

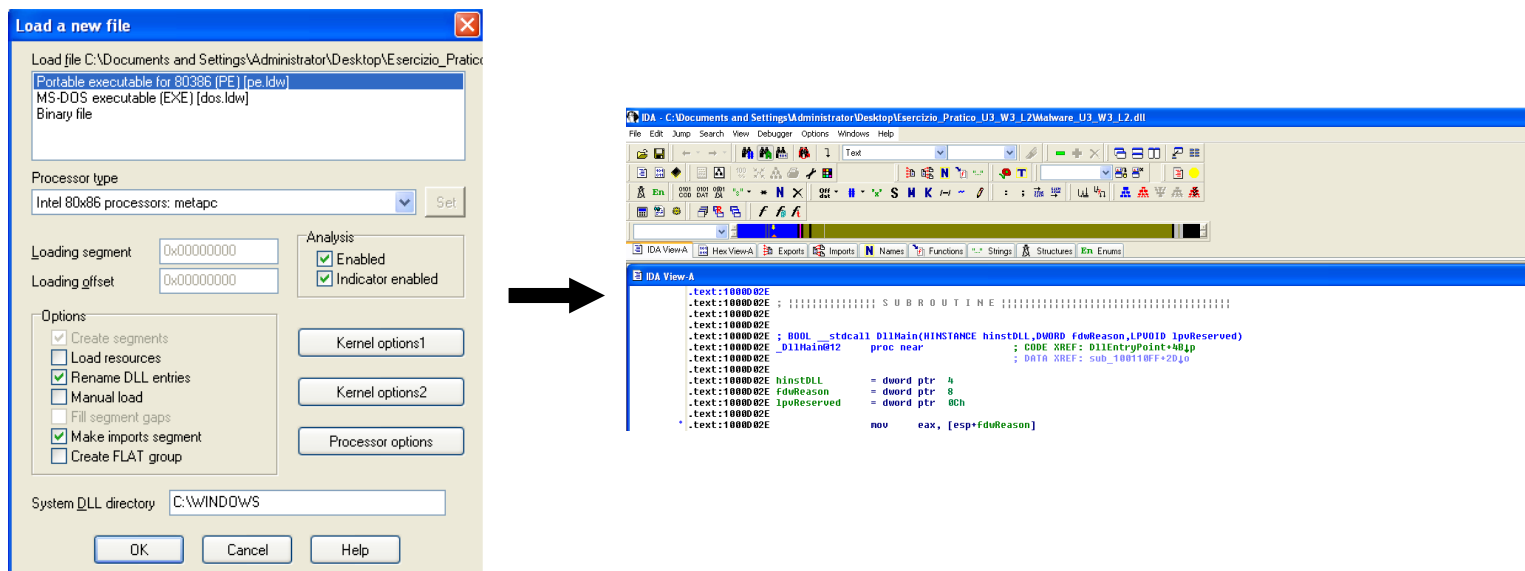
**TASK:**

Con riferimento al malware “Malware\_U3\_W3\_L2” presente sulla macchina Windows XP rispondere ai seguenti quesiti:

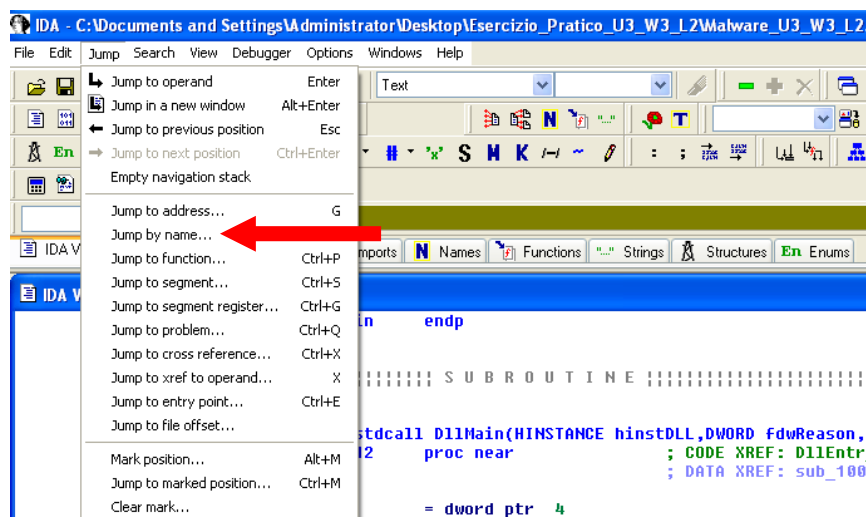
1. Individuare L'indirizzo della funzione DllMain
2. Dalla scheda "imports" individuare la funzione "gethostbyname". Qual'è l'indirizzo dell'import'
3. Quante sono le variabili locali della funzione alla locazione di memoria "0x10001656"?
4. Quante sono invece i parametri della funzione al punto 3?
5. Inserire altre considerazioi macro livello sul malware (comportamento)

