

S11-L3

O L L Y D B G

TRACCIA

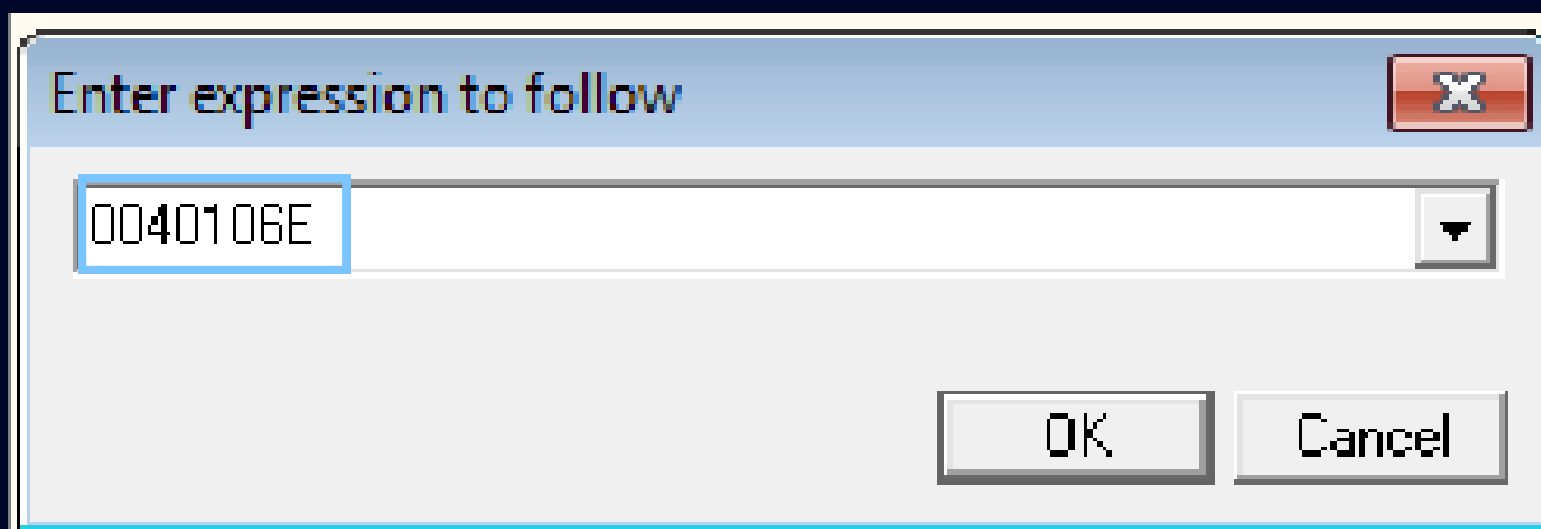
Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella sul desktop della macchina virtuale dedicata all'analisi dei malware.

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»



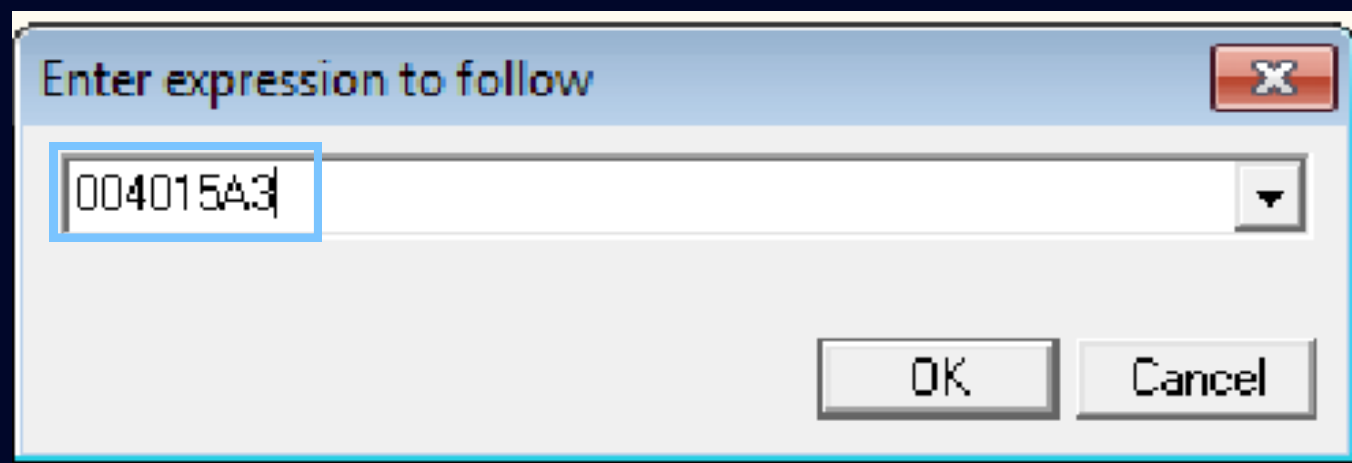
Con il comando Ctrl+g si apre questa barra di ricerca e inseriamo l'indirizzo di nostro interesse.

