

S11 / L3

ESERCITAZIONE

TRACCIA

01

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?

02

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

03

Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX

04

motivando la risposta

05

Che istruzione è stata eseguita?

TRACCIA

06 Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?

07 Eseguite un step-into. Qual è ora il valore di ECX?

08 Spiegate quale istruzione è stata eseguita

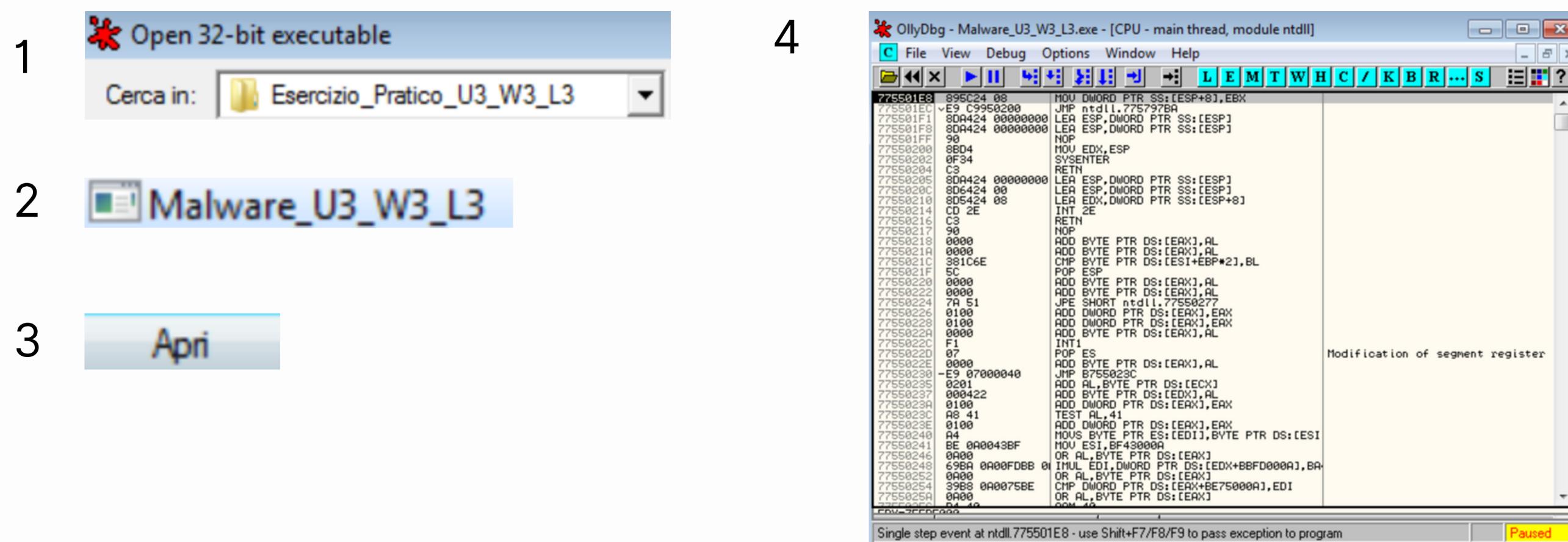
BONUS spiegare a grandi linee il funzionamento del malware

AVVIO OLLYDBG



Il software che andremo ad utilizzare è OllyDbg
un debugger a livello di codice assembly per sistemi operativi Windows. È uno strumento utilizzato principalmente da sviluppatori e ricercatori di sicurezza per eseguire il debug di programmi a livello di codice macchina.

Eseguito il tool andiamo ad aprire all'interno il malware in questione: **Malware_U3_W3_L3**



