S11-L3

OLLYDBG

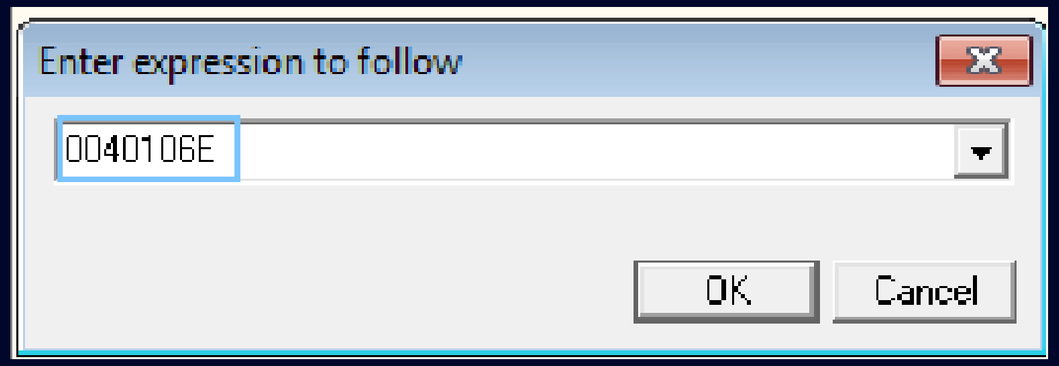
TRACCIA

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

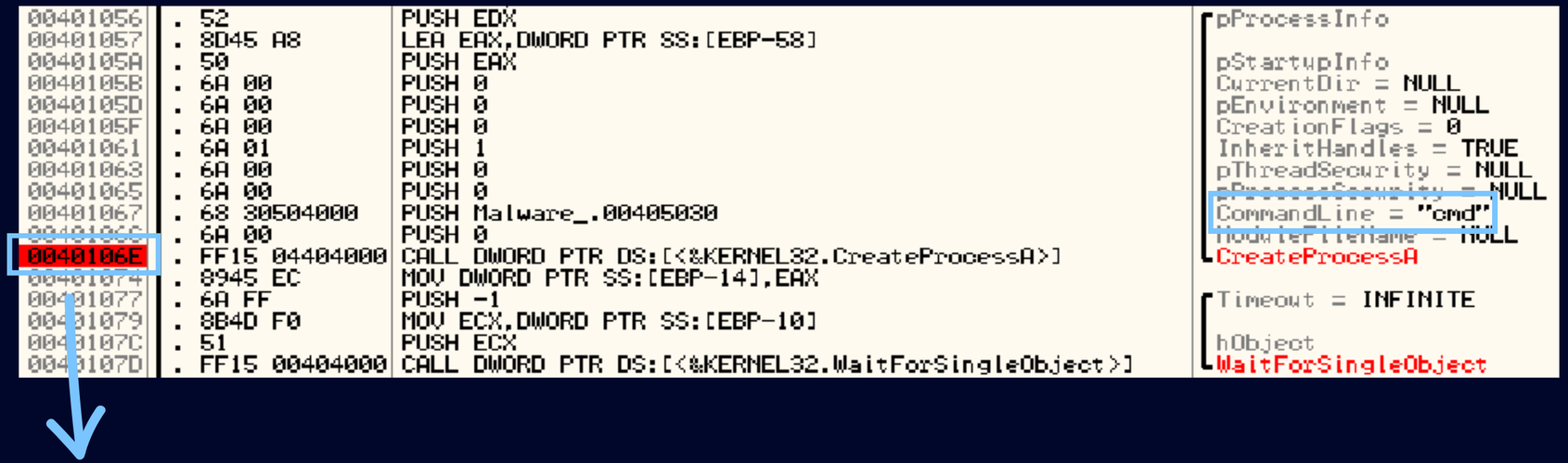
- All'indirizzo **0040106E** il Malware effettua una chiamata di funzione alla funzione «**CreateProcess**». Qual è il valore del parametro «**CommandLine**» che viene passato sullo stack? (1)
- Inserite un **breakpoint software all'indirizzo 004015A3**. Qual è il **valore del registro EDX**? (2) Eseguite 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).
- **BONUS**: spiegare a grandi linee il funzionamento del malware

02

valore del parametro «CommandLine»



