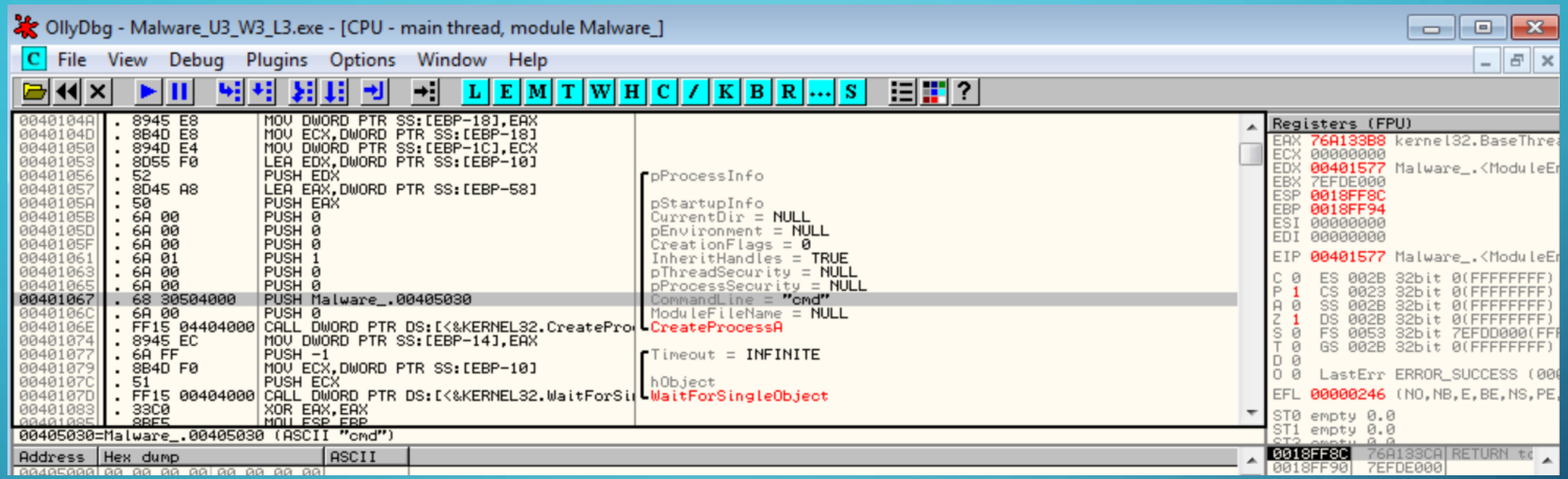
ES LEZIONE 3 SETTIMANA 11

Traccia:

Fate riferimento al malware: **Malware_U3_W3_L3**, presente all'interno della cartella **Esercizio_Pratico_U3_W3_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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**? **(1)**
- Inserite un breakpoint software 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 breakpoint all'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

1°



1°

Il valore del parametro "commandLine" che viene passato sullo stack è "Malware_.00405030".

2°3°4°5°

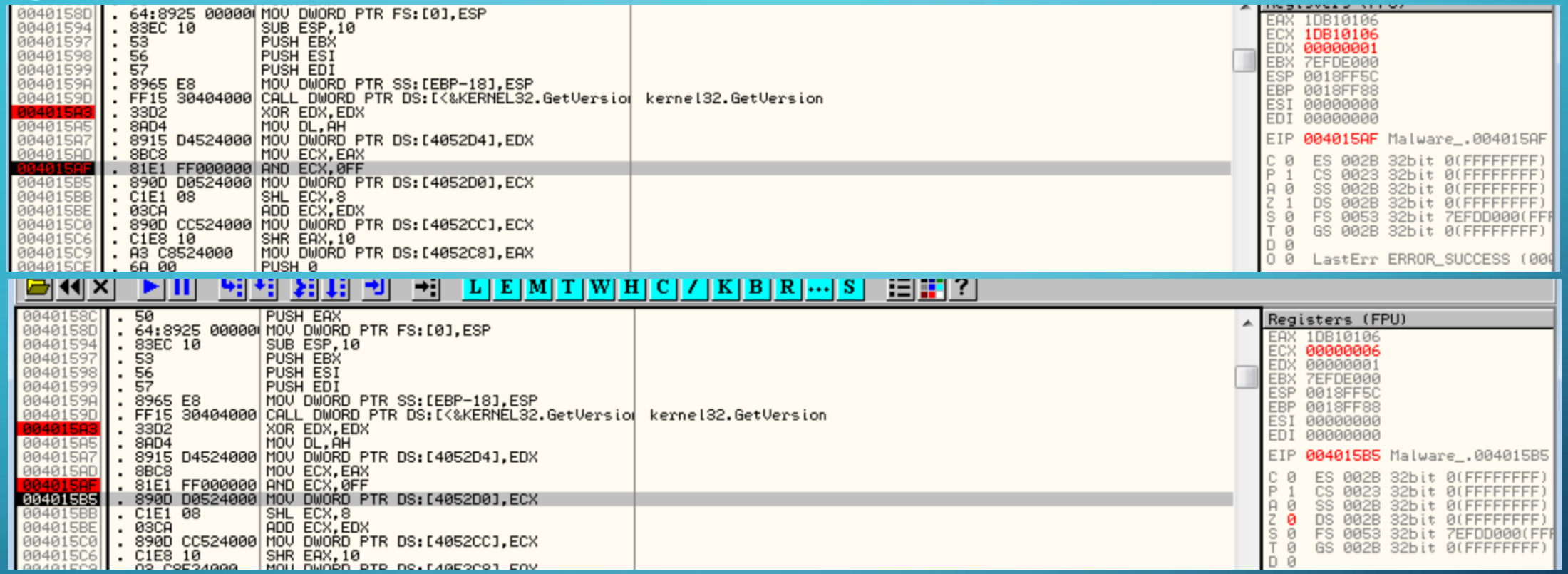
2° Inizialmente il valore di EDX è "00001DB1"

3° Successivamente il valore diventa "00000000"

4° Questo perché è stata eseguita la funzione dell'indirizzo "4015A3" ossia "XOR EDX,EDX.

5° L'OR esclusivo (XOR) è un'operazione tra due bit in cui il bit risultante vale 0 se i due bit comparati sono uguali.

6°7°8°



6° Inizialmente il valore di ECX è "1DB10106"

7° Successivamente il valore diventa "00000006"

8° Questo perché è stata eseguita la funzione dell'indirizzo "4015AF" ossia "AND ECX,OFF". Ossia la comparazione logica (AND) tra i due valori.