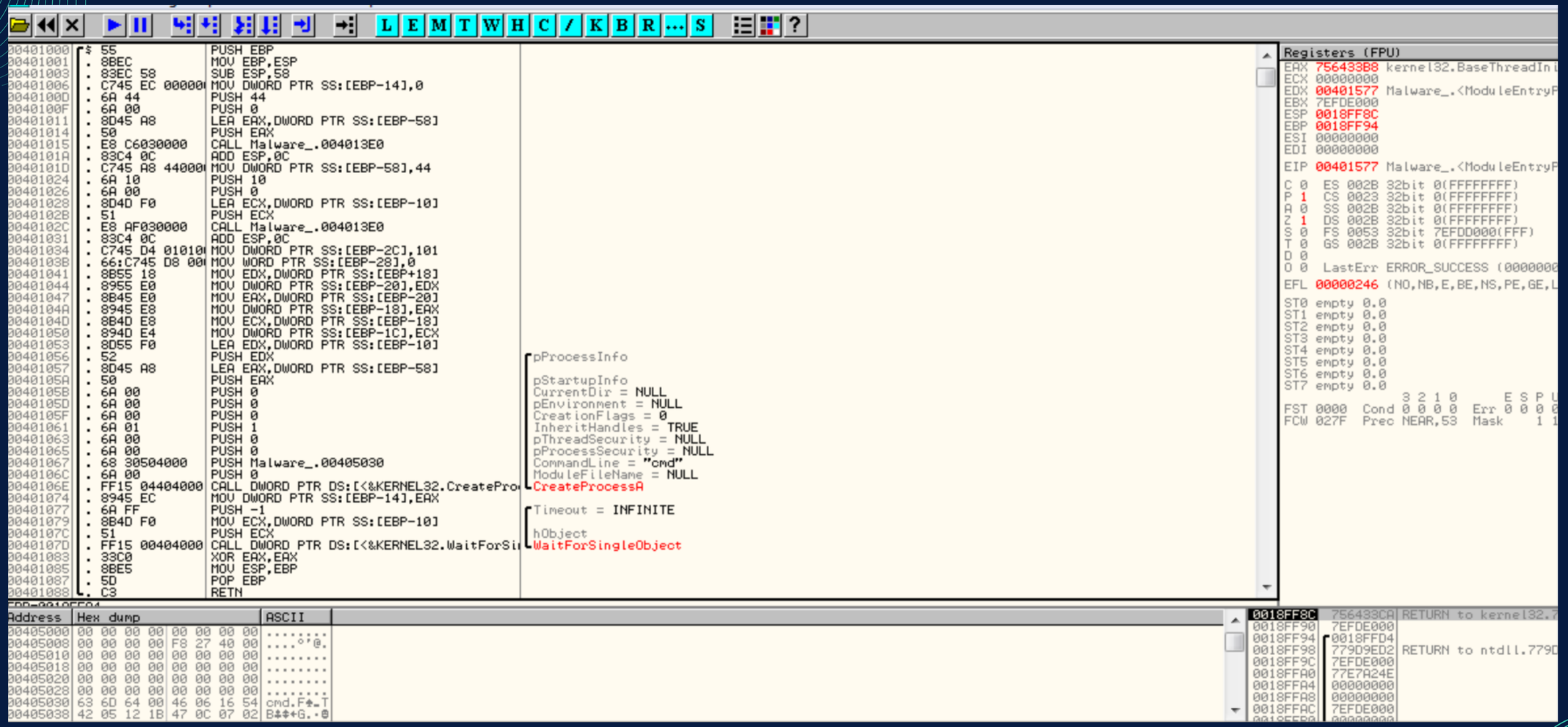
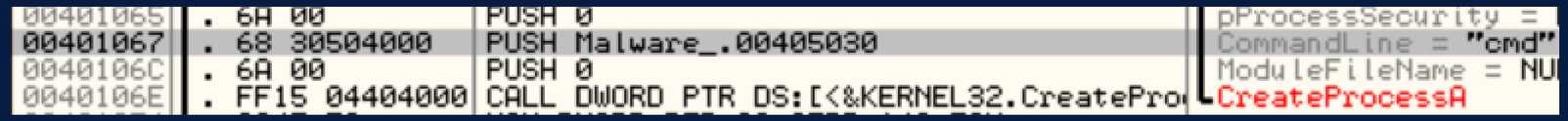
Traccia: Fate riferimento al malware: Malware_U3_W3_L3, presente all’interno della cartella Esercizio_Pratico_U3_W3_L3sul desktop della macchina virtuale dedicata all’analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG. • All’indirizzo 0040106E il Malwareeffettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?
(1) • Inserite un breakpointsoftware 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 breakpointall’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

INTERFACCIA



valore del parametro «CommandLine» che viene passato sullo stack



```
0040159D  . FF15 30404000  CALL DWORD PTR D
004015A3  . 33D2           XOR EDX,EDX
004015A5  . 8AD4           MOV DL,AH
```

1) breakpointsoftware all'indirizzo 004015A3

```
EAX 1DB10106
ECX 7EFDE000
EDX 00001DB1
EBX 7EFDE000
```

valore registro EDX

Step-into: è la tecnica di debugging che, a fronte di una chiamata di funzione, ci permette di entrare nel codice della funzione, ovvero dove essa è implementata.

Istruzione eseguita: XOR, EDX, EDX, che inizializza a zero una variabile, mi aspetto che il nuovo valore del registro EDX sia 0.

2) Eseguo «step-into»

```
00401599  . 57             PUSH EDI
0040159A  . 8965 E8        MOV DWORD PTR SS:[EBP-18],ESP
0040159D  . FF15 30404000  CALL DWORD PTR DS:[<&KERNEL32.GetVersio  kernel32.
004015A3  . 33D2           XOR EDX,EDX
004015A5  . 8AD4           MOV DL,AH
004015A7  . 8915 D4524000  MOV DWORD PTR DS:[4052D4],EDX
```

```
EAX 1DB10106
ECX 7EFDE000
EDX 00000000
EBX 7EFDE000
```

Nuovo valore registro EDX

```
004015AD  .  8BC8            MOV ECX,EAX
004015AF  .  81E1 FF000000   AND ECX,0FF
004015B5  .  890D D0524000   MOV DWORD PTR DS:[4052D0],EC
```

1) breakpointsoftware all'indirizzo 004015AF

```
ECX 1DB10106
EDX 00000001
EBX 7EFDE000
```

valore registro ECX

2) Eseguo «step-into»

```
004015AF  .  81E1 FF000000   AND ECX,0FF
004015B5  .  890D D0524000   MOV DWORD PTR DS:[4052D0],ECX
004015BB     C1E1 08         SHL ECX,8
```

Istruzione eseguita: END ECX,OFF

```
ECX 00000006
EDX 00000001
```

Nuovo valore registro ECX

MALWARE

Secondo analisi il malware risulta un trojan