015AF** e leggiamo il valore del registro **ECX**



Eseguiamo un altro **step-into** e notiamo il cambiamento del valore di **ECX**



Il cambio di valore è avvenuto per l'utilizzo dell'operatore logico **AND** nel punto precedente. Questa istruzione è un prodotto logico che esegue la and logica dei 2 operandi, in questo caso **ECX,OFF**