S11-L3

Traccia

Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

• All'indirizzo 0040106E il Malwareeffettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)

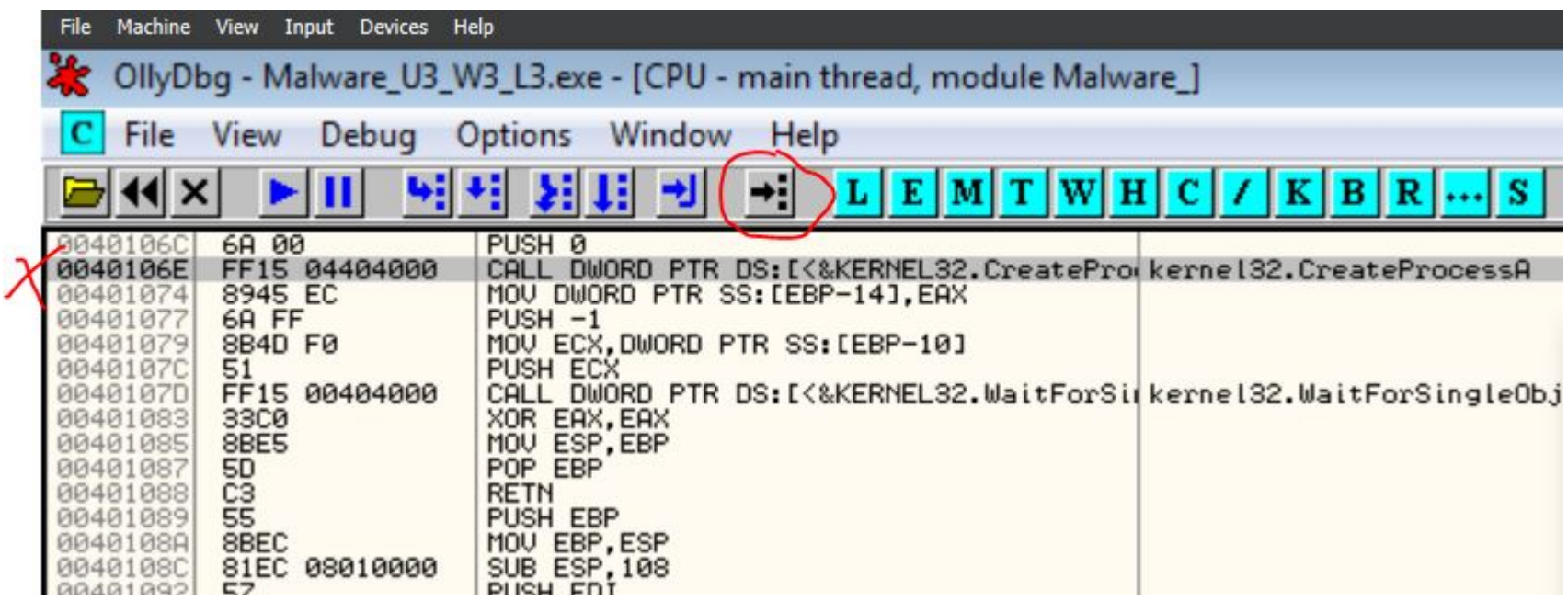
• Inserite un breakpointsoftware all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)

• Inserite un secondo breakpointall'indirizzo di memoria 004015AF. 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).

• BONUS: spiegare a grandi linee il funzionamento del malware

Task 1

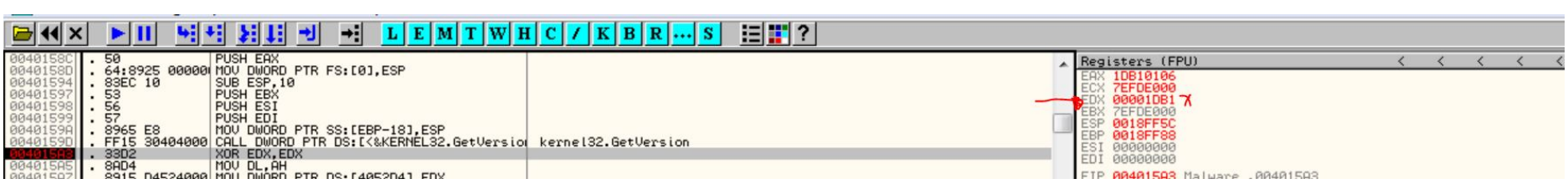
Cliccando sul pulsante cerchiato possiamo eseguire una ricerca. Nella schermata che compare inseriamo l'indirizzo 004015A3 per apprezzare a schermo quanto nell'immagine.



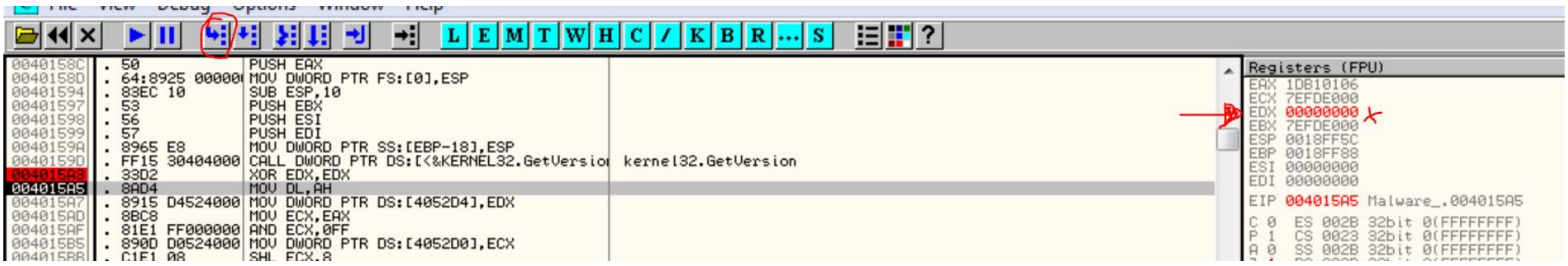
Mettiamo il breakpoint sul suddetto per poi lanciare il programma.
Il valore del parametro Commandline passato sullo stack è cmd.

