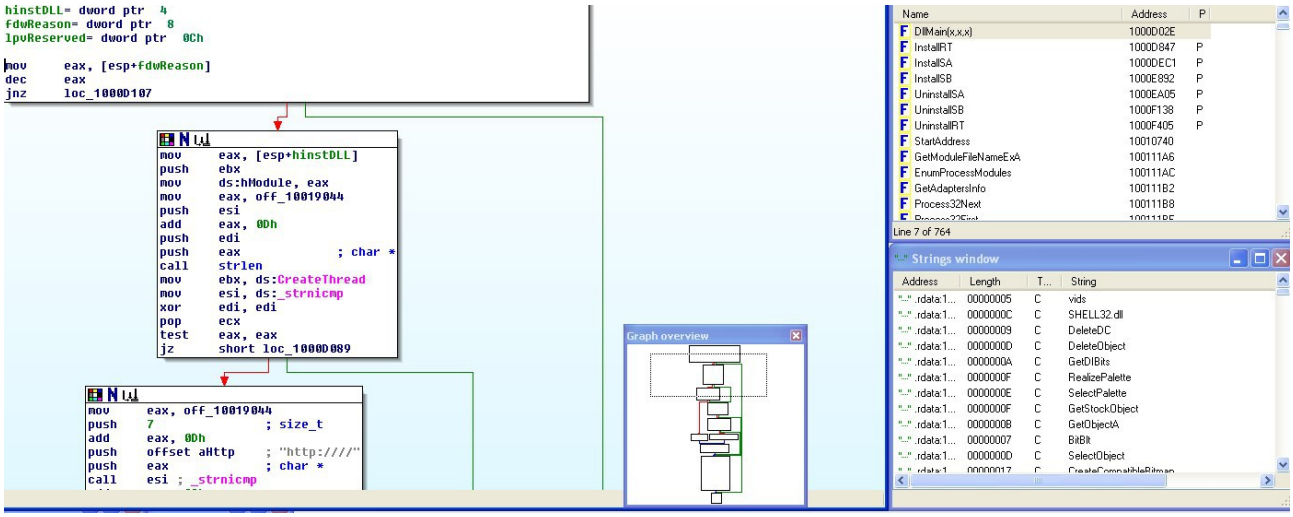
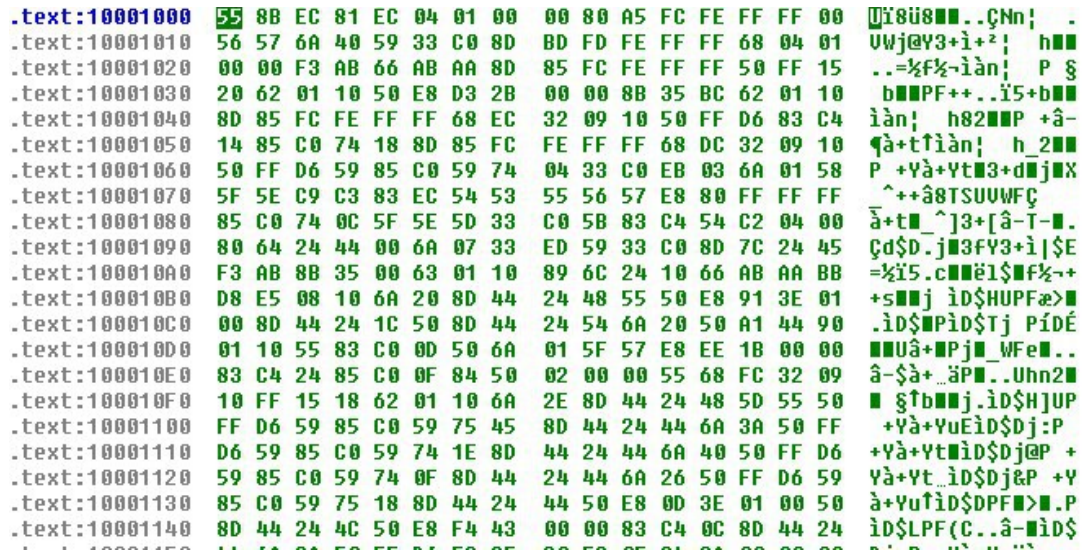
REPORT U3W3L2

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:

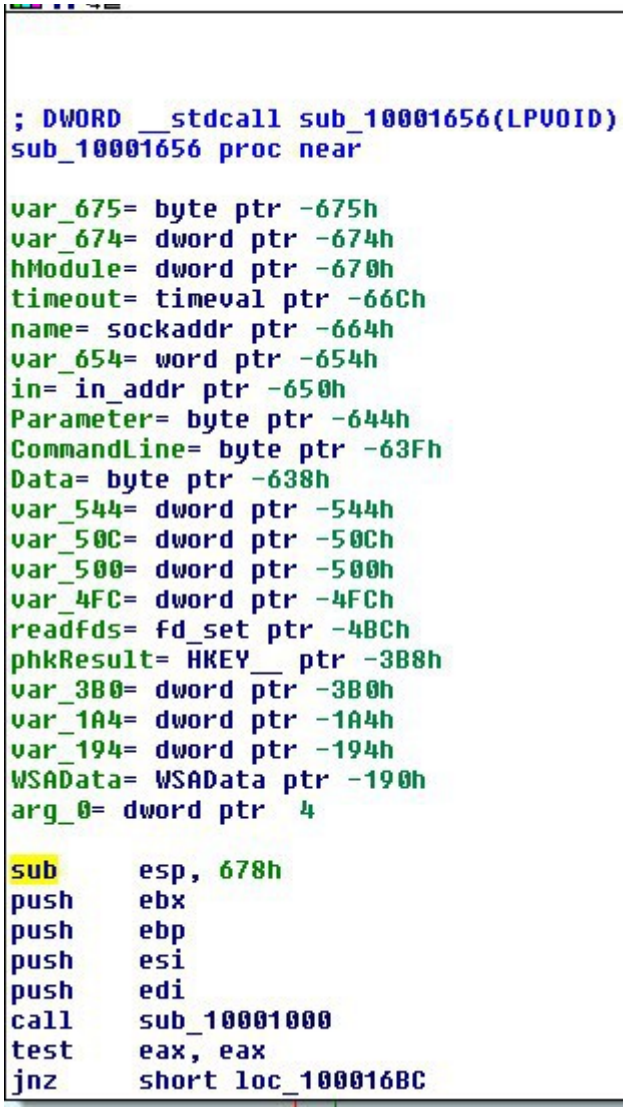


Successivamente abbiamo cercato dalla scheda imports la funzione "gethostbyname" con il suo corrispettivo indirizzo:



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:

Il parametro all'interno è uno,mentre le variabili locali sono 20.



```
; 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 .