# Progetto S11L3

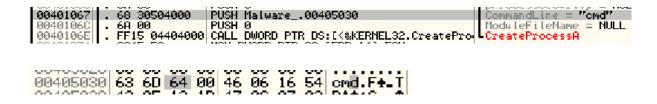
## **Alessandro Moscetti**

Dovevamo rispondere ai seguenti quesiti riguardanti il file 'Malware U3 W2 L5':

- 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

### Punto 1

Il valore di CommandLine passato alla funzione CreateProcess è il valore presente all'indirizzo di memoria **00405030**.



#### Punto 2

Inserendo il breakpoint software (tasto destro -> Toogle) all'indirizzo 004015A3 vediamo che il registro EDX ha il valore di **00000A28 (2)**.



Eseguendo uno 'step-into' vediamo che il valore del registro EDX viene azzerato (3) questo succede per l'istruzione presente alla locazione 004015A3 ossia **XOR EDX**, **EDX** (5), questa istruzione è comunemente usata per azzerare il contenuto dei registri confrontandoli agli stessi perchè confronta tutti i bit presenti dando risultato 0 (quando sono uguali) o 1 (quando sono differenti).



#### Punto 3

Inserendo il breakpoint software (tasto destro -> Toogle) all'indirizzo 004015AF vediamo che il registro ECX ha il valore di **0A280105 (6)**.

```
0040150F . 81E1 FF000000 AND ECX,0FF ECX 0A280105
```

Eseguendo uno 'step-into' vediamo che il valore del registro EDX ha il valore di 00000005 (7) questo succede per l'istruzione AND ECX, 0FF (8), questa istruzione confronta i bit contenuti in ECX con il valore 0FF, azzerando i bit disuguali. In questo caso, vengono mantenuti solo gli ultimi 8 bit di ECX, mentre gli altri bit vengono azzerati..



## **Bonus**

Analizzando alcune funzioni richiamate dal file tramite IdaPro, ho notato che il malware crea, si connette e chiude un socket.

Confrontando l'hash su VirusTotal, il file viene etichettato come un trojan.

Potremmo ipotizzare che si tratti di una backdoor.

