Esercizio OllyDBG | Marco Malizia - DataShields

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 «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)

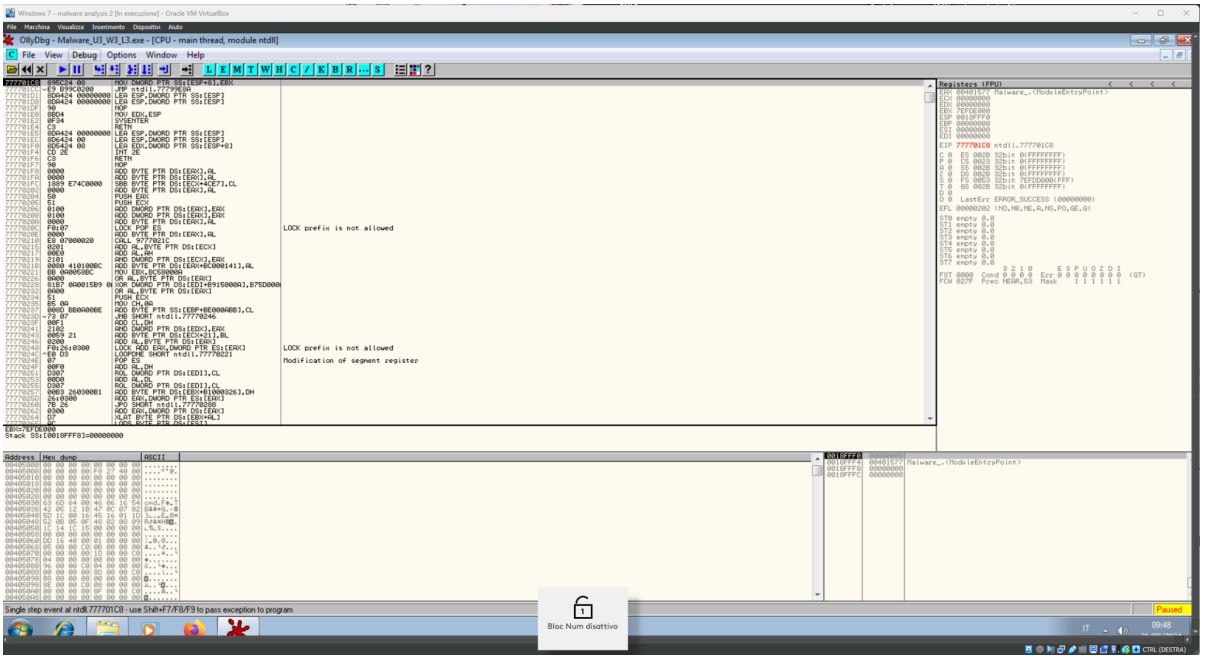
• Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)

• 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

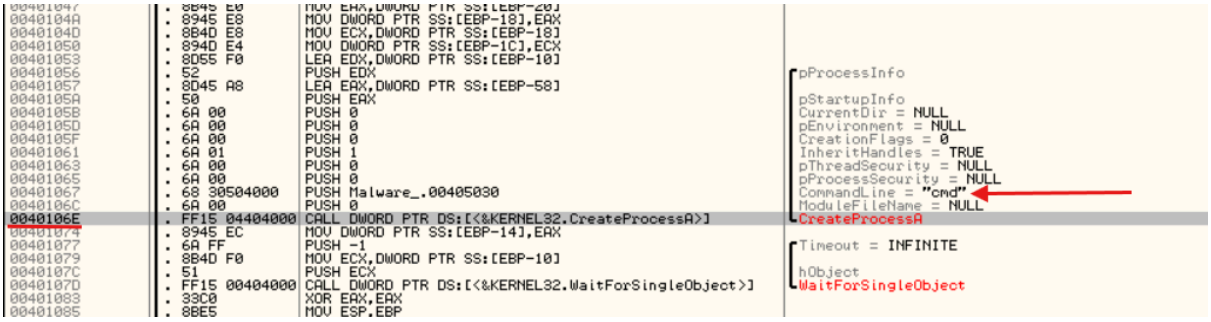
Svolgimento:

Avvio della macchina e del software OllyDBG.



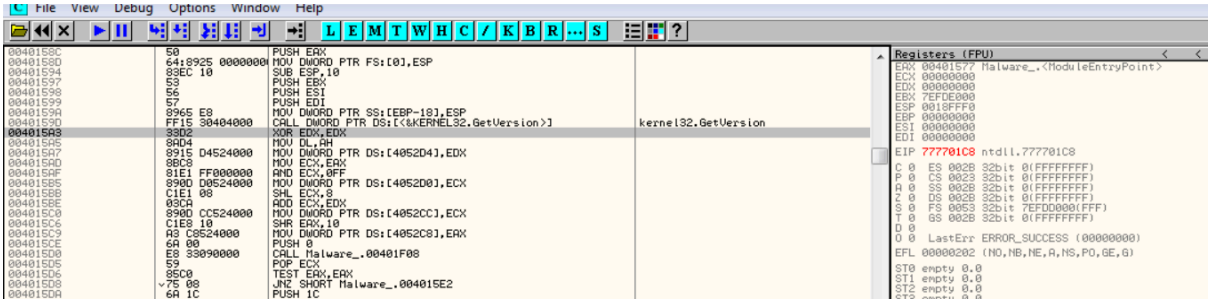
1. **All’indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?**

Dopo aver aperto il file da analizzare andiamo a ricercare l’indirizzo indicato nella traccia.
Il parametro di CommandLine è indicato nella quarta colonna e corrisponde a “cmd”.

