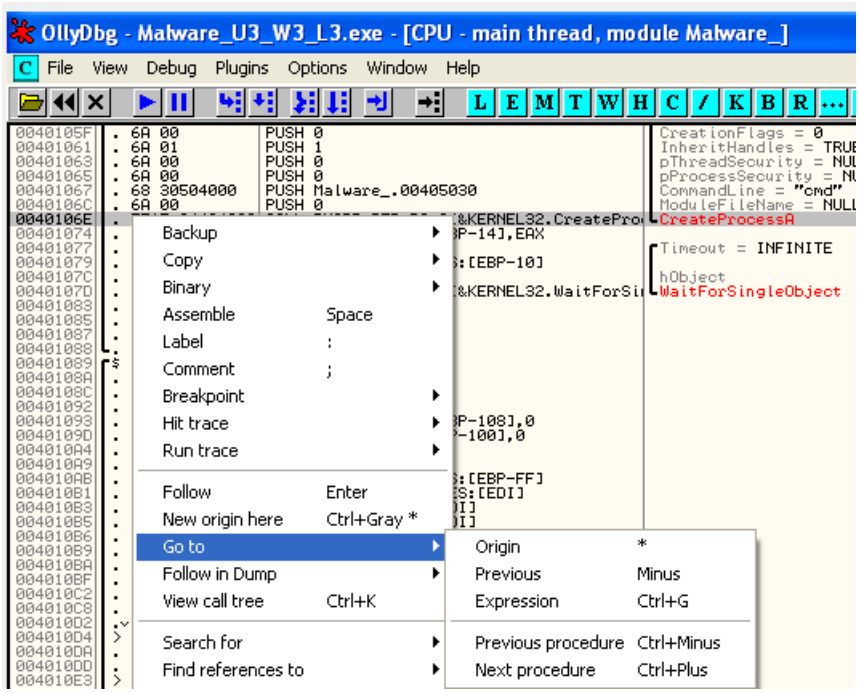
Analisi dinamica avazata con Olly DBG

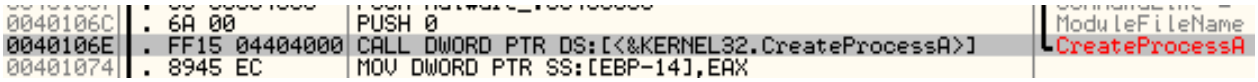
Malware_U3_W3_L3

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?

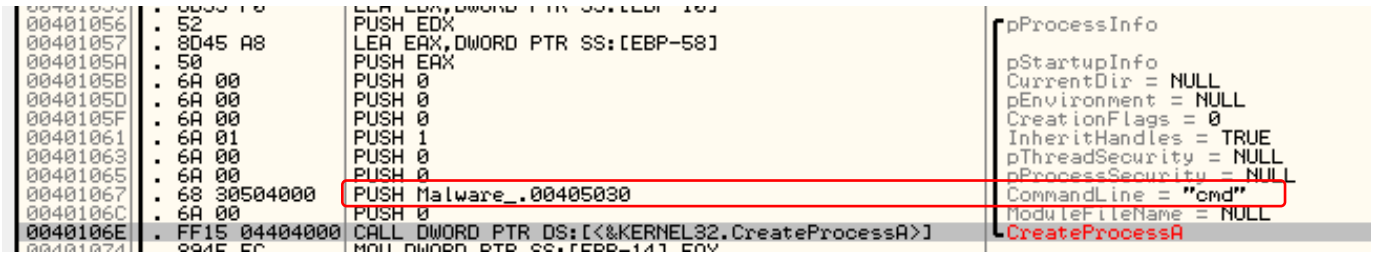
Dopo aver aperto i malware con OllyDB, cliccando col tasto destro sugli indirizzi e selezionando Go to -> Expression andiamo all'indirizzo di memoria specificato.



