

Function name	Segment	Start	Length	R	F	L	S	B	T
BlockInput	.text	100111E2	00000006	R
CreateToolhelp32Snapshot	.text	100111C4	00000006	R	T
DllEntryPoint	.text	1001516D	0000009D	R	.	L	.	B	T
DllMain(x,x,x)	.text	1000D02E	000000DF	R	T
EnumProcessModules	.text	100111AC	00000006	R
GetAdaptersInfo	.text	100111B2	00000006	R
GetModuleFileNameExA	.text	100111A6	00000006	R
HandlerProc	.text	1000C9DF	00000077	R	T
ICClose	.text	100113D6	00000006	R	T
ICCompress	.text	100113D0	00000006	R	T
ICImageCompress	.text	100113CA	00000006	R	T

1. Nello screen possiamo vedere l'indirizzo della funzione DllMain

Address	Ordinal	Name	Library
100163A4		wavelnReset	WINMM
100163A8		wavelnOpen	WINMM
100163...		wavelnClose	WINMM
100163B0		wavelnUnprepareHeader	WINMM
100163B4		wavelnPrepareHeader	WINMM
100163B8		wavelnAddBuffer	WINMM
100163...		wavelnStart	WINMM
100163C4	18	select	WS2_32
100163C8	11	inet_addr	WS2_32
100163...	52	gethostbyname	WS2_32

Line 235 of 253

IDA is analysing the input file...
 You may start to explore the input file right now.
 Using FLIRT signature: Microsoft VisualC 2-8/net runtime
 Propagating type information...
 Function argument information is propagated
 The initial autoanalysis has been finished.
 Search completed

2. Dalla scheda "imports" possiamo individuare la funzione **gethostbyname** e il suo rispettivo indirizzo **100163CC**

```

.text:10001656
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656 proc near ; DATA XREF: DllMain(x,x,x)+C8↓
.text:10001656
.text:10001656 var_675 = byte ptr -675h
.text:10001656 var_674 = dword ptr -674h
.text:10001656 hModule = dword ptr -670h
.text:10001656 timeout = timeval ptr -66Ch
.text:10001656 name = sockaddr ptr -664h
.text:10001656 var_654 = word ptr -654h
.text:10001656 in = in_addr ptr -650h
.text:10001656 Parameter = byte ptr -644h

```

00000A56 | 10001656: sub_10001656

3. Facendo una ricerca dell'allocazione di memoria della funzione **0x10001656** possiamo andare a vedere le sue variabili che sono 20

4. Invece abbiamo 2 parametri della funzione sopra

5. Il malware è probabilmente uno spyware con una backdoor oltre ad eseguire svariate altre funzioni.