

Analisi statica avanzata con IDA

Traccia

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)

Traccia 1

Per visualizzare l'indirizzo della funzione impostiamo IDA in modalità text view e leggiamo l'indirizzo corrispondente, in questo caso **1000D02E**.

```
.text:1000D02E : 8001 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
```

Traccia 2

L'indirizzo in questione è 100163CC che possiamo confermare anche cercando la funzione nella TAB IDA view

00000000100163C8	11	inet_addr	WS2_32
00000000100163CC	52	gethostbyname	WS2_32
00000000100163D0	12	inet_ntoa	WS2_32

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

La funzione gethostbyname recupera le informazioni di un host corrispondenti a un nome host da un database di host.

Traccia 3

Cercando e aprendo la funzione richiesta troviamo 23 variabili aventi offset negativo rispetto a EBP.

```
.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
.text:10001656
```

Traccia 4

Nella funzione precedente vi è un solo parametro, arg_0, che si distingue dalle variabili perchè ha offset positivo rispetto ad EBP.

```
.text:10001656 WSADATA = WSADATA ptr -190h
.text:10001656 arg_0 = dword ptr 4
.text:10001656
```

Traccia 5

Controllando la subroutine sub_1000208F troviamo dei commenti relativi a FTP e anonymous, che insieme fanno pensare a una possibile abilitazione del login anonimo via FTP

```
lea    eax, [ebp+Str]
push   offset SubStr ; "ftp://"
push   eax           ; Str
```

```
lea    eax, [ebp+var_A8C]
push   offset Source ; "anonymous"
push   eax           ; Dest
```

Nella subroutine sub_1000FF58 è presente un messaggio simpatico diretto probabilmente all'attaccante.

```
push   eax
lea    eax, [ebp+Str]
push   offset aHiMasterDDDDDD ; "Hi,Master [%d/%d/%d %d:%d:%d]\r\nWelCome "...
push   eax                   ; Dest
```

Cliccando due volte sul messaggio saltiamo al messaggio completo che contiene riferimenti a una Remote Shell.

```
* 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+14510
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
xdoors_d:10095B44 ; char aCk 10095B44
```

Questo fa supporre che si tratti di una backdoor.