Esercitazione WEEK W24D1

OllyDBG

Ettore Farris

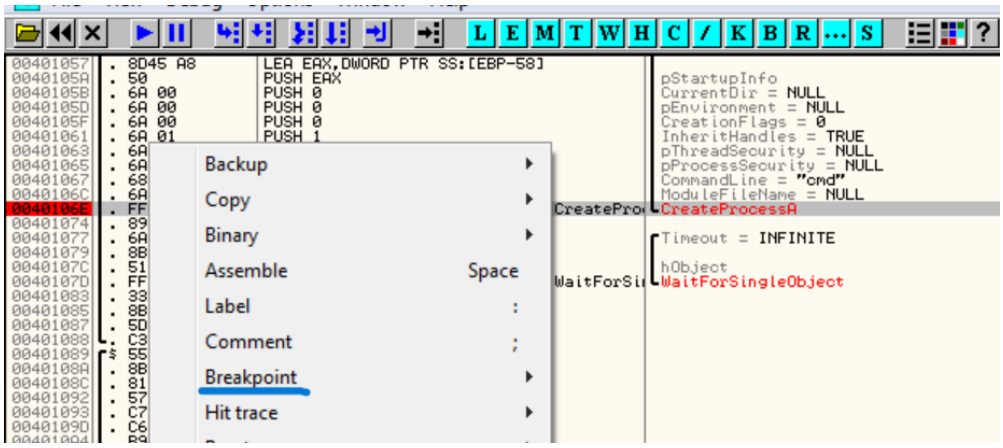
Descrizione sintetica e risoluzione

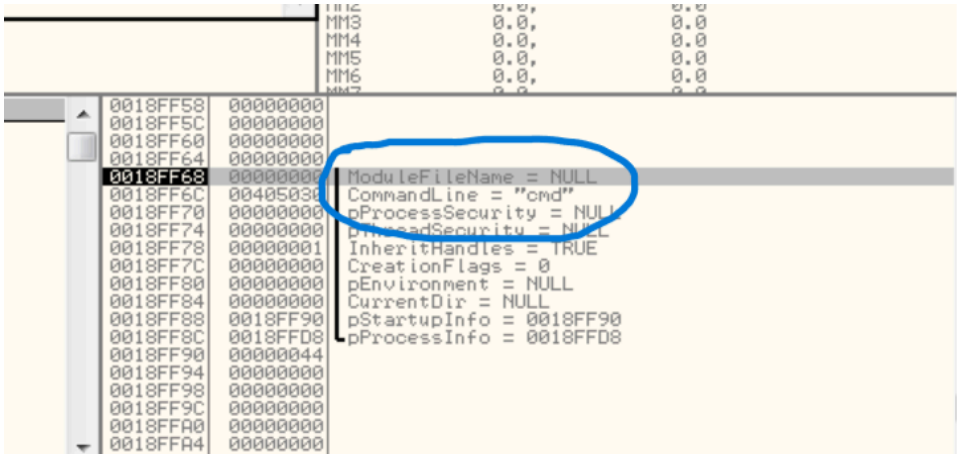
Traccia:

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)***

Una volta aperto il debugger e caricato l'eseguibile, settiamo il breakpoint all'indirizzo *0040106E* ed avviamo l'esecuzione. Sullo stack possiamo vedere che il parametro *CommandLine* ha valore "*cmd*".

