Esercizio 05-04

Traccia: facendo 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?

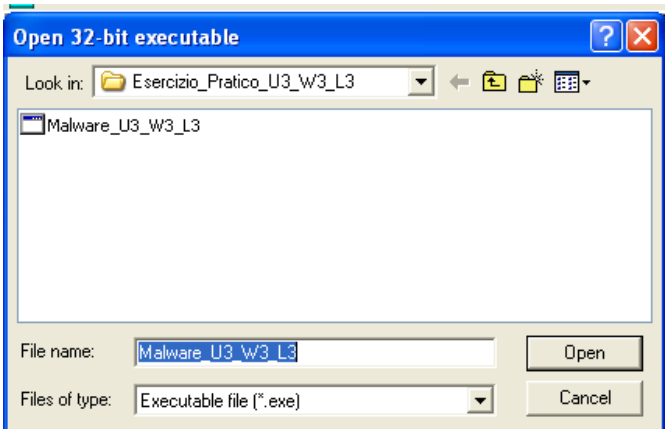
2. Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? eseguite a questi punto uno "step-into". Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

3. Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

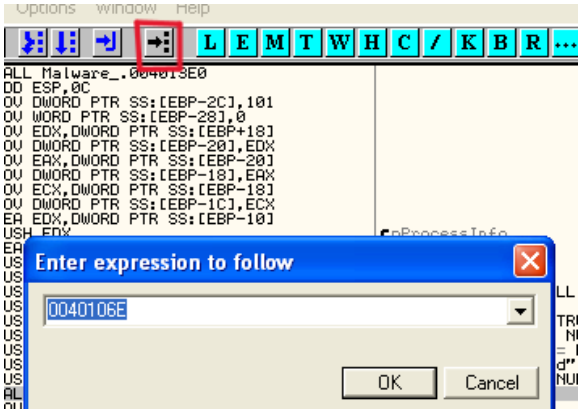
4. BONUS: ipotizzare il funzionamento del malware

1.

Dopo aver avviato OllyDBG carichiamo l'eseguibile da analizzare

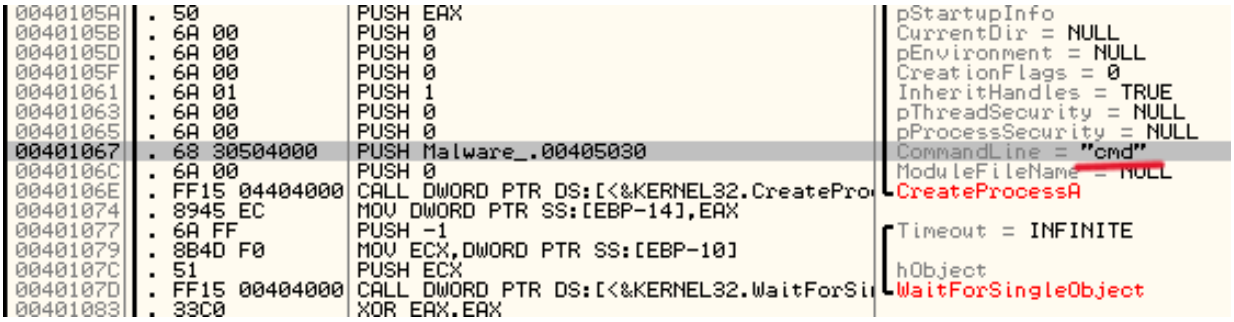


Conoscendo l'indirizzo della funzione che vogliamo analizzare (0040106E) utilizzando l'iconcina apposita possiamo spostarci direttamente all'indirizzo che mettiamo



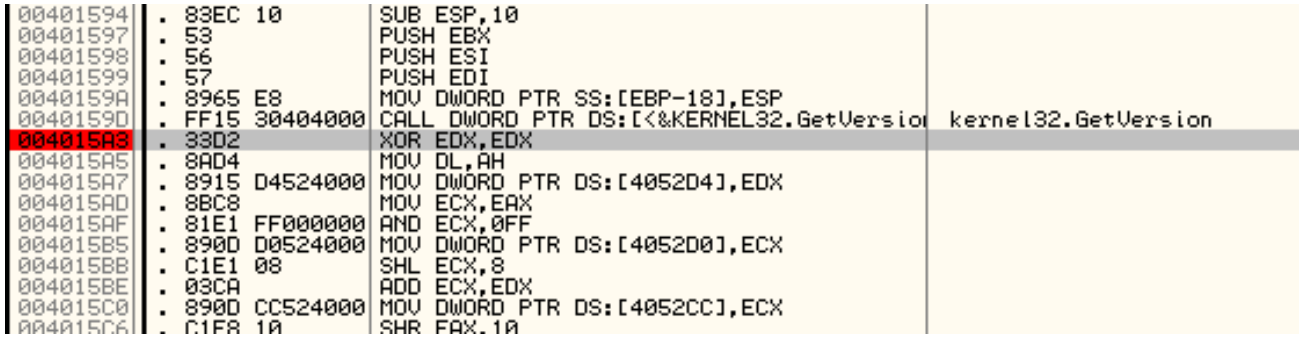
Eccoci all'indirizzo che abbiamo specificato, adesso andiamo a vedere quale valore viene passato al parametro CommandLine della funzione CreateProcess

Il parametro che viene passato a CommandLine è "cmd", il prompt comandi di Windows

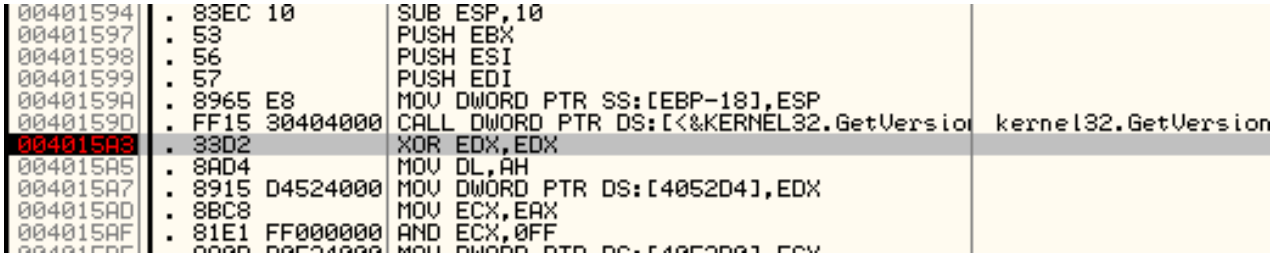


2.

