Malware analysis – OllyDBG

Sommario

Traccia S11-L3

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.

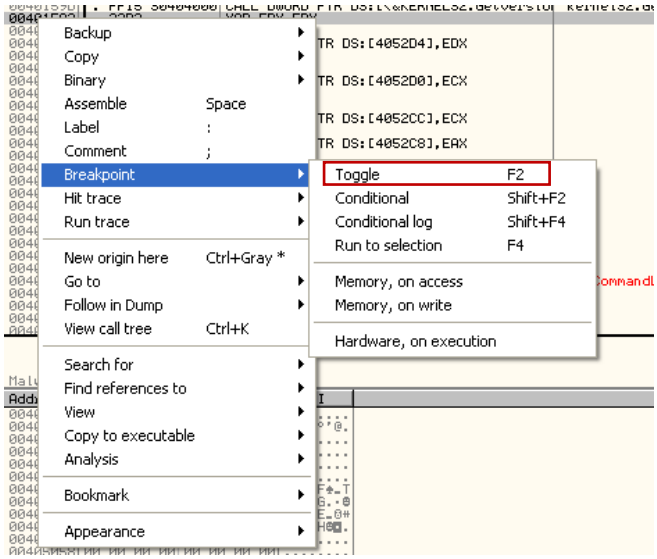
- Step 1: all'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)
- Step 2: inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite 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)
- Step 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).

Step 1

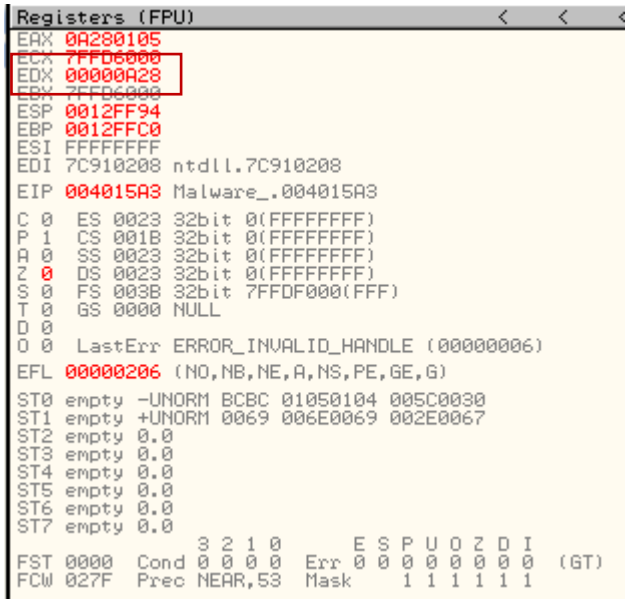
Il valore del parametro «CommandLine» passato sullo stack è "cmd"

Step 2

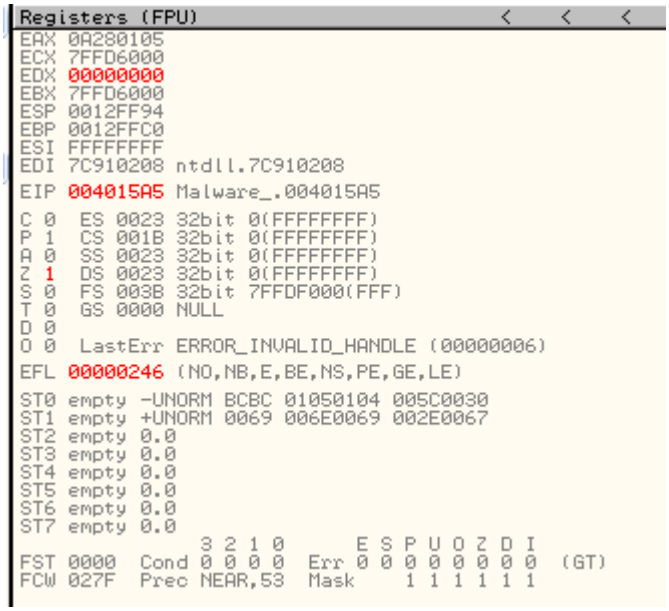
Inseriamo il breakpoint cliccando col tasto destro sull'indirizzo indicato e successivamente su breakpoint e toggle.



