Analisi statica avanzata

indirizzo funzione dll

```
000000001000D02E: DllMain(x,x,x)
```

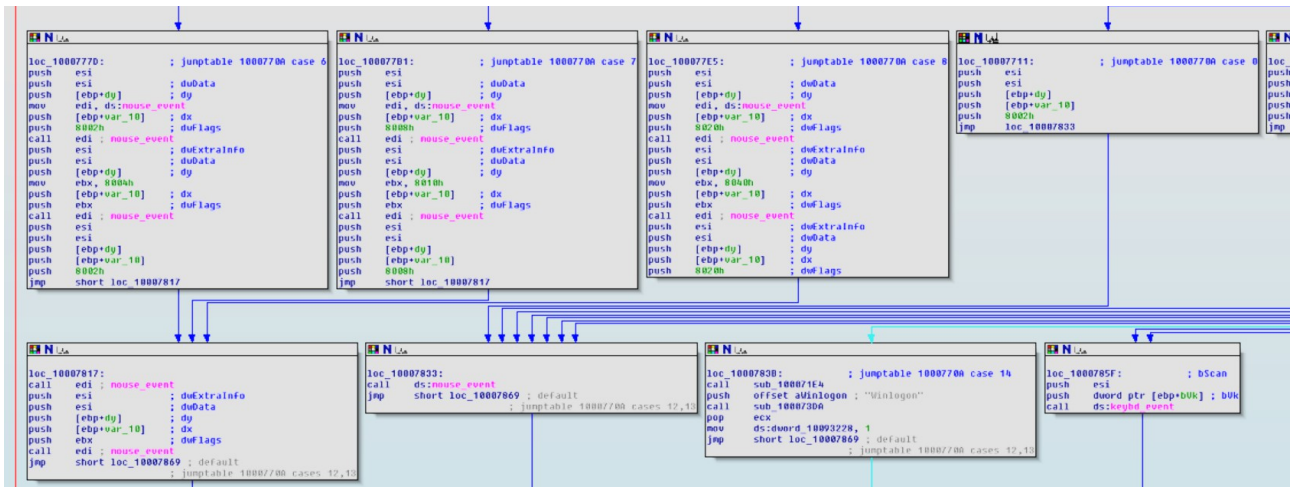
indirizzo import “gethostbyname”

```
.idata:100163C8                                         ; sub_10001074+1BF↑p ...
.idata:100163CC ; struct hostent *__stdcall gethostbyname(const char *name)
.idata:100163CC                 extrn gethostbyname:dword
```

la funzione gethostbyname recupera le informazioni host corrispondenti a un nome host da un database host

```
var_675= byte ptr -675h
var_674= dword ptr -674h
hLibModule= dword ptr -670h
timeout= timeval ptr -66Ch
name= sockaddr ptr -664h
var_654= word ptr -654h
Dst= dword ptr -650h
Parameter= byte ptr -644h
var_640= byte ptr -640h
CommandLine= byte ptr -63Fh
Source= byte ptr -63Dh
Data= byte ptr -638h
var_637= byte ptr -637h
var_544= dword ptr -544h
var_50C= dword ptr -50Ch
var_500= dword ptr -500h
Buf2= byte ptr -4FCh
readfds= fd_set ptr -4BCh
phkResult= byte 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
```

20 variabili riconoscibili dalla locazione con indirizzo negativo
1 parametro riconoscibile dal indirizzo positivo



probabilmene è una backdoor che si insinua nel registro di sistema avviandosi con l'avvio del computer