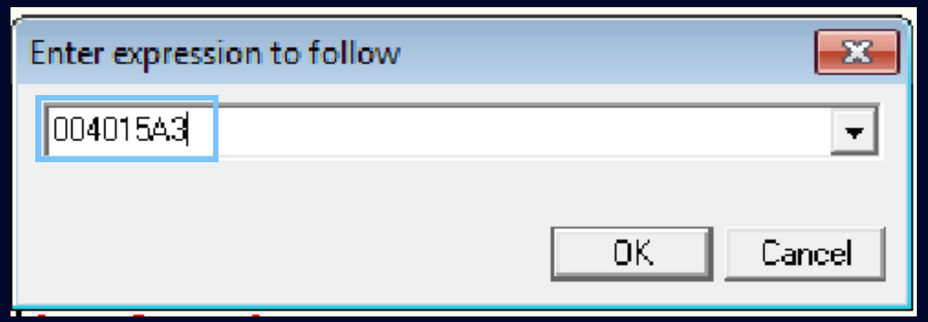
Con il comando Ctrl+g si apre questa barra di ricerca e inseriamo l'indirizzo di nostro interesse.



inseriamo qui un breakpoint e poi avviamo il programma, come si può osservare in figura poco prima della funzione CreateProcess troviamo il valore di CommandLIne che equivale a "cmd" e significa che il malware sta cercando di eseguire il programma della shell di comando di Windows (cmd.exe)

02

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




```
004015A3  . 33D2          XOR EDX,EDX
```

```
Registers (FPU)
EAX 1DB10106
ECX 7EFDE000
EDX 00001DB1
```

03

04

05

«step-into». Qual è ora il valore del registro EDX, motivando la risposta. Che istruzione è stata eseguita?

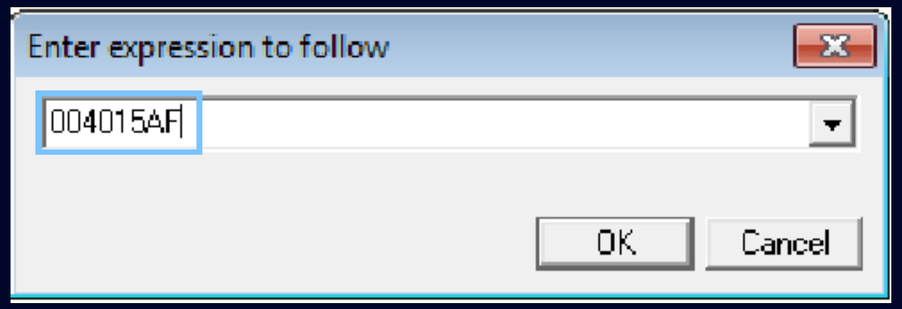
```
004015A3  . 33D2          XOR EDX,EDX
004015A5  . 8AD4          MOV DL,AH
```

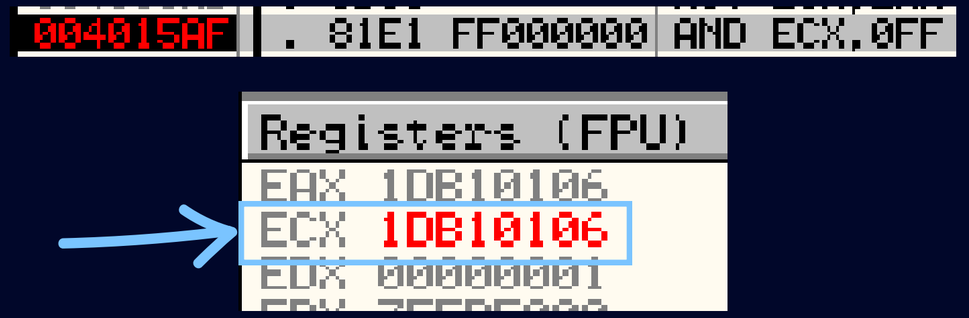
```
Registers (FPU)
EAX 1DB10106
ECX 7EFDE000
EDX 00000000
EBX 7EFDE000
```

L'istruzione che è stata eseguita è XOR EDX,EDX e il valore attuale di EDX è 0x00000000, molto probabilmente perché questa istruzione dà sempre come valore di ritorno 0.

06

breakpoint all'indirizzo 004015AF. Qual è il valore del registro ECX?





07
08

«step-into». Qual è ora il valore del registro ECX? Quale istruzione viene eseguita?

L'istruzione che è stata eseguita è AND ECX, OFF è un'operazione bitwise (bit a bit) che effettua una congiunzione logica tra il valore nel registro ECX e il valore esadecimale 0x0F. e restituisce il valore di 0x00000006.