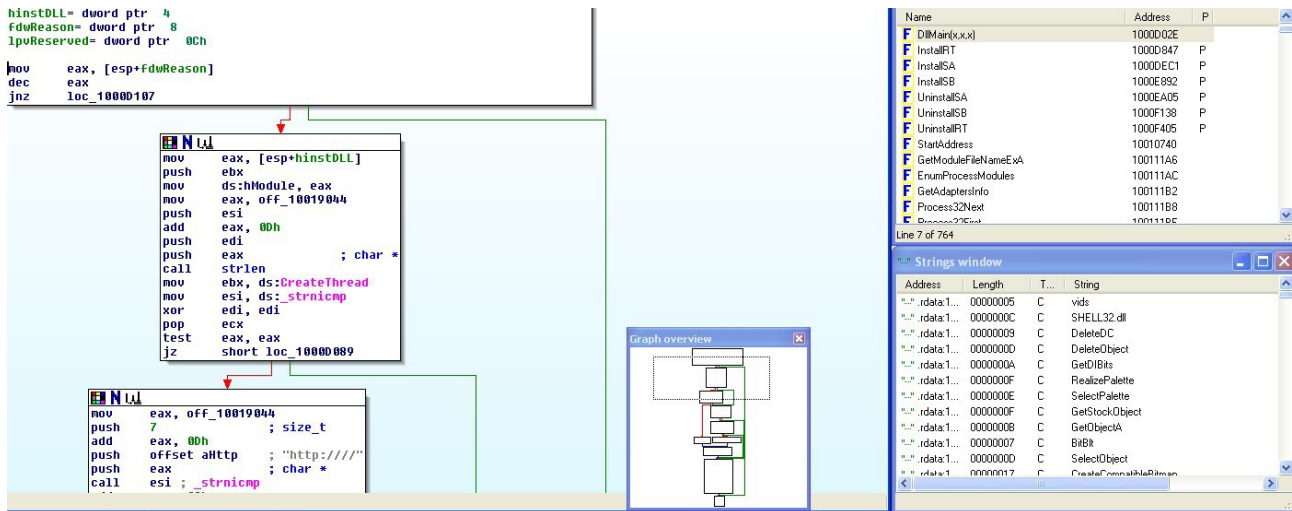


REPORT U3W3L2

Nell'esercizio di oggi andiamo ad analizzare il tool IDA Pro ,un potente Disassembler che è in grado di supportare molti file eseguibili nella loro analisi.

Per prima cosa siamo andati a trovare come chiedeva da traccia ,l'indirizzo della funzione DLLMain:



Successivamente abbiamo cercato dalla scheda imports la funzione "gethostbyname" con il suo corrispettivo indirizzo:

100163...	52	gethostbyname	WS2_32
100163E4	9	htons	WS2_32
100163C8	11	inet_addr	WS2_32

```
.text:10001000 55 8B EC 81 EC 04 01 00 00 80 A5 FC FE FF FF 00 0x8080...ÇNn; .
.text:10001010 56 57 6A 40 59 33 C0 8D BD FD FE FF FF 68 04 01 Uwj@Y3+i+z; h██
.text:10001020 00 00 F3 AB 66 AB AA 8D 85 FC FE FF FF 50 FF 15 ..=%f%-iàn! P $
.text:10001030 20 62 01 10 50 E8 D3 2B 00 00 8B 35 BC 62 01 10 b██PF++..i5+b██
.text:10001040 8D 85 FC FE FF FF 68 EC 32 09 10 50 FF D6 83 C4 àn; h2██P +â-
.text:10001050 14 85 C0 74 18 8D 85 FC FE FF FF 68 DC 32 09 10 qâ+tiân; h 2██
.text:10001060 50 FF D6 59 85 C0 59 74 04 33 C0 EB 03 6A 01 58 P +Yâ+Yt██3+dj██X
.text:10001070 5F 5E C9 C3 83 EC 54 53 55 56 57 E8 80 FF FF FF ^++â8TSUVWÇ
.text:10001080 85 C0 74 0C 5F 5E 5D 33 C0 5B 83 C4 54 C2 04 00 â+ti_^j3+[-â-T-██.
.text:10001090 80 64 24 44 00 6A 07 33 ED 59 33 C0 8D 7C 24 45 Çd$D.j██3FY3+îj$E
.text:100010A0 F3 AB 8B 35 00 63 01 10 89 6C 24 10 66 AB AA BB =%i5.c██èi$P%-z;
.text:100010B0 D8 E5 08 10 6A 20 8D 44 24 48 55 50 E8 91 3E 01 +s██j$îD$HUPFâ>██
.text:100010C0 00 8D 44 24 1C 50 8D 44 24 54 6A 20 50 A1 44 90 .îD$PîD$Tj PîDÉ
.text:100010D0 01 10 55 83 C0 0D 50 6A 01 5F 57 E8 EE 1B 00 00 ███Uâ+Pj██_WFe██.
.text:100010E0 83 C4 24 85 C0 0F 84 50 02 00 00 55 68 FC 32 09 â-â+...âP██.Uhn2██
.text:100010F0 10 FF 15 18 62 01 10 6A 2E 8D 44 24 48 5D 55 50 █ gîb██j.îD$HJUP
.text:10001100 FF D6 59 85 C0 59 75 45 8D 44 24 44 6A 3A 50 FF +Yâ+YtEîD$Dj:P
.text:10001110 D6 59 85 C0 59 74 1E 8D 44 24 44 6A 40 50 FF D6 +Yâ+YtEîD$Dj@P +
.text:10001120 59 85 C0 59 74 0F 8D 44 24 44 6A 26 50 FF D6 59 Yâ+Yt..îD$Dj@P +Y
.text:10001130 85 C0 59 75 18 8D 44 24 44 50 E8 0D 3E 01 00 50 â+YtîD$DPF██>██.P
.text:10001140 8D 44 24 4C 50 E8 F4 43 00 00 83 C4 0C 8D 44 24 îD$LPF(C..â-îD$
```

Infine siamo passati alla locazione di memoria 10001656 col comando jump to address e abbiamo analizzato i parametri e le variabili locali all'interno della funzione:

I parametri all'interno della funzione sono 20, mentre le variabili locali sono 10.

```
; DWORD __stdcall sub_10001656(LPVOID)
sub_10001656 proc near

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
arg_0= dword ptr 4

sub     esp, 678h
push    ebx
push    ebp
push    esi
push    edi
call    sub_10001000
test    eax, eax
jnz     short loc_100016BC
```

Il malware in questione si tratta di un apertura di una backdoor .