Epicode
CS-0124
Pratica S11/L2

Francesco Ficetti

1. Traccia

Lo scopo dell’esercizio è di acquisire esperienza con IDA.
Con riferimento al malware allegato, rispondere ai seguenti quesiti:

1. Individuare l'indirizzo della funzione DLLMain (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 e i parametri della funzione alla locazione di memoria 0x10001656?
4. Inserire altre considerazioni macro livello sul malware.

2. Svolgimento

2.1 Indirizzo DDLMain

L'indirizzo della funzione DLLMain è *1000D02E*, come si vede nella figura seguente.

```
.text:1000D02E
.text:1000D02E ; ============== S U B R O U T I N E =======================================
.text: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
```

2.2 Funzione gethostbyname

La funzione *gethosbyname* si trova all'indirizzo *100163CC*. Questa funzione recupera le informazioni host corrispondenti a un nome host da un database host. Se va a buon fine, restituisce un puntatore alla struttura hostent, altrimenti restituisce un puntatore *Null*.

```
.idata:100163CC ; struct hostent *__stdcall gethostbyname(const char *name)
.idata:100163CC                 extrn gethostbyname:dword
.idata:100163CC                                        ; CODE XREF: sub_10001074:loc_100011AF↑p
.idata:100163CC                                        ; sub_10001074+1D3↑p ...
```

2.3 Variabili locali e parametri

```
.text:10001656 ; ============== S U B R O U T I N E =======================================
.text:10001656
.text:10001656
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656    proc near               ; DATA XREF: DllMain(x,x,x)+C8↓o
.text:10001656
.text:10001656 var_675         = byte ptr -675h
.text:10001656 var_674         = dword ptr -674h
.text:10001656 hLibModule      = dword ptr -670h
.text:10001656 timeout         = timeval ptr -66Ch
.text:10001656 name            = sockaddr ptr -664h
.text:10001656 var_654         = word ptr -654h
.text:10001656 Dst             = dword ptr -650h
.text:10001656 Parameter       = byte ptr -644h
.text:10001656 var_640         = byte ptr -640h
.text:10001656 CommandLine     = byte ptr -63Fh
.text:10001656 Source          = byte ptr -63Dh
.text:10001656 Data            = byte ptr -638h
.text:10001656 var_637         = byte ptr -637h
.text:10001656 var_544         = dword ptr -544h
.text:10001656 var_50C         = dword ptr -50Ch
.text:10001656 var_500         = dword ptr -500h
.text:10001656 Buf2            = byte ptr -4FCh
.text:10001656 readfds         = fd_set ptr -4BCh
.text:10001656 phkResult       = byte ptr -3B8h
.text:10001656 var_3B0         = dword ptr -3B0h
.text:10001656 var_1A4         = dword ptr -1A4h
.text:10001656 var_194         = dword ptr -194h
.text:10001656 WSAData         = WSAData ptr -190h
.text:10001656 arg_0           = dword ptr  4
```

Per riconoscere una variabile da un parametro, è sufficiente guardare il loro offset rispetto al registro EBP. Se è negativo sono variabili, se è positivo sono parametri. Di conseguenza, quelle elencate in figura sono tutte variabili tranne l'ultima voce, che è un parametro.

2.4 Considerazioni sul malware

Analizzando il codice in maniera più approfondita, si notano diversi elementi che portano a pensare che questo malware sia una backdoor. Prima tra tutti, la funzione BackdoorServer.

```
xdoors_d:10093D74 ; char aBackdoorServer[]
xdoors_d:10093D74 aBackdoorServer db 0Dh,0Ah             ; DATA XREF: sub_100042DB+B5↑o
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
xdoors_d:10093D74                 db 0Dh,0Ah,0
```