Vediamo che a questo indirizzo il malware effettua la chiamata alla funzione CreateProcessA

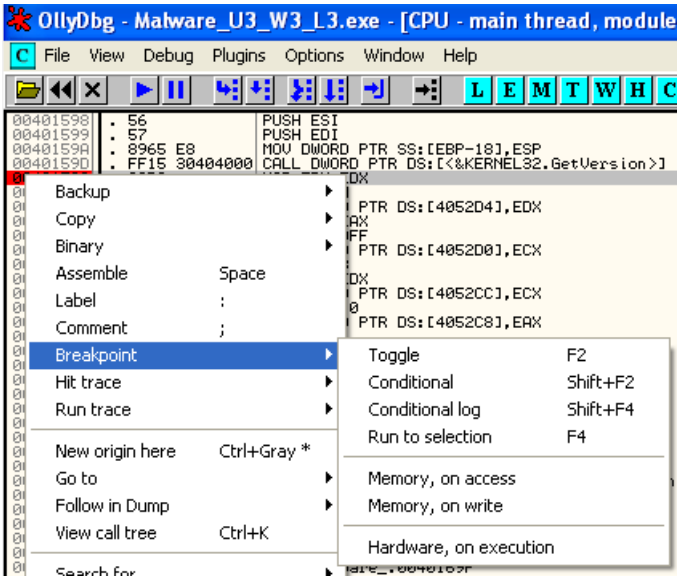


Guardando il blocco di comandi evidenziato da OllyDBG con la parentesi nera a destra, vediamo i parametri che sono passati alla funzione con le istruzioni push. Alla riga corrispondente al parametro CommandLine troviamo il valore "**cmd**", che in Assembly è passato come **Malware_.0045030**.

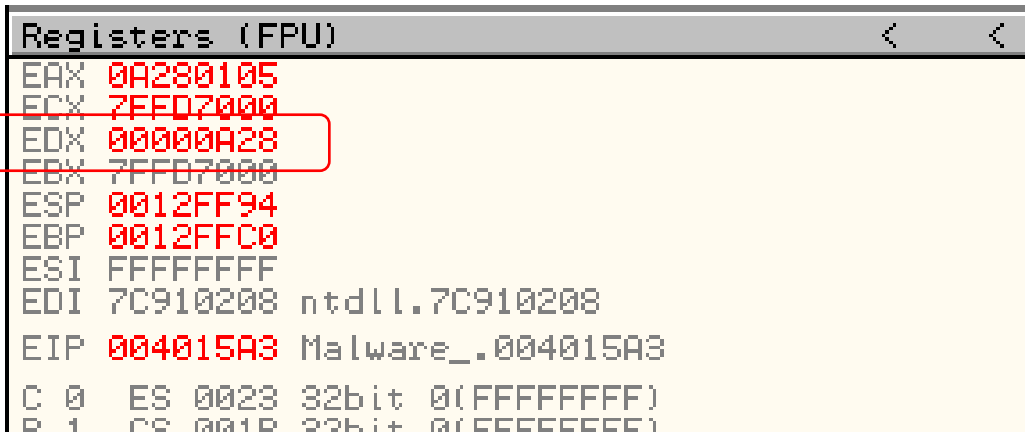


Inserire un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?

Cliccando col tasto destro sull'indirizzo 004015A3 e selezionando Breakpoint -> Toggle inseriamo un breakpoint software e vediamo che l'indirizzo si colora di rosso.



Eseguiamo il malware che si fermerà al breakpoint inserito. Dal pannello Registri sulla destra possiamo verificare che all'indirizzo 004015A3 il registro EDX ha subito una modifica (è colorato in rosso) e ha un valore di 00000A28, che è il numero 2600 in esadecimale.



Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

Clicchiamo sul pulsante  per eseguire lo step into. Veniamo indirizzati all'indirizzo 004015A5, che è l'indirizzo successivo della funzione.

```
00401598  . 56              PUSH ESI
00401599  . 57              PUSH EDI
0040159A  . 8965 E8         MOV DWORD PTR SS:[EBP-18],ESP
0040159D  . FF15 30404000   CALL DWORD PTR DS:[<&KERNEL32.GetVersio  kernel32.GetVersion
004015A3  . 33D2            XOR EDX,EDX
004015A5  . 8AD4            MOV DL,AH
004015A7  . 8915 D4524000   MOV DWORD PTR DS:[4052D4],EDX
004015AD  . 8BC8            MOV ECX,EAX
004015AF  . 81E1 FF000000   AND ECX,0FF
004015B5  . 890D D0524000   MOV DWORD PTR DS:[4052D0],ECX
```

Dal pannello Registri sulla destra possiamo verificare che il registro EDX adesso ha valore 0.

