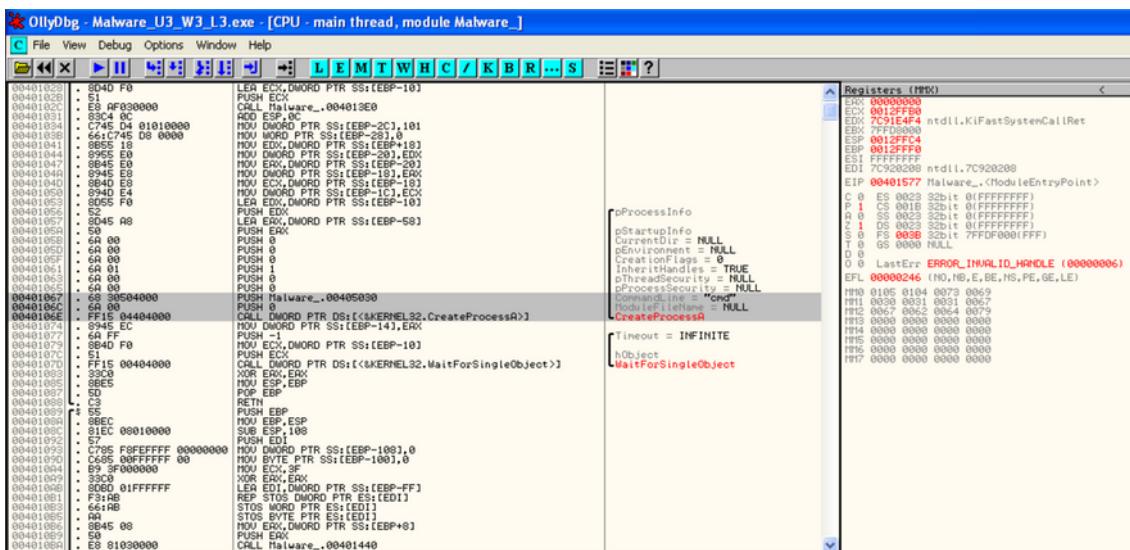


Esercizio S11L3

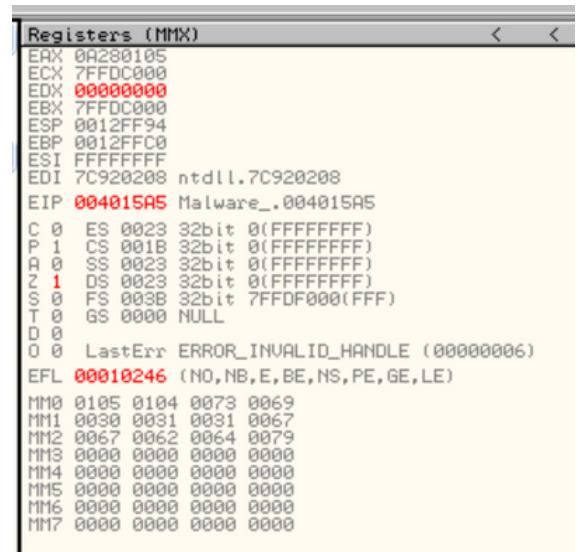
Traccia:

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).
 - BONUS: spiegare a grandi linee il funzionamento del malware



il valore è 0 perchè vi è l'istruzione logica xor che Inizializza a 0 il registro EAX. L'operatore logico tra due bit identici restituisce sempre 0 invece tra due bit diversi restituisce sempre 1.



Registers (MMX)

EAX 0A280105
 ECX 00000001
 EDX 00000001
 EBX 7FFDC000
 ECSP 00000004
 EBP 0012FFC0
 ESI FFFFFFFF
 EDI 7C920208 ntdll.7C920208
 EIP 004015AF Malware_.004015AF
 C 0 ES 0023 32bit 0(FFFFFFF)
 P 1 CS 001B 32bit 0(FFFFFFF)
 A 0 SS 0023 32bit 0(FFFFFFF)
 Z 1 DS 0023 32bit 0(FFFFFFF)
 S 0 FS 003B 32bit 7FFDF000(F)
 G 0 GS 0000 NULL
 D 0
 O 0 LastErr ERROR_INVALID_HANDLE (00000006)
 EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

