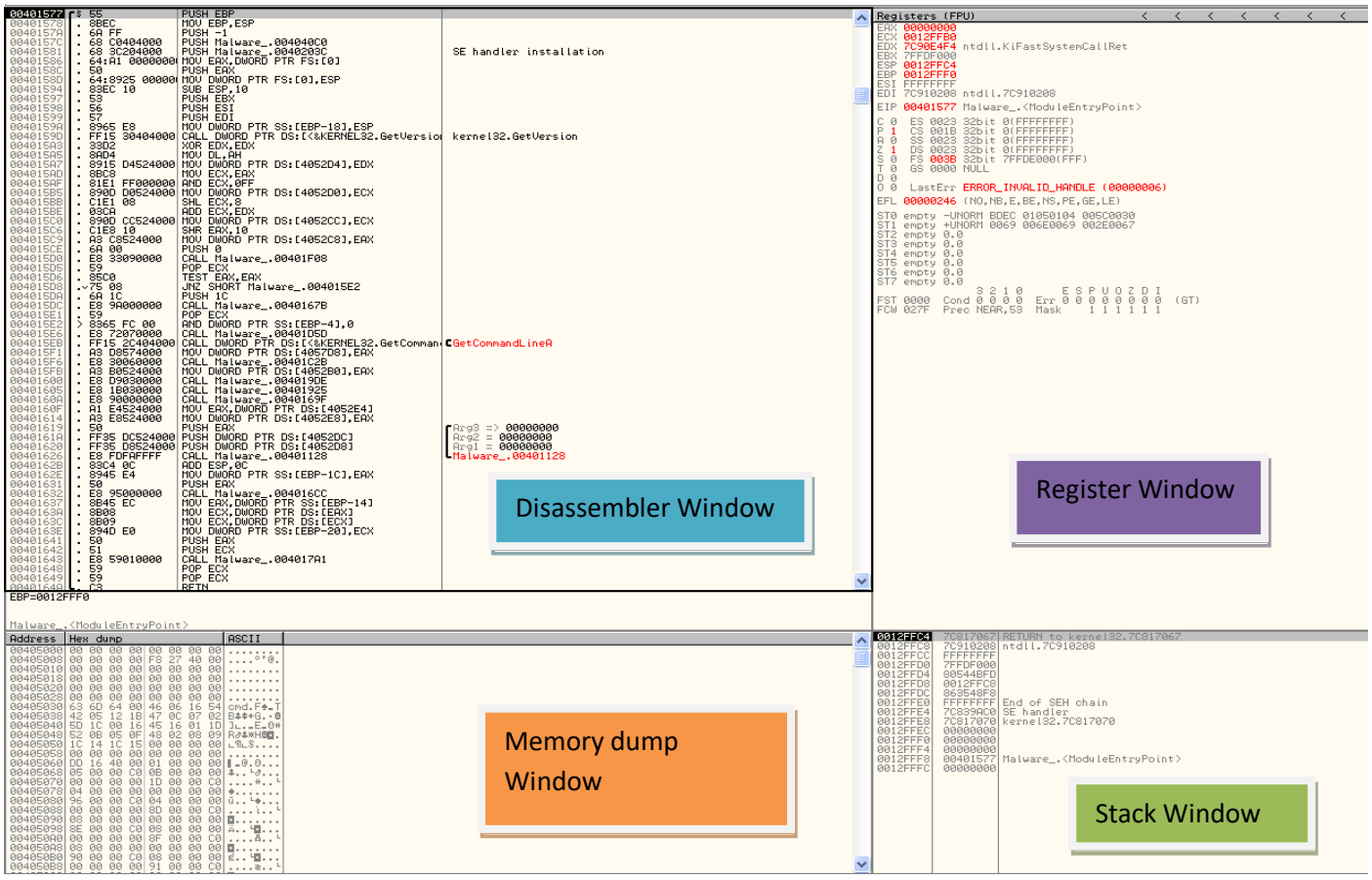
OLLY DBG

Tramite il tool OllyDBG, un debugger per sistemi Windows, che traccia registri, riconosce le funzioni e i parametri passati alle principali librerie standard,variabili,stringhe, eventuali salti condizionali ed altre componenti di codice, sarà possibile rispondere ai quesiti richiesti dalle task odierne.

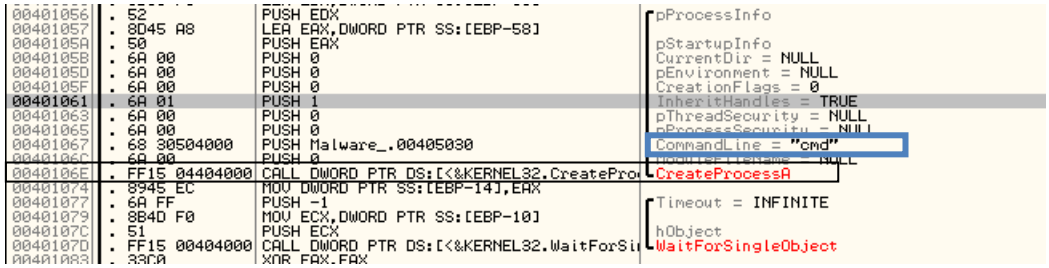
1.