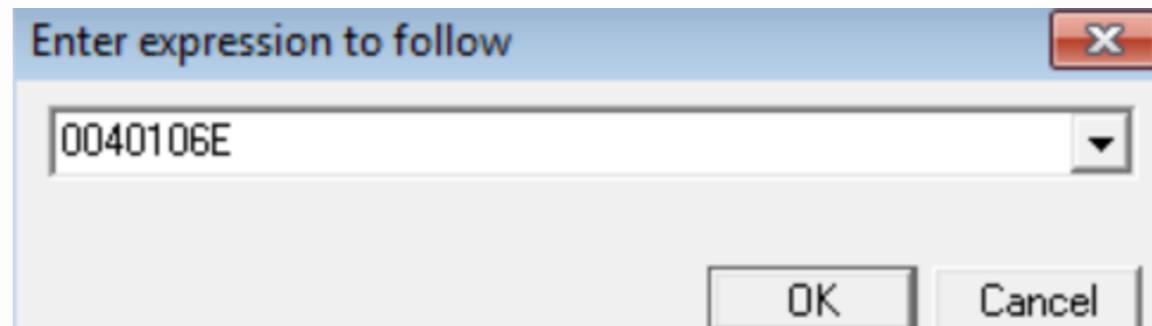
Ora
possiamo
andare ad
analizzare
il Malware

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?

Ci rechiamo in primis all'indirizzo **0040106E**

Tasto DX Go to Expression Ctrl+G

Inseriamo l'indirizzo e clicchiamo OK



OllyBgd ci porterà al'indirizzo richiesto

0040106E FF15 04404000 | CALL DWORD PTR DS:[&KERNEL32.CreateProcessW] kernel32.Creat

Inseriamo un Breakpoint con doppio click

0040106E FF15 04404000

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?

clicchiamo Play



Torniamo all'indirizzo **0410106E**

con **ctr G**

The screenshot shows assembly code for the `CreateProcessA` function. The assembly code is as follows:

```
00401056: 52          ; PUSH EDX
00401057: 8D45 A8    ; LEA EAX, DWORD PTR SS:[EBP-58]
0040105A: 50          ; PUSH EAX
0040105B: 6A 00        ; PUSH 0
0040105D: 6A 00        ; PUSH 0
0040105F: 6A 00        ; PUSH 0
00401061: 6A 01        ; PUSH 1
00401063: 6A 00        ; PUSH 0
00401065: 6A 00        ; PUSH 0
00401067: 68 30504000  ; PUSH Malware_.00405030
0040106C: 6A 00        ; PUSH 0
0040106E: FF15 04404000 ; CALL DWORD PTR DS:[&KERNEL32.CreateProcessA]
```

The parameters for the `CreateProcessA` function are listed on the right side of the debugger window:

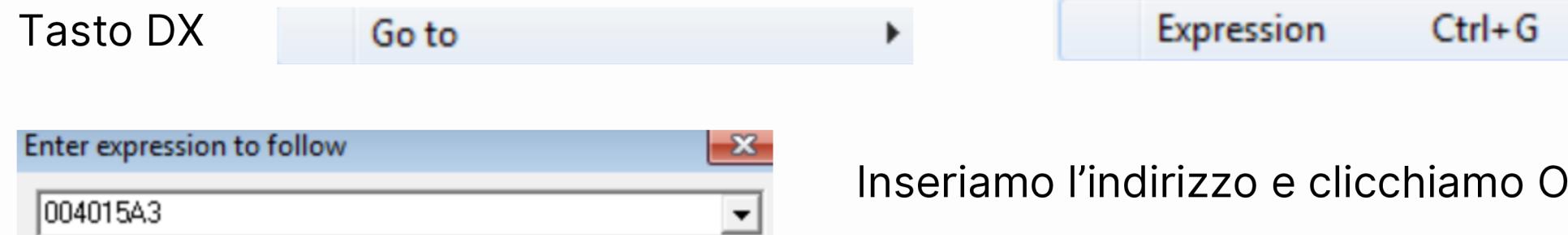
- pProcessInfo
- pStartupInfo
- CurrentDir = NULL
- pEnvironment = NULL
- CreationFlags = 0
- InheritHandles = TRUE
- pThreadSecurity = NULL
- pProcessSecurity = NULL
- CommandLine = "cmd"
- ModuleFileName = NULL

Come possiamo notare nella sezione a destra, scrollando in alto troveremo il parametro **CommandLine** con valore **cmd**

CommandLine = "cmd"

INSERITE UN BREAKPOINT SOFTWARE ALL'INDIRIZZO 004015A3. QUAL È IL VALORE DEL REGISTRO EDX?

