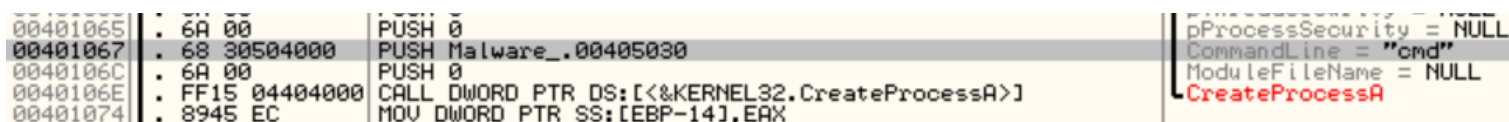


## CONSEGNA S11L3

L'obiettivo di oggi, in 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, rispondere 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

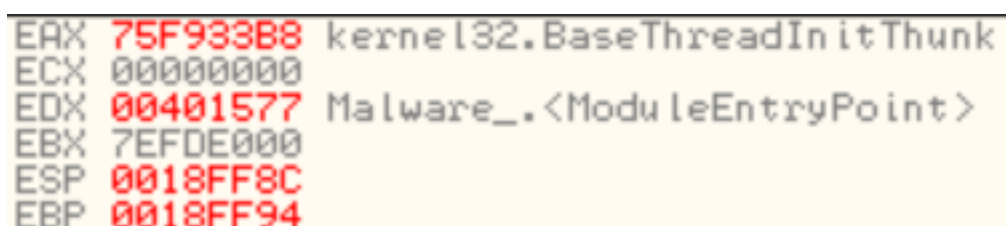
- 1) Il valore del parametro CommandLine, che viene poi passato sullo stack, è "cmd". (Fig.1)
- 2) Il valore del registro EDX è 00401577. (Fig.2)



```
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>]
00401074 . 8945 EC MOV DWORD PTR SS:[EBP-14],EAX
```

Call Stack:  
CreateProcessA  
pProcessSecurity = NULL  
CommandLine = "cmd"  
ModuleFileName = NULL

Fig.1



```
EAX 75F933B8 kernel32.BaseThreadInitThunk
ECX 00000000
EDX 00401577 Malware_.<ModuleEntryPoint>
EBX 7EFDE000
ESP 0018FF8C
EBP 0018FF94
```

Fig.2

- 3) Dopo aver eseguito lo step-into, il valore di EDX diventa 00000000. (Fig.3)



```
EAX 1DB10106
ECX 7EFDE000
EDX 00000000
EBX 7EFDE000
ESP 0018FF5C
EBP 0018FF88
ESI 00000000
EDI 00000000
```

Fig.3

- 4) Il valore cambia perché viene eseguita l'istruzione XOR EDX,EDX
- 5) Viene usato l'operatore logico XOR, che equivale ad inizializzare a zero una variabile. Infatti, dopo lo step-into, il valore del registro è 0
- 6) Il valore del registro ECX è 1DB10106



Fig.4

- 7) Dopo aver eseguito lo step-into, il valore di ECX diventa 00000006

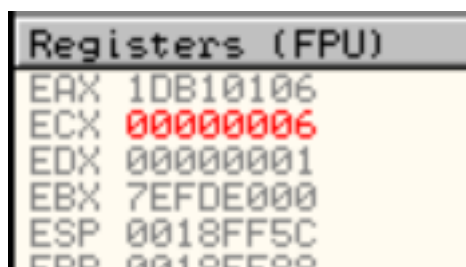


Fig.5

- 8) E' stata eseguita l'istruzione AND ECX,0FF: per eseguire questo calcolo, eseguiamo l'AND logico tra i bit di EAX (in binario) e il valore esadecimale FF (in binario).

ESADECIMALE	BINARIO
1DB10106	0001 1101 1011 0001 0000 0001 0000 0110
FF	0000 0000 0000 0000 0000 0000 1111 1111

Quindi avremo come risultato: 0000 0000 0000 0000 0000 0000 0000 0110

In esadecimale : 00000006

- 8) Risalendo all'hash tramite CFF Explorer, e caricandolo su Virus Total, sembra che questo malware sia un trojan.