

Fate 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. 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?
- 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. Che istruzione è stata eseguita?
- 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.
- BONUS: spiegare a grandi linee il funzionamento del malware

```
LEA EDX, DWORD PTR SS: [EBP-10]
. 8055 FØ
                                                                  rpProcessInfo
                  PUSH EDX
. 8D45 A8
                  LEA EAX, DWORD PTR SS: [EBP-58]
                  PUSH EAX
                  PUSH 0
                  PUSH 0
                  PUSH 0
                  PUSH
                  PUSH
. 6A
                  PUSH 0
. 68 30504000
                  PUSH Malware_.00405030
. FF15 04404000 CALL DWORD PTR DS:[<&KERNEL32.CreatePro CreatePro MOV DWORD PTR SS:[EBP-14],EAX
```

Il valore del parametro è : cmd

Il valore di EDX è: 00401577

Si esegue l'istruzione di XOR del valore di EDX, ovvero si azzera il suo valore.

Il valore di EDX è: 00000000

```
Registers (FPU)

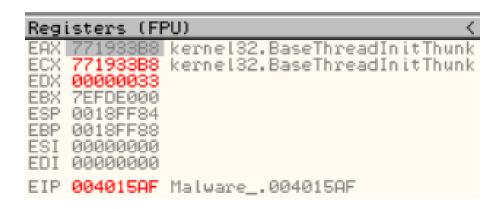
EAX 771933B8 kernel32.BaseThreadInitThunk
ECX 00000000
EDX 00401577 Malware_.<ModuleEntryPoint>
EBX 7EFDE000
ESP 0018FF84
EBP 0018FF88
ESI 00000000
EDI 00000000
```

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

Il valore di ECX è: 771933B8

Si esegue AND tra il valore di ECX ed il numero 0FF "255".

Il valore di ECX è: 000000B8



004015AF . 81E1 FF000000 AND ECX,0FF