Individuazione della funzione DLLmain

```
| Lext:1808082E | Lext:1808082
```

Individuazione della funzione gethostbyname

ECTE 10010510		TO II	1110 Y C( ) 1
🅰 100162A0		fwrite	MSVCRT
100163CC	52	gethostbyname	WS2_32
<b>६६</b> 100163E4	9	htons	WS2_32
🅰 100163C8	11	inet_addr	W\$2_32
mail a control of	40	*	U/00 00

- Individuazione delle variabili alla locazione di memoria 0x10001656

```
III N W
          stdcall sub 10001656(LPVOID)
; DWORD
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= bute 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
                _ ptr -3B8h
phkResult= HKEY
var_3B0= dword ptr -3B0h
var 1A4= dword ptr -1A4h
var 194= dword ptr -194h
WSAData= WSAData ptr -190h
arg_0= dword ptr
cub
             470h
```

```
.text:1000D0F6
                                             push
text:1000DOFB
 .text:10000 0FC
.text:10000 0FD
.text:10000 0FF
.text:10000 190
.text:10000 190
.text:10000 190
                                             push
                                             .
call
                                                         edi var_380
esi var_104
ds:dword_100;var_194
ebx WSAData
                                             pop
                                                                                                 = WSAData ptr -190h
= dword ptr 4
                                             pop
                                                        ebx
                                                                          arg_0
 .text:18880187
 .text:1000D107 loc_1000D107:
.text:1000D107
                                                                                                 sub
                                                                                                            esp, 678h
                                             push
.text:1000D109
                                                                                                 push
                                             pop
```

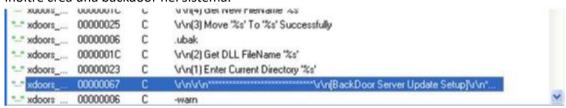
## Considerazioni finali

Il Malware va ad intaccare i seguenti servizi:

## **IEXPLORE.exe** e FTP



## Inoltre crea una backdoor nel sistema.



Dal prossimo screen è possibile vedere inoltre come il malware sia programmato per controllare se l'ambiente in cui viene eseguito è una macchina virtuale o meno.

