OllyDBG

ESERCIZIO

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).

Parametro «CommandLine»

Il valore del parametro «CommandLine» che viene passato sullo stack è **“cmd”**

Valore registro EDX

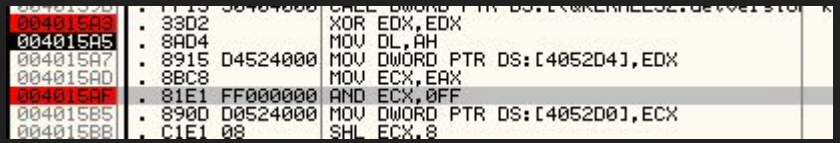
Cliccando col destro e scegliamo la voce Breakpoint sull'indirizzo 004015A3

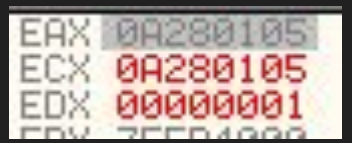
Dopo lo step-in il valore del registro EDX è cambiato in:

poichè l'istruzione XOR EDX,EDX inizializza la variabile a 0

Valore registro ECX

Cliccando col destro e scegliamo la voce Breakpoint sull'indirizzo 004015AF





Dopo lo step-in il valore del registro ECX è cambiato in:

l'istruzione AND ECX, 0ff fa si che i bit in ECX vengano confrontati con 0ff, e se i bit in colonna sono entrambi 1 restituirà 1, altrimenti sarà 0. Dopo l'AND i bit vengono tradotti in esadecimale e il risultato sarà appunto 0000.0005