**OllyDBG**

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 Malware effettua una chiamata di funzione alla funzione «Create Process». Qual è il valore del parametro «Command Line» 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)

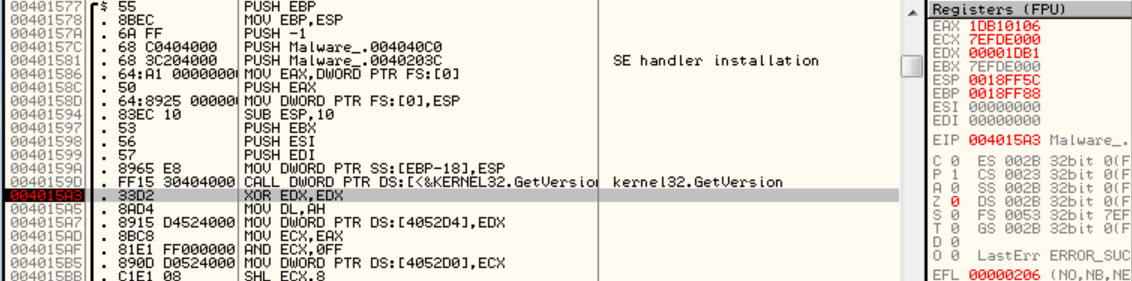
• Inserite un secondo breakpoint all’indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).

1) Il valore del parametro «Command Line» che viene passato sullo stack è CMD all’indirizzo 00401067

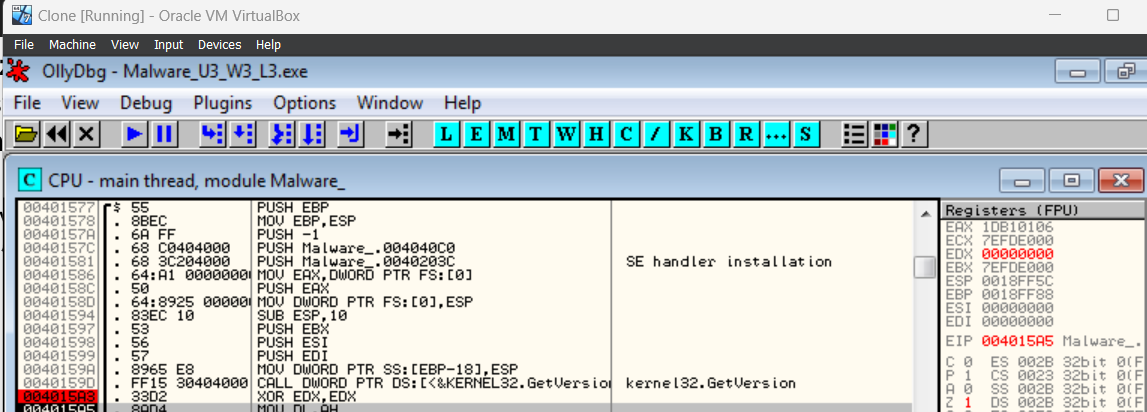
A screenshot of a computer program

Description automatically generated

2) E' il valore del registro EDX è 00001DB1:



3) Il valore di EDX dopo lo step into è 00000000 quindi 0



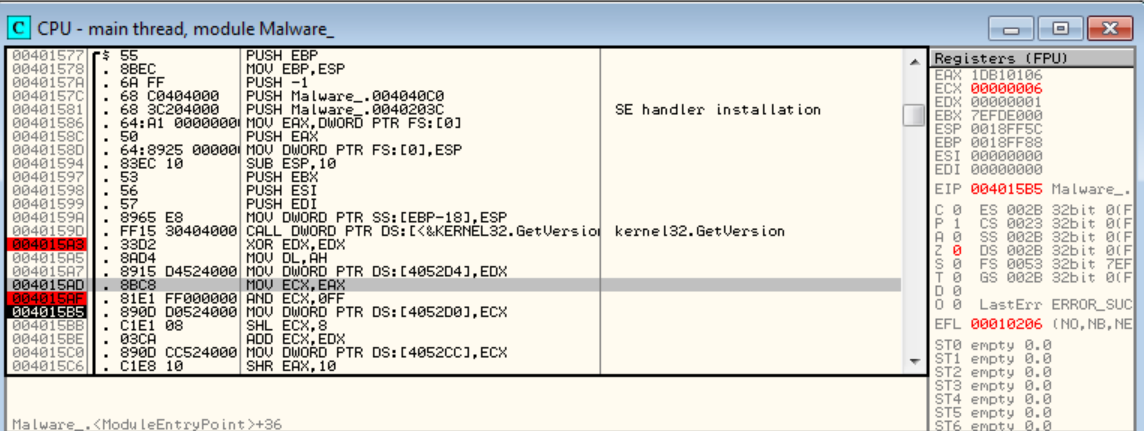
4) Dopo lo step-into, l’istruzione XOR, EDX, EDX viene eseguita che di fatto equivale ad analizzare a zero una variabile; quindi, il valore di EDX dopo lo step into è 0.

5) L’istruzione eseguita è XOR, EDX, EDX

6) Il valore del registro ECX è IDB10106A screenshot of a computer

Description automatically generated

7) il valore di ECX dopo lo step into è 000000006:



8) L’istruzione eseguita è AND, ECX, OFF