ANALISI STATICA AVANZATA CON IDA

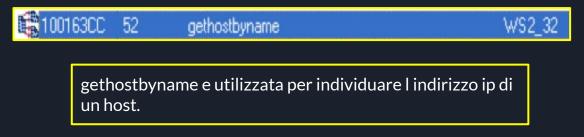
Individuare l'indirizzo della funzione DLLMain (così com'è, in esadecimale)

```
; BOOL __stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
_DllMain@12 proc near

1|888D82E 8B 44 24 68 48 8F 85 CE 88 88 88 44 24 84 53 iD$.H.à+...iD$.S

L'indirizzo usato dalla funzione e 1000D02E.
```

2. Dalla scheda «imports» individuare la funzione «gethostbyname ». Qualè l'indirizzo dell'import? Cosa fa la funzione?



struct hostent *__stdcall gethostbyname(const char *name)
extrn gethostbyname:dword

3. Quante sono le **variabili locali** della **funzione** alla locazione di memoria 0x10001656?

Le variabili locali sono 23

```
sub_10001656 proc near
var 675= bute ptr -675h
var 674= dword ptr -674h
hLibHodule- dword ptr -670h
timeout= timeval ptr -66Ch
name- sockaddr ptr -664h
var 654= word ptr -654h
Dst- duord ptr -650h
Paraneter= bute ptr -644h
var 648- bute ptr -640h
CommandLine- byte ptr -63Fh
Source= bute ptr -63Dh
Data- byte ptr -638h
var 637= byte ptr -637h
var 544- dword ptr -544h
var 58C= dword ptr -50Ch
var 500- dword ptr -500h
Buf2= bute ptr -4FCh
readfds= fd set ptr -48Ch
phkResult- bute ptr -388h
var 388= dword ptr -388h
var 184- dword ptr -184h
var 194= dword ptr -194h
WSAData- WSAData ptr -190h
arg 0= dword ptr 4
```

4. Quantisono, invece, i parametri della funzione sopra?

I parametri sono solo 1:

arg 0= dword ptr 4

5. Inserire altre considerazioni macro livello sul malware (comportamento)

Deduco sia una backdoor poiché troviamo funzioni e variabili inerenti ad un'ipotetica "backdoorserver"

```
; 1pBuffer
push
push
       edi
                        ; nBufferLength
call
       ds:GetCurrentDirectoryA
       esi, ds:sprintf
       eax, [ebp+buf]
1ea
       offset aBackdoorServer ; "\r\n\r\n***************************\r\n[Ba"..
                        ; Dest
push
call
       esi ; sprintf
       ebx, [ebp+s]
lea
       eax, [ebp+buf]
push
       eax
                        ; buf
call
       sub 100038BB
       esp, 10h
lea
        eax, [ebp+PathName]
                        ; 1pPathName
       eax
       ds:SetCurrentDirectoryA
call
       eax. eax
       10c 100046E1
```