| | | | |
|----------|-----------------|---|-------------------------|
| 00401056 | . 52 | PUSH EDI | pProcessInfo |
| 00401057 | . 8D45 A8 | LEA EAX,DWORD PTR SS:[EBP-58] | pStartupInfo |
| 0040105A | . 50 | PUSH EAX | CurrentDir = NULL |
| 0040105B | . 6A 00 | PUSH 0 | pEnvironment = NULL |
| 0040105D | . 6A 00 | PUSH 0 | CreationFlags = 0 |
| 0040105F | . 6A 00 | PUSH 0 | InheritHandles = TRUE |
| 00401061 | . 6A 01 | PUSH 1 | pThreadSecurity = NULL |
| 00401063 | . 6A 00 | PUSH 0 | pProcessSecurity = NULL |
| 00401065 | . 6A 00 | PUSH 0 | CommandLine = "cmd" |
| 00401067 | . 68 30504000 | PUSH Malware_.00405030 | ModuleFileName = NULL |
| 00401069 | . 6A 00 | PUSH 0 | CreateProcessA |
| 0040106E | . FF15 04404000 | CALL DWORD PTR DS:[&KERNEL32.CreateProcessA] | |
| 00401074 | . 8945 EC | MOV DWORD PTR SS:[EBP-14],EAX | Timeout = INFINITE |
| 00401077 | . 6A FF | PUSH -1 | hObject |
| 00401079 | . 8B4D F0 | MOV ECX,DWORD PTR SS:[EBP-10] | WaitForSingleObject |
| 0040107C | . 51 | PUSH ECX | |
| 0040107D | . FF15 00404000 | CALL DWORD PTR DS:[&KERNEL32.WaitForSingleObject] | |

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

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

04

05

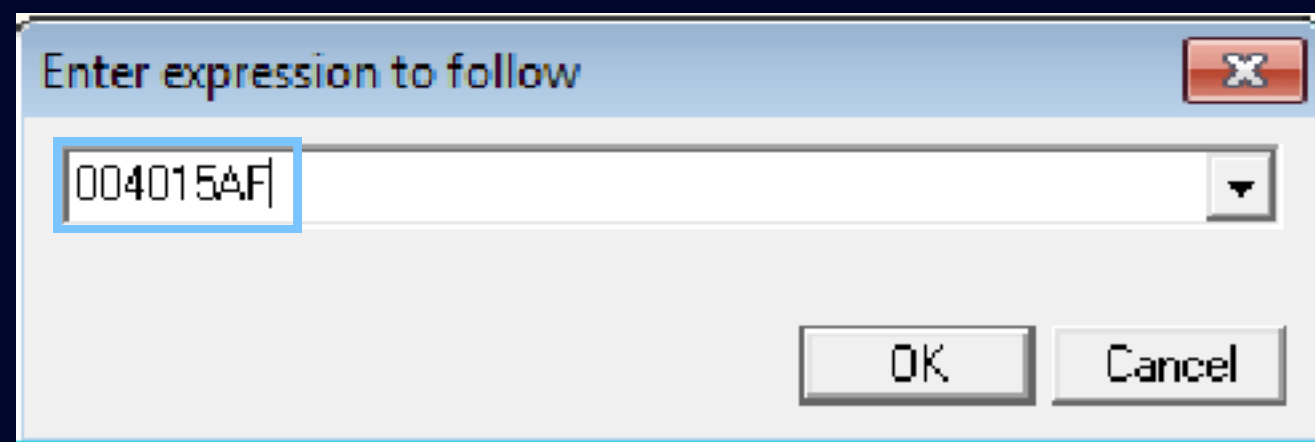
| | | |
|----------|--------|-------------|
| 004015A3 | . 33D2 | XOR EDX,EDX |
| 004015A5 | . 8AD4 | MOV DL,AH |

| Registers (FPU) | |
|-----------------|----------|
| EAX | 1DB10106 |
| ECX | 7EFDE000 |
| EDX | 00000000 |
| EBX | 7EFDE000 |
| ESP | 0010FFFF |

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?



004015AF . 81E1 FF000000 AND ECX,0FF

Registers (FPU)

EAX 1DB10106

ECX 1DB10106

EDX 00000001

EBX 77777777

07

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

08

004015AF . 81E1 FF000000 AND ECX,0FF
004015B5 . 890D 00524000 MOV DWORD PTR DS:[405200],ECX

Registers (FPU)

EAX 1DB10106

ECX 00000006

EDX 00000001

L'istruzione che è stata eseguita è AND ECX, 0FF 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.