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?

Dopo aver caricato il file d'interesse sul debugger, la schermata che si aprirà sarà la seguente



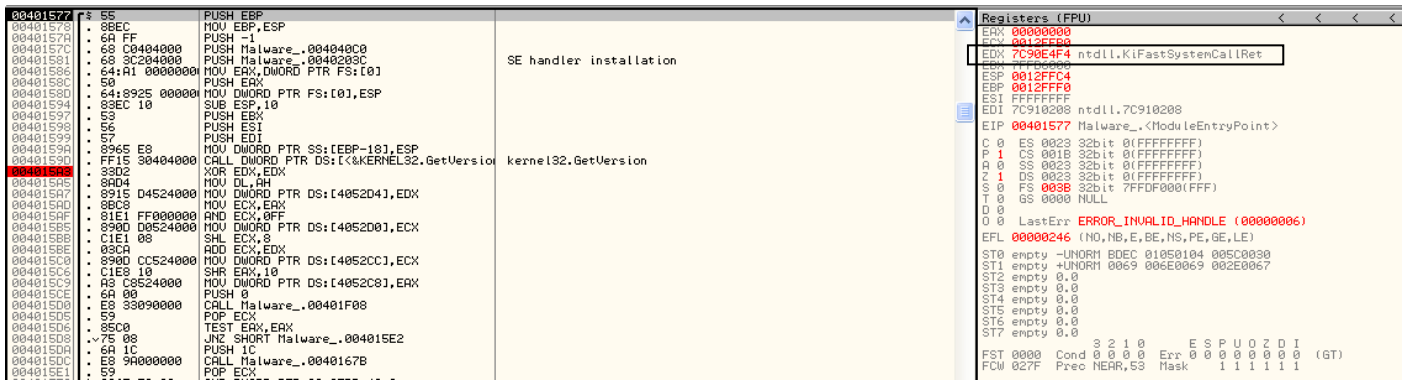
Per ritrovare informazioni circa le istruzioni eseguite dalla CPU, in questo caso specifico per capire il valore del parametro "Command Line" passato allo stack, sarà necessario analizzare attentamente la **Disassembler window**



Il valore del parametro <Command line> che viene passato sullo stack è <cmd> .

2. Cambiamento dei valori di registro EDX

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?



Cerchiamo l' indirizzo assegnato, 004015A3, con tasto desto scorriamo nella finestra a cascata fino alla sezione "breakpoint" scegliendone uno software, ossia "toggle"

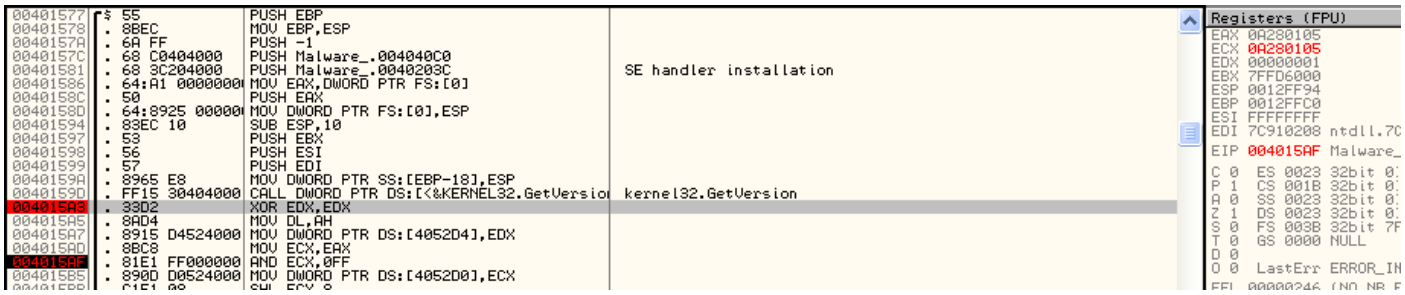
Il valore iniziale EDX sarà 7C90E4F4

Dopo aver inserito il breakpoint ed aver eseguito uno "step into" sarà possibile notare che alla "register window" è avvenuto un cambiamento nel valore del registro EDX

Il valore del registro EDX è adesso 00000000

3. Cambiamenti dei valori di registro ECX

Inserite un secondo breakpoint all'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.



Valore iniziale all'indirizzo di memoria 004015AF è 0A280105

Dopo aver inserito un breakpoint Toggle all'indirizzo specificato, ed eseguito uno step into il valore di ECX sarà 000000005