ESERCIZIO S11-L2

Lo scopo dell'esercizio di oggi è quello di familiarizzare con IDA pro. In riferimento al "Malware_U3_W3_L2" dobbiamo rispondere ai seguenti quesiti:

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

1. L'indirizzo della funzione DLLMain è 1000D02E.

```
.text:1000D02E
.text:1000D02E ; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpvReserved)
.text:1000D02E _DllMain@12     proc near               ; CODE XREF: DllEntryPoint+4B↓p
.text:1000D02E                                         ; DATA XREF: sub_100110FF+2D↓o
.text:1000D02E
.text:1000D02E hinstDLL        = dword ptr  4
.text:1000D02E fdwReason       = dword ptr  8
.text:1000D02E lpvReserved     = dword ptr  0Ch
.text:1000D02E
.text:1000D02E                 mov     eax, [esp+fdwReason]
.text:1000D032                 dec     eax
.text:1000D033                 jnz     loc_1000D107
.text:1000D039                 mov     eax, [esp+hinstDLL]
```

2. La funzione "gethostbyname" è una funzione che converte un nome di dominio in un indirizzo IP associato. In questo caso l'indirizzo dell'import è 100163CC.

3. Le variabili locali della funzione alla locazione di memoria 0x10001656 sono 20.

```
var_675= byte ptr -675h
var_674= dword ptr -674h
hModule= dword ptr -670h
timeout= timeval ptr -66Ch
name= sockaddr ptr -664h
var_654= word ptr -654h
in= in_addr ptr -650h
Parameter= byte ptr -644h
CommandLine= byte ptr -63Fh
Data= byte ptr -638h
var_544= dword ptr -544h
var_50C= dword ptr -50Ch
var_500= dword ptr -500h
var_4FC= dword ptr -4FCh
readfds= fd_set ptr -4BCh
phkResult= HKEY__ ptr -3B8h
var_3B0= dword ptr -3B0h
var_1A4= dword ptr -1A4h
var_194= dword ptr -194h
WSAData= WSAData ptr -190h
```

4. Di parametri invece ce n'è soltanto uno perché ha offset positivo ed è la seguente:

```
arg_0= dword ptr  4
```

5. Per capire meglio di che tipo di malware si tratta, dobbiamo guardare altre parti di codice e infatti vediamo che questo malware permette di creare cartelle, copiarle, cancellarle ecc…ma soprattutto all'indirizzo 10093D74 c'è scritto proprio backdoor server, quindi è chiaro che si tratti di una backdoor la quale permette di prendere il controllo del dispositivo.

```
xdoors_d:10093D73                 align 4
xdoors_d:10093D74 ; char aBackdoorServer[]
xdoors_d:10093D74 aBackdoorServer db 0Dh,0Ah              ; DATA XREF: sub_100042DB+B5↑o
                  Flow
xdoors_d:10093D74                 db 0Dh,0Ah
xdoors_d:10093D74                 db '*****************************',0Dh,0Ah
xdoors_d:10093D74                 db '[BackDoor Server Update Setup]',0Dh,0Ah
xdoors_d:10093D74                 db '*****************************',0Dh,0Ah
```