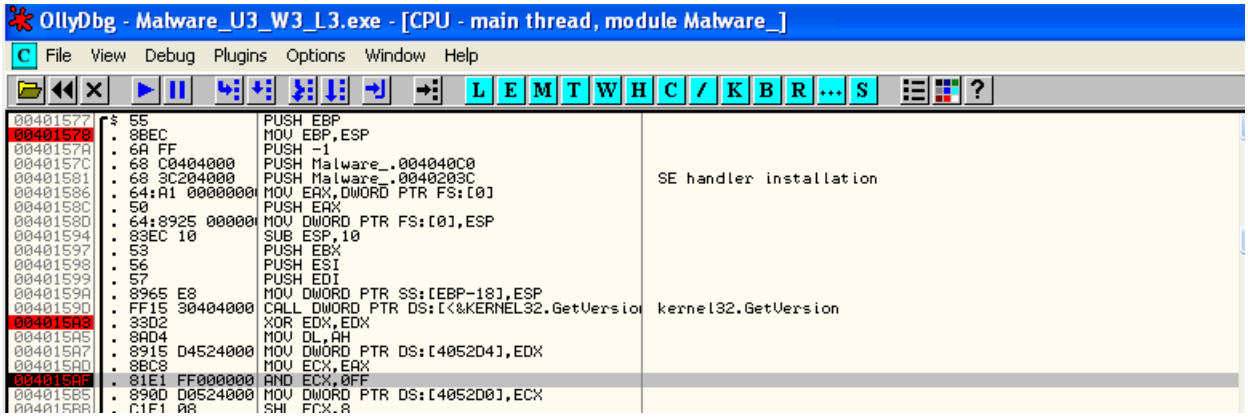
```
Registers (FPU)
EAX 0A280105
ECX 7FFDE000
EDX 00000000
EBX 7FFDE000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C910208 ntdll.7C910208

EIP 004015A5 Malware_.004015A5

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
```

L'istruzione precedente, infatti, conteneva l'operazione XOR EDX, EDX, che esegue lo XOR sul valore del registro EDX. Questa operazione ha azzerato il valore di un registro.

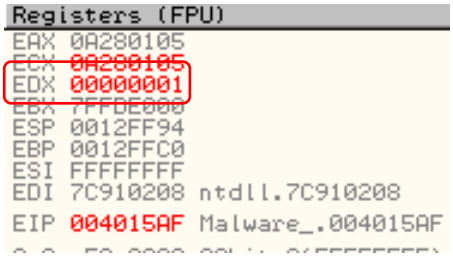
```
00401598  . 56              PUSH ESI
00401599  . 57              PUSH EDI
0040159A  . 8965 E8         MOV DWORD PTR SS:[EBP-18],ESP
0040159D  . FF15 30404000   CALL DWORD PTR DS:[<&KERNEL32.Get
004015A3  . 33D2            XOR EDX,EDX
004015A5  . 8AD4            MOV DL,AH
004015A7  . 8915 D4524000   MOV DWORD PTR DS:[4052D4],EDX
004015AD  . 8BC8            MOV ECX,EAX
004015AF  . 81E1 FF000000   AND ECX,0FF
004015B5  . 890D D0524000   MOV DWORD PTR DS:[4052D0],ECX
```

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

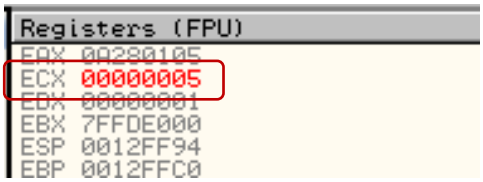
Inseriamo ora un breakpoint all'indirizzo di memoria 004015AF ed eseguiamo il malware.



Dal pannello Registri sulla destra possiamo verificare che il registro ECX ha subito una modifica (è colorato in rosso) e ha un valore di 0A280105, che corrisponde al numero 170.393.861 in esadecimale.



Clicchiamo sul pulsante  per eseguire lo step into. Veniamo indirizzati all'indirizzo 004015B5, che è l'indirizzo successivo della funzione.



L'istruzione precedente, infatti, conteneva l'operazione AND ECX, 0FF, che esegue un AND logico tra il valore di ECX (0A280105) e 0FF. Questa operazione ha impostato il registro ECX con il 0000005, il risultato dell'AND.