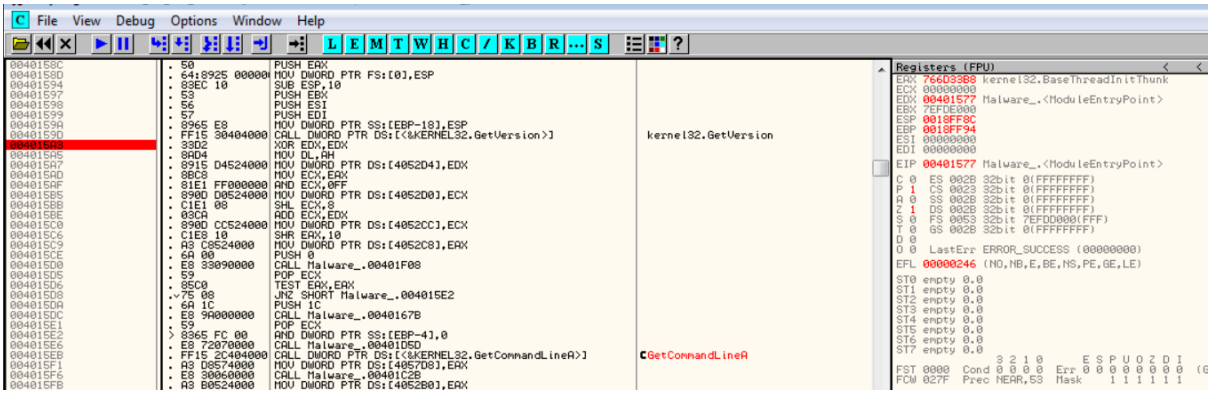


2. **Inserite un breakpoint software all’indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)**

Questa è la sequenza delle azioni, nella prima immagine andiamo ad identificare l’indirizzo oggetto di analisi.

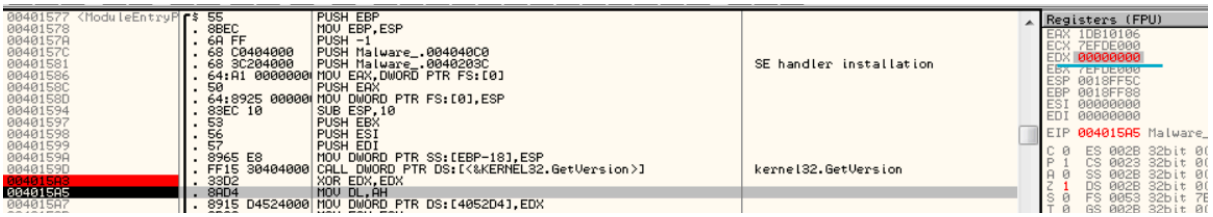


In questa immagine mostriamo come andiamo ad inserire il “breakpoint”.



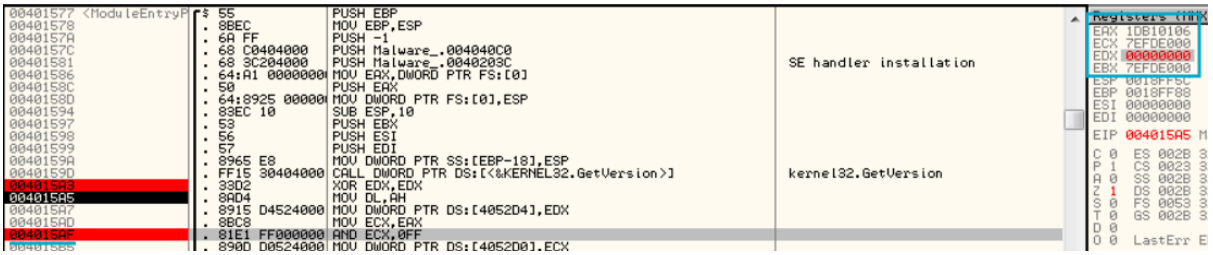
Eseguendo il programma possiamo vedere come il valore del registro EDX è diventato **0001DB1**.

Utilizzando la funzione “Step-into” nella barra degli strumenti, che permette di entrare nel codice della funzione in esame, abbiamo notato che il valore EDX nel registro è mutato in **00000000**

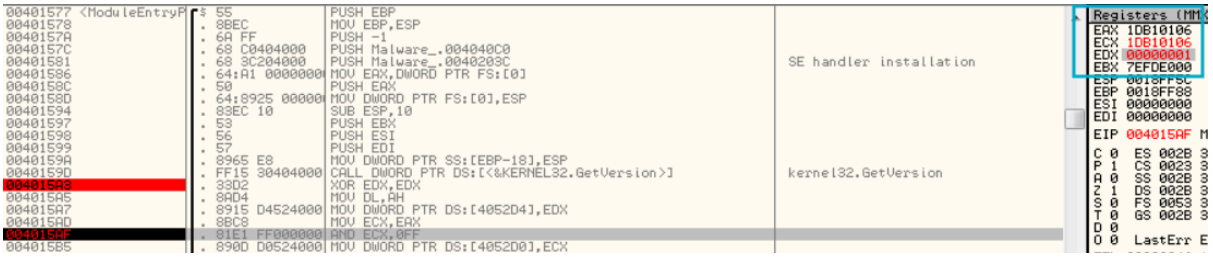


Questo cambiamento è dovuto all'operazione logica XOR nel codice, che restituisce sempre 0 quando applicata a due valori uguali. In questo caso, l'operazione XOR ha annullato il valore precedente di EDX, impostandolo a zero.

3. **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).**



Configuro il secondo breakpoint, il valore del registro ECX è **1DB10106**



Dopo lo step-into il valore del registro ECX è stato modificato in **00000006** in quanto è stata eseguita l'istruzione AND ECX, FF.
In questo caso c'è un operato logico AND il quale ricevendo in ingresso almeno due valori restituisce 1 solo se tutti i valori di ingresso hanno valore