SE handler installation

kernel32.GetVersion

```

00401568: .v74 04 JE SHORT Malware_.00401571
0040156D: .33C0 XOR EAX,EAX
0040156E: .EB 02 JMP SHORT Malware_.00401573
0040156F: .C7 00 MOV EAX,EDI
00401570: .C3 CLD
00401571: .5F POP EDI
00401572: .C9 LEAVE
00401573: .C3 RETN
00401574: .5F PUSH EBP
00401575: .C9 MOV EBP,ESP
00401576: .5F PUSH -1
00401577: .5F PUSH Malware_.00404000
00401578: .6A FF PUSH Malware_.0040203C
00401579: .64A1 00000000 MOV EDX,0MDOR PTR FS:[0]
0040157A: .C3 C3 PUSH EBP
0040157B: .648925 00000000 MOV EDOR PTR FS:[0],ESP
0040157C: .83EC 10 SUB ESP,10
0040157D: .53 PUSH EBX
0040157E: .55 PUSH ESI
0040157F: .55 PUSH ECX
00401580: .5965 E8 MOV EDOR PTR SS:[EBP-18],ESP
00401581: .FF15 30404000 CALL EDOR PTR DS:[<KERNEL32.GetVersion>]
00401582: .8A04 XOR EDX,EDX
00401583: .33D2 MOV DL,AL
00401584: .8915 D4524000 MOV EDOR PTR DS:[4052D4],EDX
00401585: .8918 FF000000 AND EDX,0FF
00401586: .8900 D0524000 MOV EDOR PTR DS:[4052D0],ECX
00401587: .C1E1 08 SHL ECX,8
00401588: .03CA ADD ECX,EDX
00401589: .8960 CC524000 MOV EDOR PTR DS:[4052CC],ECX

```

Restituisce l'AND logico tra i bit di EAX e la forma binaria del numero 0FF(decimal=255 e in binario=11111111).

Aggiorna poi EAX con il risultato dell'operazione

Registers (MMX)

EAX 0A280105
 ECX 00000005
 EDX 00000001
 EBX 7FFDC000
 ESP 0012FF94
 EBP 0012FFC0
 ESI FFFFFFFF
 EDI 7C920208 ntdll.7C920208
 EIP 004015B5 Malware_.004015B5

C 0 ES 0023 32bit 0(FFFFFFF)
 P 1 CS 001B 32bit 0(FFFFFFF)
 A 0 SS 0023 32bit 0(FFFFFFF)
 Z 0 DS 0023 32bit 0(FFFFFFF)
 S 0 FS 003B 32bit 7FFDF000(F)
 T 0 GS 0000 NULL
 D 0
 O 0 LastErr ERROR_INVALID_HANDLE (00000006)
 EFL 00010206 (NO,NB,NE,A,NS,PE,GE,G)

MM0 0105 0104 0073 0069
 MM1 0030 0031 0031 0067
 MM2 0067 0062 0064 0079
 MM3 0000 0000 0000 0000
 MM4 0000 0000 0000 0000
 MM5 0000 0000 0000 0000
 MM6 0000 0000 0000 0000
 MM7 0000 0000 0000 0000

ASCII del malware ottenuta con il tool md5deep-4.3:

251f4d0caf6eadae453488f9c9c0ea95

44 security vendors and no sandboxes flagged this file as malicious

File: Malware_U3_W2_15.exe

Module Name Imports OFTs TimeStamp ForwarderChain Name RVA FTs (IAT)

KERNEL32.dll 44 00006518 00000000 00000000 000065EC 00006000

WININET.dll 5 000065CC 00000000 00000000 00006664 000060B4

Do you want to automate checks?

File: Malware_U3_W2_15.exe

Module Name Imports OFTs TimeStamp ForwarderChain Name RVA FTs (IAT)

KERNEL32.dll 44 00006518 00000000 00000000 000065EC 00006000

WININET.dll 5 000065CC 00000000 00000000 00006664 000060B4

Module Name Imports OFTs TimeStamp ForwarderChain Name RVA FTs (IAT)

KERNEL32.dll 44 00006518 00000000 00000000 000065EC 00006000

WININET.dll 5 000065CC 00000000 00000000 00006664 000060B4

Secondo virustotal sembra che il malware sia un trojan che si presenta come un'applicazione legittima o un file affidabile, ma che in realtà nasconde funzionalità dannose.

Con l'aiuto del tool CFF Explorer potrebbe confermare che sia un trojan dato che tra le funzioni della libreria Kernel32.dll vi sono scritte delle azioni riguardanti a un file eseguito in tempo reale dedotto dalla funzione Heap

Heap: viene utilizzato per l'allocazione di memoria dinamicamente durante l'esecuzione di un programma