

# Pratica S11/L2

Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica. A tal proposito, con riferimento al malware chiamato «Malware\_U3\_W3\_L2» presente all'interno della cartella «Esercizio\_Pratico\_U3\_W3\_L2» sul Desktop della macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.

## 1. Individuare l'indirizzo della funzione DLLMain

```
.text:1000D02B ServiceMain      endp
.text:1000D02B
.text:1000D02E
.text:1000D02E ; |-----| S U B R O U T I N E |-----|
.text:1000D02E
.text:1000D02E ; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPUVOID lpvReserved)
.text:1000D02E _DllMain@12      proc near          ; CODE XREF: DllEntryPoint+4B↓p
.text:1000D02E                                     ; DATA XREF: sub_100110FF+2D↓o
.text:1000D02E
.text:1000D02E hinstDLL          = dword ptr  4
.text:1000D02E fdwReason         = dword ptr  8
.text:1000D02E lpvReserved       = dword ptr 0Ch
.text:1000D02E
* .text:1000D02E      mov     eax, [esp+fdwReason]
* .text:1000D032      dec     eax
* .text:1000D033      jnz     loc_1000D107
```

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

100162...	tree	MSVCR1
100162...	fseek	MSVCRT
10016278	ftell	MSVCRT
100162A0	fwrite	MSVCRT
100163... 52	gethostbyname	WS2_32
100163E4 9	htons	WS2_32
100163C8 11	inet_addr	WS2_32

```
data:100163C8 ; struct hostent * __stdcall gethostbyname(const char *name)
data:100163CC extrn gethostbyname:dword
data:100163CC ; DATA XREF: sub_10001074:loc_100011AF↑r
data:100163CC ; sub_10001074+1D3↑r ...
* data:100163D0 ; char * __stdcall inet_ntoa(struct in_addr in)
data:100163D0 extrn inet_ntoa:dword ; DATA XREF: sub_10001074:loc_10001311↑r
data:100163D0 ; sub_10001365:loc_10001602↑r ...
* data:100163D4 ; int __stdcall recv(SOCKET s,char *buf,int len,int flags)
data:100163D4 extrn recv:dword ; DATA XREF: sub_10001656+2D5↑r
data:100163D4 ; sub_10001656+2E5↑r
```

Imports list:

- nullsub\_2
- StartExS
- HandlerProc
- ServiceMain
- DllMain(xxx)
- InstallRT

Line 4 of 764

La funzione "gethostbyname" è uno strumento di programmazione di rete che traduce un nome di dominio in un indirizzo IP.

3.Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656? **20**

```

; DWORD __stdcall sub_10001656(LPVOID)
sub_10001656 proc near

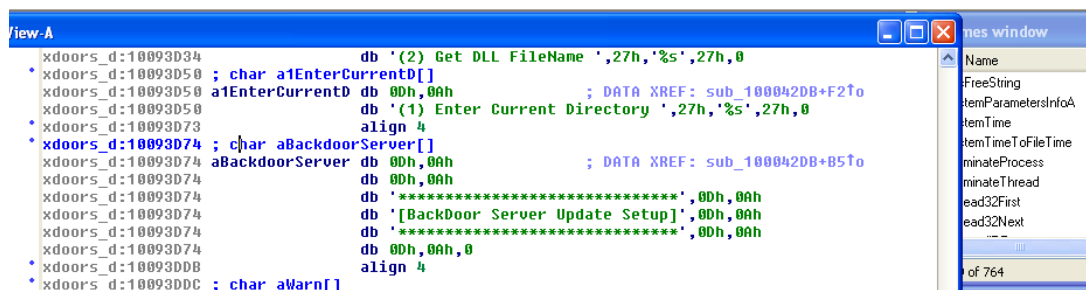
var_675= byte ptr -675h
var_674= dword ptr -674h
hModule= dword ptr -670h
timeout= timeval ptr -66Ch
name= sockaddr ptr -664h
var_654= word ptr -654h
in= in_addr ptr -650h
Parameter= byte ptr -644h
CommandLine= byte ptr -63Fh
Data= byte ptr -638h
var_544= dword ptr -544h
var_50C= dword ptr -50Ch
var_500= 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

```

4.Quanti sono, invece, i parametri della funzione sopra? **Un parametro - offset positivo**

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

Il malware funge da **backdoor** e permette di accedere al sistema offrendo all'attaccante un controllo praticamente completo sul dispositivo compromesso.



```

view-A
xdoors_d:10093D34      db '(2) Get DLL FileName ',27h,'%s',27h,0
xdoors_d:10093D50      ; char a1EnterCurrentD[]
xdoors_d:10093D50      a1EnterCurrentD db 0Dh,0Ah          ; DATA XREF: sub_100042DB+F2f0
xdoors_d:10093D50      db '(1) Enter Current Directory ',27h,'%s',27h,0
xdoors_d:10093D73      align 4
xdoors_d:10093D74      ; char aBackdoorServer[]
xdoors_d:10093D74      aBackdoorServer db 0Dh,0Ah          ; DATA XREF: sub_100042DB+B5f0
xdoors_d:10093D74      db 0Dh,0Ah
xdoors_d:10093D74      db '*****',0Dh,0Ah
xdoors_d:10093D74      db '[BackDoor Server Update Setup]',0Dh,0Ah
xdoors_d:10093D74      db '*****',0Dh,0Ah
xdoors_d:10093D74      db 0Dh,0Ah,0
xdoors_d:10093DDB      align 4
xdoors_d:10093DDC      ; char aWarn[]

```

Names window

Name
FreeString
ItemParametersInfoA
ItemTime
ItemTimeToFileTime
minateProcess
minateThread
read32First
read32Next
...
... of 764