

- Individuazione della funzione DLLmain

```

.text:1000002E ; R00L stdcall DLLMain(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpvReserved)
.text:1000002E ; CODE XREF: DllEntryPoint+481p
.text:1000002E ; DATA XREF: sub_100110FF+2D1p
.text:1000002E ;-----
.text:1000002E ; jmp short loc_10015203
.text:1000002E ;
.text:1000002E hinstDLL = dword ptr 4
.text:1000002E fdwReason = dword ptr 8
.text:1000002E lpvReserved = dword ptr 0Ch
.text:1000002E mov eax, [esp+fdwReason]
.text:10000032 dec eax
.text:10000032 jnz loc_10000107
.text:10000039 mov eax, [esp+hinstDLL]
.text:1000003D push ebx
.text:1000003E ds:hModule, eax
.text:10000043 mov eax, off_10019044

```

```

loc_100151B5:
push edi
push esi
push ebx
call DllMain@12
cmp esi, 1
; CODE XREF: DllEntryPoint+241j
; DllEntryPoint:loc_100151AFj
; lpvReserved
; fdwReason
; hinstDLL
; DllMain(X,X,X)

```

- Individuazione della funzione gethostbyname

10016210		read	MSVCRT
100162A0		fwrite	MSVCRT
100163CC	52	gethostbyname	WS2_32
100163E4	9	htons	WS2_32
100163C8	11	inet_addr	WS2_32
100163D0	12	...	WS2_32

- Individuazione delle variabili alla locazione di memoria 0x10001656

```

; 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

```

```

.text:100000F6 push offset sub_10001656 ; lpStartAddress
.text:100000FB push edi
.text:100000FC push edi
.text:100000FD call ebx ; Create
.text:100000FF pop edi
.text:10000100 pop esi
.text:10000101 mov ds:dword_10001656, var_194
.text:10000106 pop ebx

```

```

loc_10000107:
push 1
pop eax
ret

```

```

sub esp, 678h
push ebx

```

Il Malware va ad intaccare i seguenti servizi:

IEXPLORE.exe e FTP

```

... xdoors_... 00000012 C SOCKET ERROR... M
... xdoors_... 00000008 C IEuser@
... xdoors_... 0000000A C anonymous
... xdoors_... 00000007 C FTP://
... xdoors_... 00000007 C ftp://
... xdoors_... 00000010 C Content-Length:
... xdoors_... 00000000 C UTTPM 1 E

```

Inoltre crea una backdoor nel sistema.

```
xdoors_... 0000001C C \v\n(4) Get New FileName "%s"
xdoors_... 00000025 C \v\n(3) Move "%s" To "%s" Successfully
xdoors_... 00000006 C .ubak
xdoors_... 0000001C C \v\n(2) Get DLL FileName "%s"
xdoors_... 00000023 C \v\n(1) Enter Current Directory "%s"
xdoors_... 00000067 C \v\n\v\n*****\v\n[BackDoor Server Update Setup]\v\n...
xdoors_... 00000006 C -warn
```

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.

```

.text:1000      ; xdoors..... 00000000 C      0.0.0.0
.text:1000      ; xdoors..... 0000001E C      Microsoft TV/Video Connection
.text:1000      ; xdoors..... 00000020 C      VMware Virtual Ethernet Adapter
.text:1000      ; xdoors..... 00000011 C      Fail To Send[V\n
.text:1000      ; xdoors..... 00000006 C      %s %s
.text:1000      ; xdoors..... 00000000 C      0x00000000
.text:1000      ; xdoors..... 00000001 C      0x00000001
.text:1000      ; xdoors..... 0000001C C      V\n\n\n[Language:] id.0x%V\n\n\n
.text:1000      ; xdoors..... 00000051 C      V\n[install Log] %dV\n[Detect VM :] %dV\n[SSDT Ring3:] %dV\n[SSDT ...
.text:1000      ; xdoors..... 00000054 C      V\n[Host connect type :] %dV\n[Host Reconnect Time:] %dV\n[CURL Re...
.text:1000      ; xdoors..... 00000017 C      V\n[MAIN NAME:]
.text:1000      ; xdoors..... 00000000 C      0x00000000
.text:1000      ; xdoors..... 0000001E C      if exist \"%s\" goto selkillV\n
.text:1000      ; xdoors..... 00000008 C      del \"%s\"V\n
.text:1000      ; xdoors..... 0000001A C      attrib -a -r -s -h \"%s\"V\n
.text:1000      ; xdoors..... 0000000C C      :selkillV\n
.text:1000      ; xdoors..... 0000000C C      @echo offV\n
.text:1000      ; xdoors..... 00000010 C      V\nselfdel.bat
.text:1000      ; xdoors..... 00000008 C      kstarttype
.text:1000      ; xdoors..... 00000019 C      CreateT\nselfdel25seconds

```