Task 2

Identifichiamo 004015A3 e mettiamo il breakpoint.
Fatto questo lanciamo il programma ed osserviamo l'EDX (00001DB1)



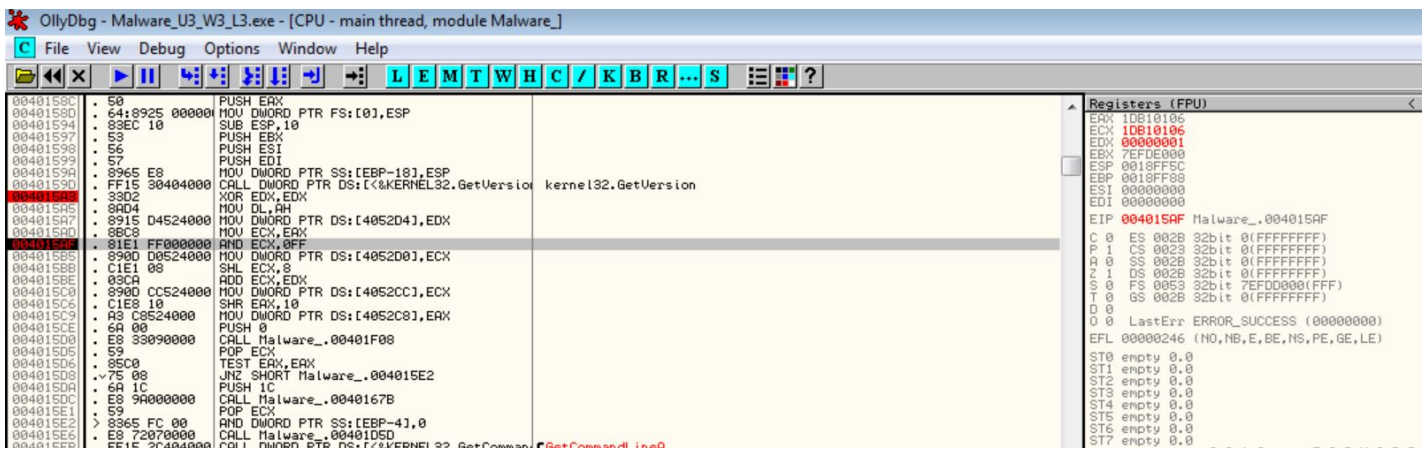
Eseguiamo quindi step-into ed osserviamo come varia il valore del registro EDX (diventerà 00000000):



L'output è 0 dato che stiamo parlando di XOR ed in questo caso i due valori sono uguali (EDX ed EDX).

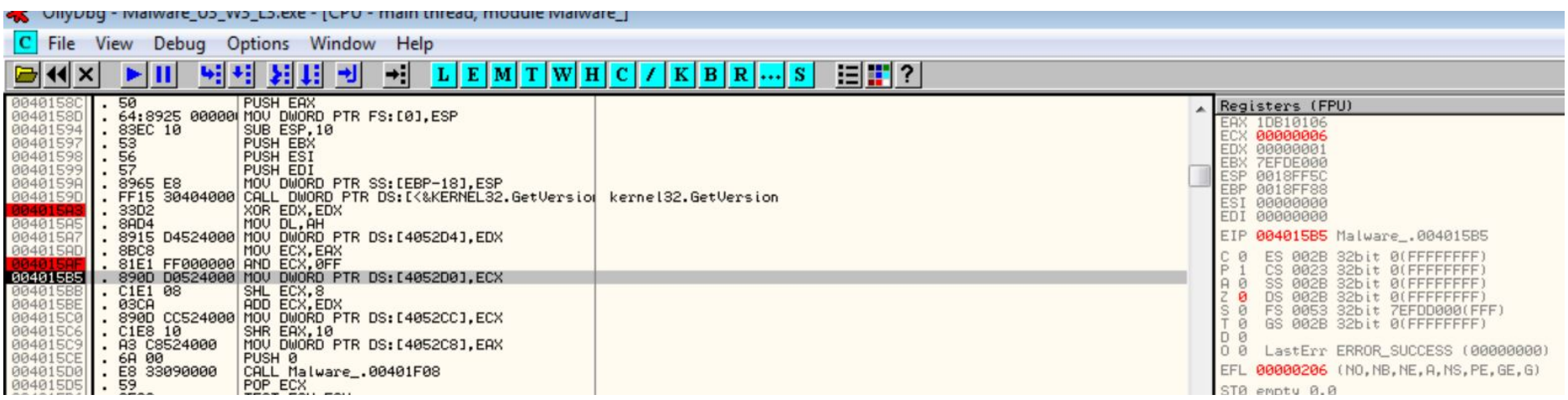
Task 3

Mettiamo il secondo breakpoint come nell'immagine sotto e lanciamo il tutto.



Come possiamo vedere, l'ECX è: 1DB10106.

Come richiesto dalla traccia procediamo con lo step-into per apprezzare i cambiamenti del registro EXC.



In questo caso diventa 00000006

Bonus

Da quanto appreso possiamo notare come il malware può creare sia processi che connessioni di rete. Non sono in grado di dedurre altro.