Ci rechiamo in primis all'indirizzo **004015A3**



Inseriamo l'indirizzo e clicchiamo OK

OllyBgd ci porterà all'indirizzo richiesto

Inseriamo un Breakpoint con doppio click

004015A3 | . 33D2 | XOR EDX,EDX

Verifichiamo il valore del registro EDX nella sezione FPU situato a destra

come possiamo notare il valore di EDX è 00001DB1

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

ESEGUITE A QUESTO PUNTO UNO «STEP-INTO». INDICATE QUAL È ORA IL VALORE DEL REGISTRO EDX

004015A3 | . 33D2 XOR EDX, EDX

Eseguiamo ora **STEP-INTO** all'indirizzo **004015A3**



Ci darà **0** come valore di EDX

EDX 00000000

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

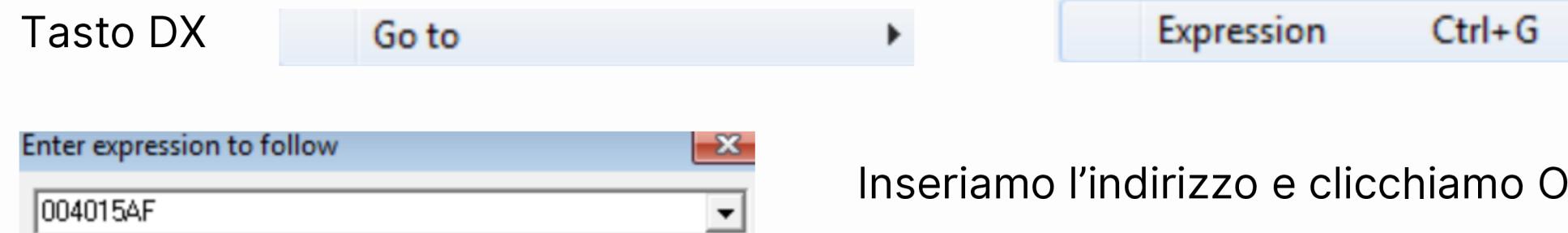
MOTIVANDO LA RISPOSTA

Istruzione: **XOR EDX, EDX**

Poiché **XOR** di un valore con sé stesso dà sempre zero, il risultato è che il registro **EDX** viene azzerato.

**INSERITE UN SECONDO BREAKPOINT ALL'INDIRIZZO DI MEMORIA 004015AF.
QUAL È IL VALORE DEL REGISTRO ECX?**

Ci rechiamo in primis all'indirizzo **004015AF**



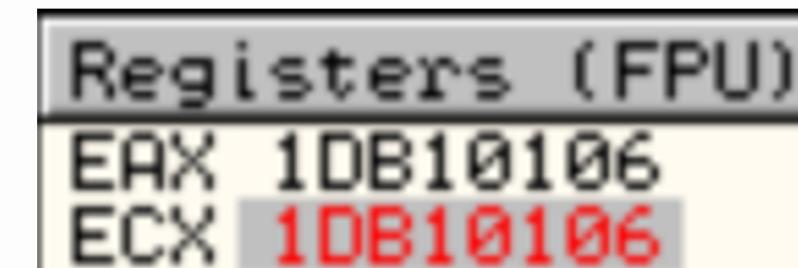
OllyBgd ci porterà all'indirizzo richiesto

Inseriamo un Breakpoint con doppio click

004015AF || . 81E1 FF000000 AND ECX.0FF

Verifichiamo il valore del registro ECX nella sezione FPU situato a destra

come possiamo notare il valore di ECX è 1DB10106



ESEGUITE UN STEP-INTO. QUAL È ORA IL VALORE DI ECX?

004015AF | . 81E1 FF000000 AND ECX, OFF

Eseguiamo ora **STEP-INTO** all'indirizzo **004015AF**



004015B5 | . 890D 00524000 MOU DWORD PTR DS:[405200], ECX

Registers (FPU)
EAX 1DB10106
ECX 00000006

Ci darà **00000006** come valore di ECX

MOTIVANDO LA RISPOSTA

L'istruzione **AND ECX, OFF** maschera il contenuto del registro ECX, mantenendo solo i bit meno significativi (gli ultimi 8 bit), mentre azzera tutti gli altri.

Il risultato finale è che solo gli ultimi 8 bit di ECX vengono mantenuti **00000006**