S11L3

Traccia: 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? (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).

```
pStartupInfo
CurrentDir = NULL
pEnvironment = NULL
CreationFlags = 0
                                            PUSH EAX
PUSH 0
PUSH 0
PUSH 0
                    6A
6A
6A
6A
6A
6A
                         00
00
0040105F
                         91
99
99
39594999
99
                                            PUSH 1
PUSH 0
PUSH 0
PUSH Malware_.00405030
0040106
                                                                                                                                             = TRUE
= NULL
00401063
                                                                                                                      ThreadSecurity
00401065
00401067
                                                                                                                                                   NULL
                                                                                                                                            "emd"
                                                                                                                                             = NULL
                                             PUSH 0
                    FF15 04404000 CALL DWORD PTR DS:[<&KERNEL32.CreatePro
```

Il valore è "cmd" (1)



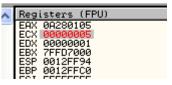
valore al breakpoint (2)



Eseguendo uno step into il valore è 00000000 per lo XOR effettuato all'interno dell'istruzione (3,4,5)

```
Registers (FPU)
EAX 0A280105
ECX 0A280105
EDX 00000001
EBX 7FFD7000
ESP 0012FF94
EBP 0012FF06
ESI FFFFFFF
EDI 7C910208 ntdll.7C910208
```

valore al breakpoint (6)



effettuando lo step into il valore cambia a 00000005 per via dell'operatore AND effettuato all'interno dell'istruzione.(7,8)