Report Esercizio

W24-D2

Redatto da Andrea Sciattella

01/08/2024

TRACCIA

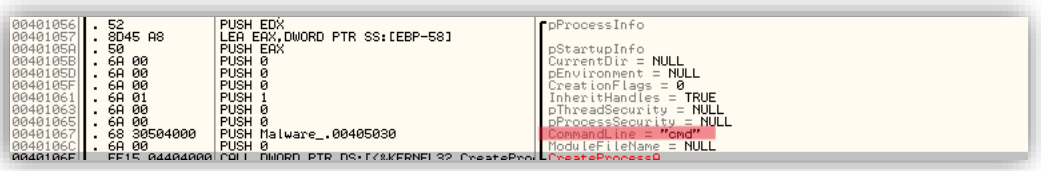
Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3 sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

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?
2. Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?
3. Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta, Che istruzione è stata eseguita?
4. Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?
5. Eseguite uno step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

SVOLGIMENTO ESERCIZIO

Impostiamo il nostro laboratorio aprendo il debugger OllyDBG. Selezioniamo in alto a destra la cartella e navighiamo nella cartella del nostro eseguibile da analizzare, nel nostro caso "Malware_U3_W3_L3".

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?*

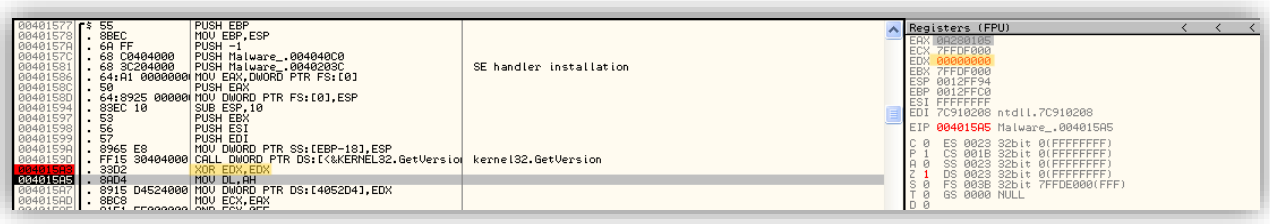


- Nello screenshot vediamo la risposta evidenziata in rosso, nel parametro "CommandLine" viene passato il valore "cmd" sullo stack.

2. *Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?*

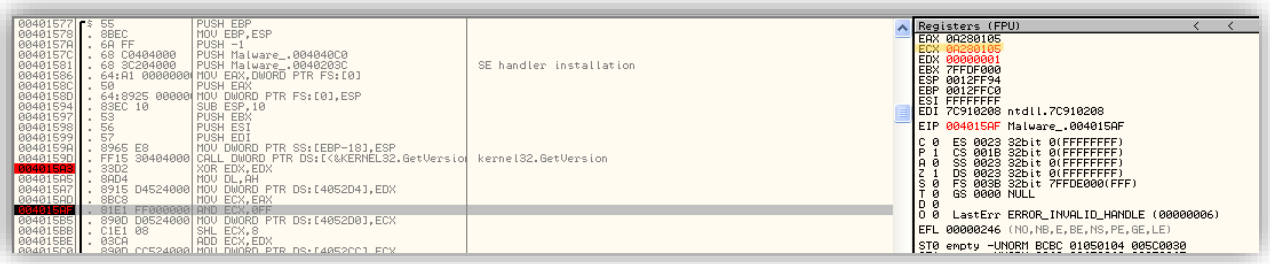
- Per inserire il breakpoint selezioniamo prima l'indirizzo, tasto destro e scendiamo alla voce breakpoint e poi toggle per inserire il breakpoint software. Il valore del registro EDX è "***00000A28***".

3. *Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta, Che istruzione è stata eseguita?*



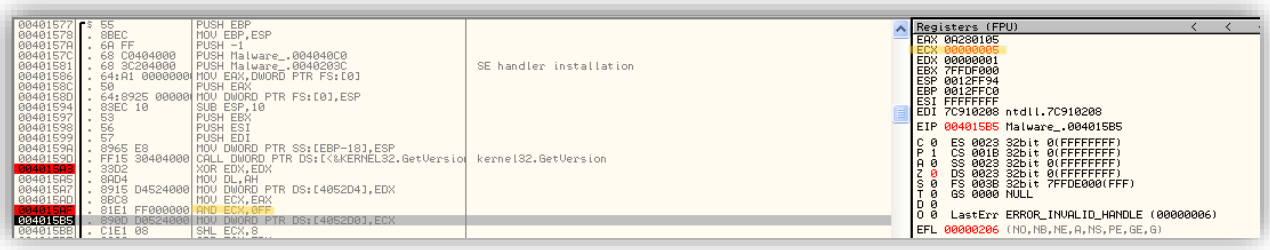
- Eseguiamo lo step-into per analizzare l'azione compiuta. L'azione compiuta è un XOR logico tra il medesimo registro (EDX, EDX), che visto l'uguaglianza dei valori del registro restituisce "***00000000***", il nuovo valore di EDX.

4. *Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?*



- Impostiamo il secondo breakpoint all'indirizzo "*004015AF".* Il valore di ECX ora è "***0A280105***".

5. *Eseguite uno step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.*



- Eseguiamo lo step-into dal breakpoint per analizzare i valori. Ora verrà eseguita l'istruzione con loperatore logico AND (AND ECX, 0FF). La condizione logica di questo operatore diventa vera solo quando le entrambe condizioni sono vere (quindi 1 in binario). Il risultato tra i due dati trasformati in binari da esadecimali di ECX

(10100010100000000000100000101) ed il valore 0FF (1111 1111) è 101 che in esadecimale equivale a 5. Il nuovo valore di ECX è "***00000005***".