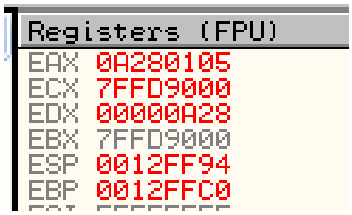
Aggiunta di un software breakpoint all'indirizzo 004015A3, in questo punto il registro EDX diventa "0", essendo risultato di uno XOR che compara due registri uguali



Eseguendo il programma con il comando “run” il flusso si bloccherà al breakpoint appena messo

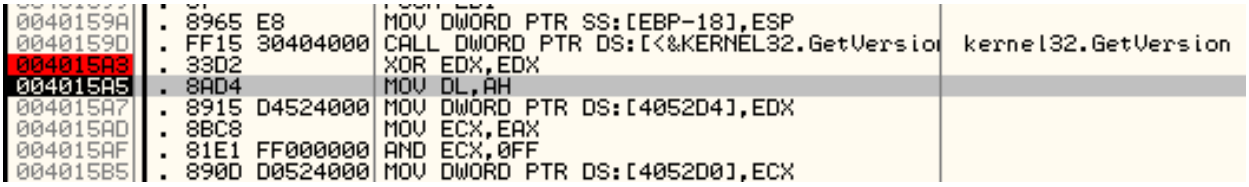


Il valore di EDX in esadecimale e di A28 (2 600 decimale)

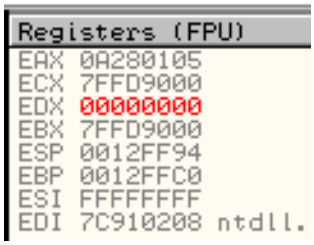


Adesso eseguiamo uno “step - into” con l’icona apposita o F7

Il codice è proseguito all’istruzione successiva

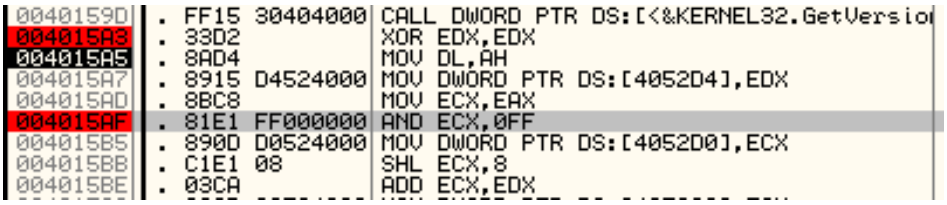


Il valore di EDX è cambiato, come conseguenza dello XOR tra due valori uguali restituisce “0”

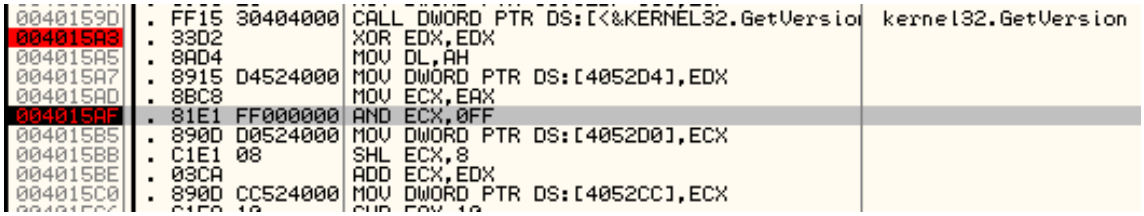


3.

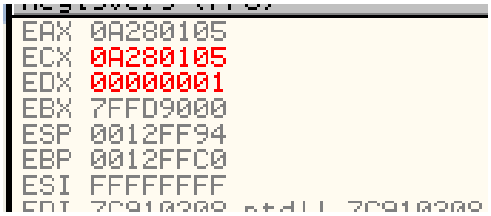
Aggiunta di un breakpoint all'indirizzo 004015AF



Cliccando su "run" il flusso del programma prosegue e raggiunge il breakpoint

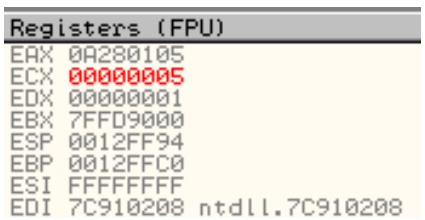


Qui il valore di ECX è A280105 che in decimale corrisponde a 170 393 861



Eseguendo uno "step - into" il codice prosegue all'istruzione successiva

Il valore di ECX è cambiato, come risultato dell' AND precedente restituisce il valore 5 (corrispondente a 5 anche in decimale)



Risoluzione dell'operazione con i valori in codice binario

FF = 0000 0000 0000 0000 0000 0000 1111 1111

A280105 = 0000 1010 0010 1000 0000 0001 0000 0101

Risultato = 0000 0000 0000 0000 0000 0000 0000 0101 = 5