S11/L2

Analisi Statica con IDA Pro

Stefano Di Prospero

Traccia:

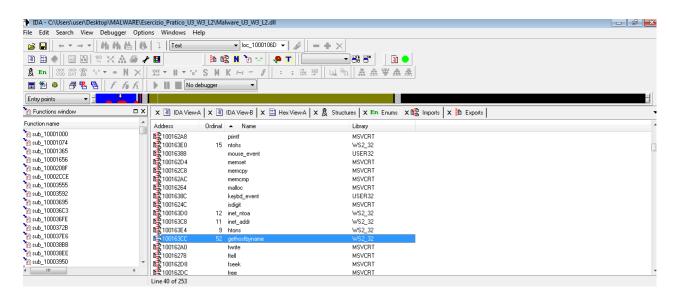
Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica. A tal proposito, con riferimento al malware chiamato «Malware_U3_W3_L2» presente all'interno della cartella «Esercizio_Pratico_U3_W3_L2» sul Desktop della macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.

- 1. Individuare l'indirizzo della funzione DLLMain(così com'è, in esadecimale)
- 2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?
 - 3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?
 - 4. Quanti sono, invece, i parametri della funzione sopra?
- 5. Inserire altre considerazioni macro livello sul malware (comportamento)

1)

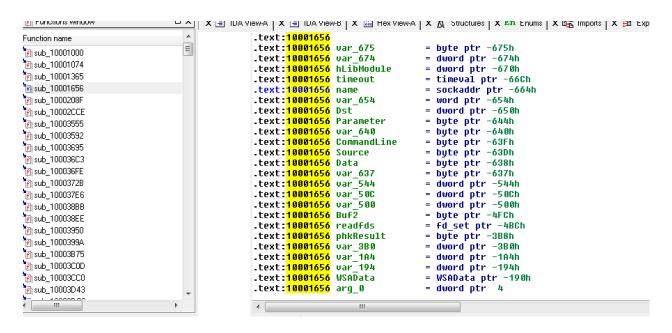
```
er\Desktop\MALWARE\Esercizio Pratico U3 W3 L2\Malware U3 W3 L2.dll
        Jump Search View Debugger Options Windows Help
                                                       ▼ loc_1000106D ▼ | 🔗 | 💻 🛊
                                                         0101 0101 0101 0101 "s" - * N × | 0ff - # - 'x' S M K /-/
                                        No debugger
                                         x 🖹 IDA View-A | x 🖺 IDA View-B | x 🕮 Hex View-A | x 🤼 Structures | x En. Enums | x 🛍 Imports | x 🏚 Exports |
nction name
                                                     .text:1000D02B ServiceMain
.text:1000D02B
hsub 10001000
                                                     .text:1000D02E
|sub_10001000
|sub_10001074
|sub_10001365
|sub_10001656
                                                     .text:1000D02E ; ------ S U B R O U T I N E -----
                                                     .text:1000D02E
.text:1000D02E
                                                     .text:1000002E; B00L _std.
.text:1000002E; B00L _std.
.text:1000002E _011Main@12
.text:1000002E
.text:1000002E hinstDLL
.text:1000002E fdwReason
.text:1000002E fdwReason
.text:1000002E
                                                                        sub_1000208F
sub_10002CCE
sub 10003555
sub_10003592
sub_10003695
sub 100036C3
sub_100036FE
sub_1000372B
                                                                                                        eax, [esp+fdwReason]
                                                     .text:1000D02E
sub 100037E6
                                                      text:1000D032
                                                                                                        eax
loc_1000D107
 sub_100038BB
sub_100038EE
                                                     .text:1000D033
                                                                                                         eax, [esp+hinstDLL]
                                                     .text:1000D039
```

2)

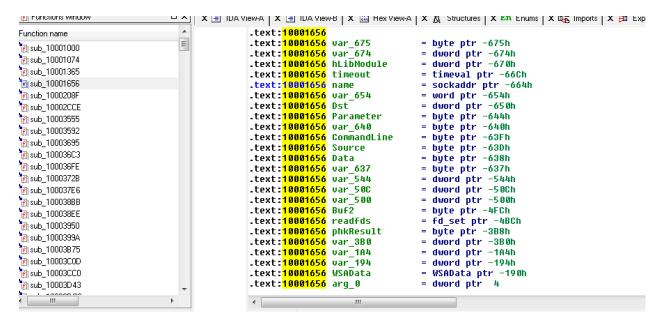


L'Indirizzo della funzione *"gethostbyname"* è 100163CC. Questa funzione si occupa di recuperare l'indirizzo IP associato ad un nome host.

3)



Nell'indirizzo 10001656 si contano, come da figura, 23 variabili. Queste variabili hanno un offset negativo.



L'unico parametro constante risulta l'unico con offset positivo, ovvero "arg_0".

5) Dalle funzioni richiamate e dall'analisi dell'hash il malware sembra essere una backdoor.