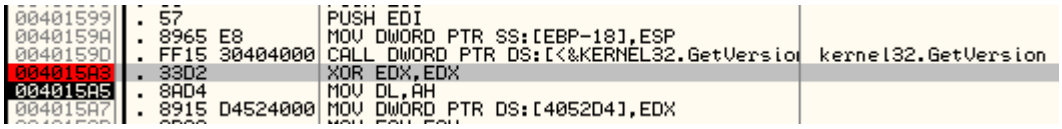
Avviamo il debugging del codice col tasto play e possiamo vedere che nella finestra Registers (FPU) che il valore del registro EDX è 00000A28.



Ora eseguiamo lo step-into cliccando sul tasto nel riquadro rosso. Lo utilizziamo per esaminare righe di codice e, a fronte di una chiamata di funzione, per accedere alla sua implementazione

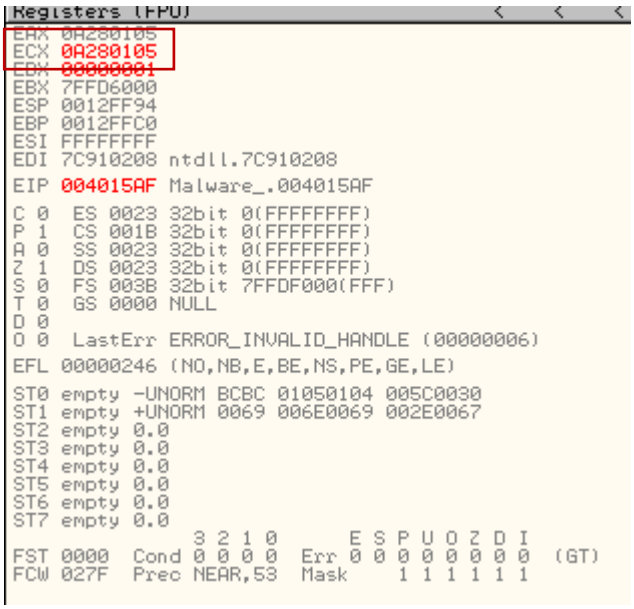


Il valore del registro EDX ora è 0, perché la funzione XOR contenuta inizializza il registro a 0, siccome il risultato di uno XOR tra due operandi uguali è sempre 0.

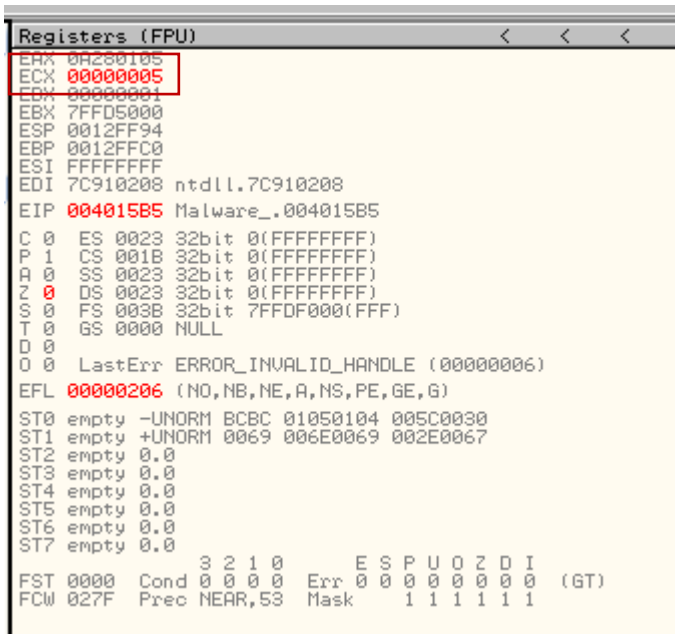


Step 3

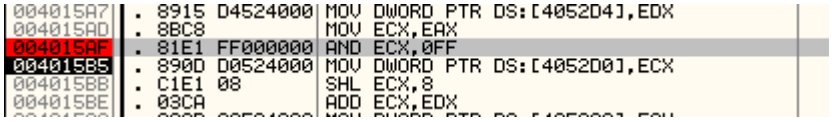
Inseriamo un secondo breakpoint all'indirizzo di memoria 004015AF. Il valore del registro ECX è 0A280105.



Effettuiamo nuovamente anche lo step-in e possiamo vedere che il registro ECX ha ora il valore di 5.



Questo perché in questa posizione l'istruzione **and ECX, 0FF** esegue un'operazione AND bit a bit tra il valore nel registro ECX e 0ff.



ECX: 00001010 00101000 00000001 00000101 (0A280105 in binario)

0FF: 00000000 00000000 00000000 11111111 (000000FF in binario)

Risultato: 00000000 00000000 00000000 00000101 (00000005 in binario)