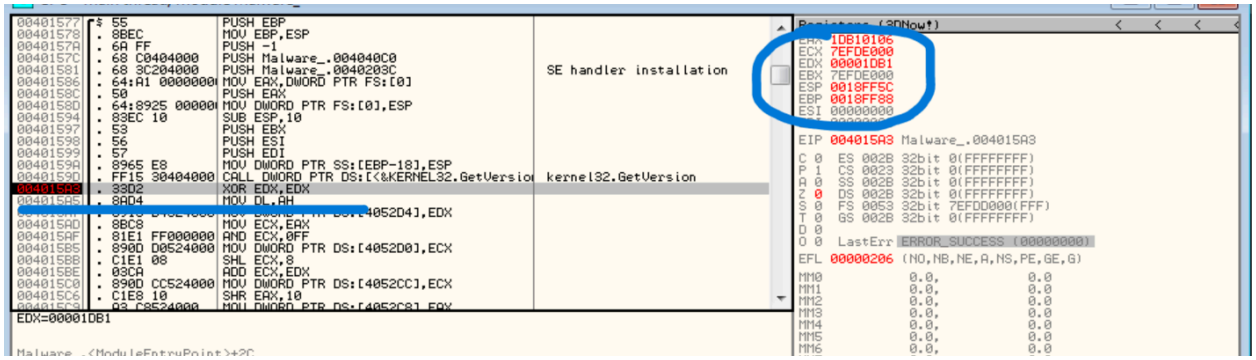




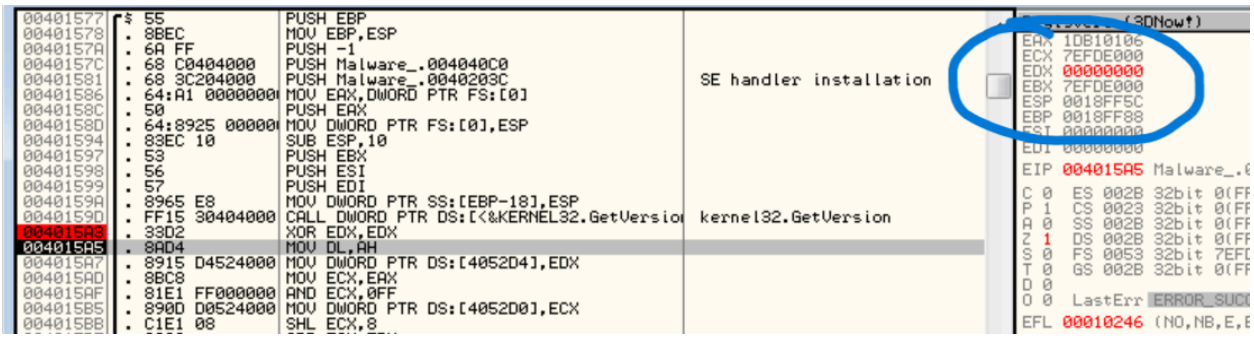
- ***Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)***

Una volta settato il breakpoint, il valore di EDX è 00001DB1. L'istruzione effettua una XOR EDX, EDX settando quindi il registro a 0. Eseguita l'istruzione quindi, il valore del registro EDX viene azzerato.

Prima dell'esecuzione

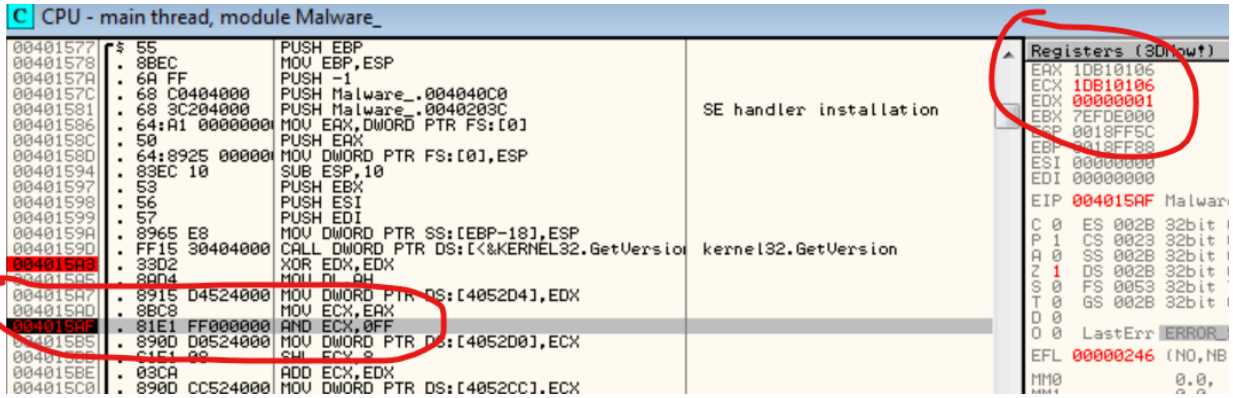


Dopo l'esecuzione



- ***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).***

A partire dal punto precedente, impostiamo il breakpoint su *004015AF.* Il valore del registro ECX è 1DB10106(in binario 0001 1101 1011 0001 0000 0001 0000 0110).



Effettuando la *step-into,* viene eseguita un'istruzione AND tra il valore del registro ECX e il valore esadecimale *0FF* (0000 0000 0000 0000 0000 0000 1111 1111 in binario usando 32 bit). Quindi, l'AND *bitwise* (cioè bit a bit) tra:

- 0000 0000 0000 0000 0000 0000 1111 1111

e

- 0001 1101 1011 0001 0000 0001 0000 0110

corrisponde a:
0000 0000 0000 0000 0000 0000 0000 0110

che in esadecimale vale *6*.

Eseguendo l'istruzione, il valore del registro ECX vale infatti *6*.