ANALISI STATICA CON IDA

ANALISI AVANZATA

04-04-2023

PUNTO 1:
Con lo shortcut CTRL+L apro la barra di ricerca per nome ed inserisco DllMain, cliccando IDA mi riporta alla parte di codice in cui è contenuta quella funzione specifica.

```
.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
```

PUNTO 2:
Dalla scheda import individuo la funzione gethostbyname, analizzando il risultato capisco la locazione di memoria in cui tale funzione è stata importata.

```
.idata:100163C8                                        ; sub_10001074+1BF↑r ...
.idata:100163CC ; struct hostent *__stdcall gethostbyname(const char *name)
.idata:100163CC                 extrn gethostbyname:dword
.idata:100163CC                                        ; DATA XREF: sub_10001074:loc_100011AF↑r
.idata:100163CC                                        ; sub_10001074+1D3↑r ...
```

100162...		fseek	MSVCRT
10016278		ftell	MSVCRT
100162A0		fwrite	MSVCRT
100163CC	52	gethostbyname	WS2_32
100163E4	9	htons	WS2_32
100163C8	11	inet_addr	WS2_32
100163...	12	inet_ntoa	WS2_32
1001624C		isdigit	MSVCRT

PUNTO 3:
Con lo shortcut "G" apro la barra di ricerca degli indirizzi di memoria e dopo aver inserito quello indicato noto che sono istanziate 21 variabili locali.

```
.text:10001656
.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 hModule         = dword ptr -670h
.text:10001656 timeout         = timeval ptr -66Ch
.text:10001656 name            = sockaddr ptr -664h
.text:10001656 var_654         = word ptr -654h
.text:10001656 in              = in_addr ptr -650h
.text:10001656 Parameter       = byte ptr -644h
.text:10001656 CommandLine     = byte ptr -63Fh
.text:10001656 Data            = byte ptr -638h
.text:10001656 var_544         = dword ptr -544h
.text:10001656 var_50C         = dword ptr -50Ch
.text:10001656 var_500         = dword ptr -500h
.text:10001656 var_4FC         = dword ptr -4FCh
.text:10001656 readfds         = fd_set ptr -4BCh
.text:10001656 phkResult       = HKEY__ 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
.text:10001656
.text:10001656                 sub     esp, 678h
```

PUNTO 4:
I parametri locali della funzione sopra sono solo 4.

```
.text:10001365
.text:10001365 ; ================ S U B R O U T I N E =======================================
.text:10001365
.text:10001365
.text:10001365 ; DWORD __stdcall sub_10001365(LPVOID)
.text:10001365 sub_10001365    proc near               ; DATA XREF: DllMain(x,x,x)+8A↓o
.text:10001365
.text:10001365 var_54          = FILE ptr -54h
.text:10001365 var_30          = word ptr -30h
.text:10001365 in              = in_addr ptr -2Ch
.text:10001365 name            = dword ptr -28h
.text:10001365
.text:10001365                 sub     esp, 54h
```

PUNTO 5:

Questo malware contiene al suo interno vari frammenti di codice che son volti a minare l'integrità dei registri di sistema, eseguendo controlli specifici sulla macchina vittima per procedere nella direzione giusta.
A seguito dell'individuazione di funzioni che vanno a creare socket ed interagire con la console spostandosi tra le cartelle possiamo pensare che si tratti di un malware di tipo Backdoor / Remote Shell.

```
xdoors_d:10095B20 ; char aCommand_exeC[]
xdoors_d:10095B20 aCommand_exeC   db '\command.exe /c ',0 ; DATA XREF: sub_1000FF58:loc_100101D7↑o
xdoors_d:10095B31                 align 4
xdoors_d:10095B34 aCmd_exeC       db '\cmd.exe /c ',0     ; DATA XREF: sub_1000FF58+278↑o
xdoors_d:10095B41                 align 4
xdoors_d:10095B44 ; char aHiMasterDDDDDD[]
xdoors_d:10095B44 aHiMasterDDDDDD db 'Hi,Master [%d/%d/%d %d:%d:%d]',0Dh,0Ah
xdoors_d:10095B44                                         ; DATA XREF: sub_1000FF58+145↑o
xdoors_d:10095B44                 db 'WelCome Back...Are You Enjoying Today?',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah
xdoors_d:10095B44                 db 'Machine UpTime  [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Secon'
xdoors_d:10095B44                 db 'ds]',0Dh,0Ah
xdoors_d:10095B44                 db 'Machine IdleTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Seco'
xdoors_d:10095B44                 db 'nds]',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah
xdoors_d:10095B44                 db 'Encrypt Magic Number For This Remote Shell Session [0x%02x]',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah,0
```