

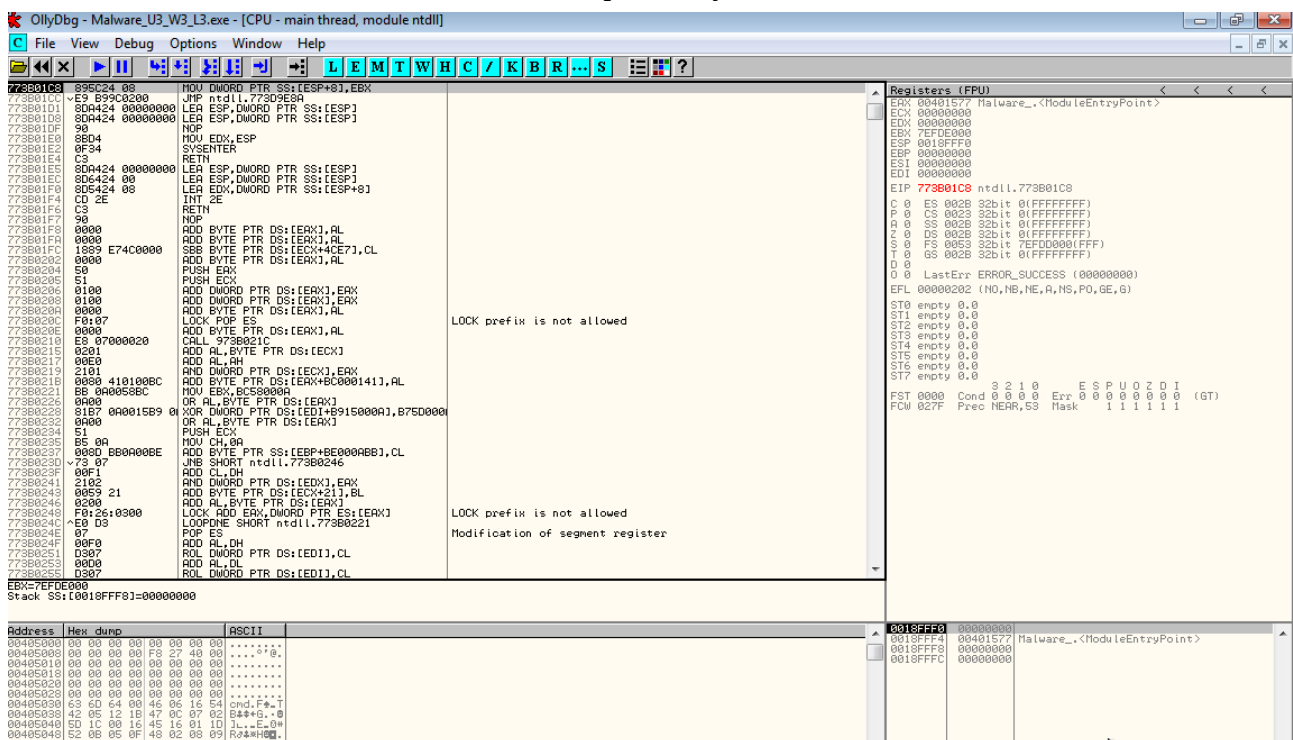
Amarfii Adrian 18/01/2023
Report
Task

Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella

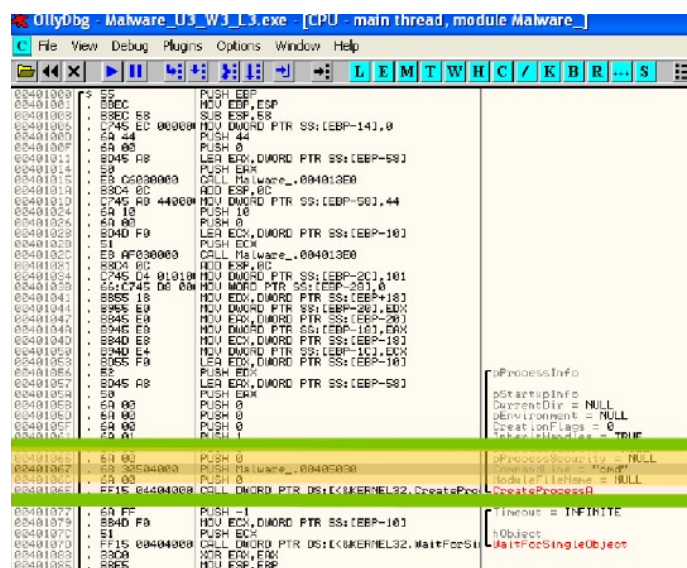
Esercizio_Pratico_U3_W3_L3 sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX 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.

Andiamo sulla nostra machina e andiamo ad aprire OllyDBG e selezioniamo il file richiesto.



Andiamo all'indirizzo che ci da la traccia 0040106E e notiamo che nel Command Line viene fatto un push e il valore è Malware_00405030.



Andiamo all'indirizzo 004015A3 e mettiamo un breakpoint e vediamo il comportamento del registro EDX prima e dopo .Prima il valore di EDX è uguale a 00000A28. Dopo aver fatto un step into notiamo che il registro EDX viene inizializzato a 0.

```
Registers (FPU)
EAX: 0A280105
ECX: 00000000
EDX: 00000A28
ESP: 0012FF94
EBP: 0012FFC0
ESI: FFFFFFFF
EDI: 7C910208 ntdll.7C910208
EIP: 004015A3 Malware_.004015A3
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr: ERROR_INVALID_HANDLE (00000006)
EFL: 00000206 (NO, NB, NE, A, NS, PE, GE, G)
ST0 empty -UNORM BCBC 01050104 005C0030
ST1 empty +UNORM 0069 006E0069 002E0067
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FST: 0000 Cond: 0 0 0 0 Err: 0 0 0 0 0 0 0 0 (GT)
FCW: 627F Prec: NEAR, 53 Mask: 1 1 1 1 1 1 1 1
```

Come abbiamo fatto sopra andiamo all'indirizzo 004015AF e facciamo lo stesso procedimento che abbiamo fatto sopra .Inizialmente il valore del registro ECX è 0A280105 dopo il step-into il valore cambia in 00000005 .Viene prima processato l'operatore logico AND che prende i valori ECX e off.AND nasconde alcuni bit di un determinato dato e azzerà questo a 0 che corrispondono a un dato valore .

```
Registers (FPU)
EAX: 0A280105
ECX: 00000005
EDX: 00000000
EBX: 7FFDF000
ESP: 0012FF94
EBP: 0012FFC0
ESI: FFFFFFFF
EDI: 7C910208 ntdll.7C910208
EIP: 004015B5 Malware_.004015B5
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr: ERROR_INVALID_HANDLE (00000006)
EFL: 00000206 (NO, NB, NE, A, NS, PE, GE, G)
ST0 empty -UNORM BCBC 01050104 005C0030
ST1 empty +UNORM 0069 006E0069 002E0067
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FST: 0000 Cond: 0 0 0 0 Err: 0 0 0 0 0 0 0 0 (GT)
FCW: 627F Prec: NEAR, 53 Mask: 1 1 1 1 1 1 1 1
```