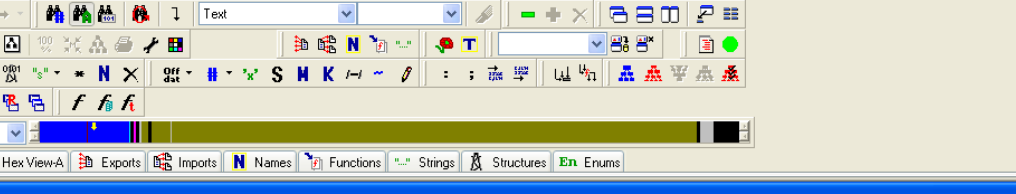
1)

Dopo avere aperto il Malware indicato in traccia con il programma IDA Pro lasciando le impostazioni di base ho ottenuto questa schermata:



A questo punto sono andato a cercare tramite la funzione jump by name la funzione DllMain:





The screenshot shows the IDA Pro interface with the assembly code for the `ServiceMain` function. The code is as follows:

```

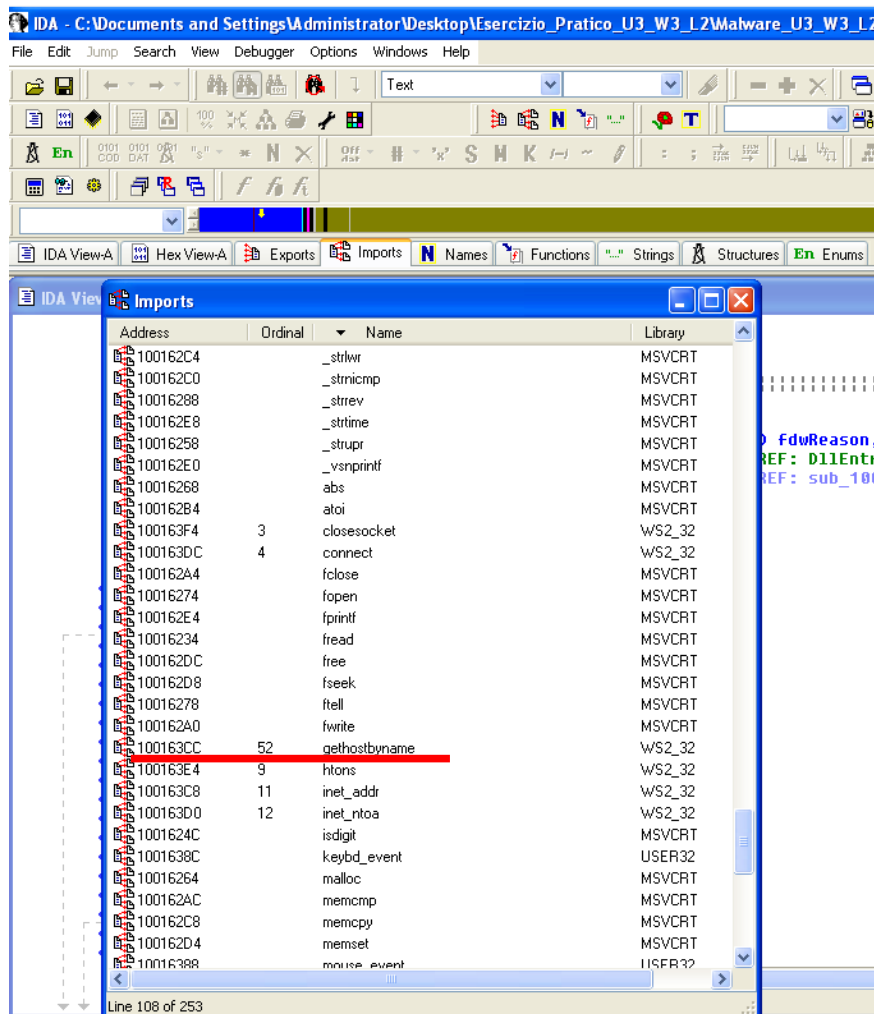
.text:100002B  ServiceMain  endp
.text:100002B
.text:100002E
.text:100002E  ; ::::::::::::::: S U B R O U T I N E :::::::::::::::
.text:100002E
.text:100002E
.text:100002E  ; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpvReserved)
.text:100002E  _DllMain@12    proc near                ; CODE XREF: DllEntryPoint+4Bip
.text:100002E                                           ; DATA XREF: sub_100110FF+2Dj0
.text:100002E
.text:100002E  hinstDLL      = dword ptr  4
.text:100002E  fdwReason     = dword ptr  8
.text:100002E  lpvReserved   = dword ptr  0Ch
.text:100002E
.text:100002E  mov     eax, [esp+fdwReason]
.text:1000032  dec     eax
.text:1000033  jnz     loc_10000107

```

The red box highlights the assembly code from the `ServiceMain` function, specifically the `__stdcall DllMain` function signature and the initial setup of the `hinstDLL`, `fdwReason`, and `lpvReserved` parameters.

A questo punto mi sono spostato sulla scheda “imports” per andare ad individuare la funzione “gethostbyname”:

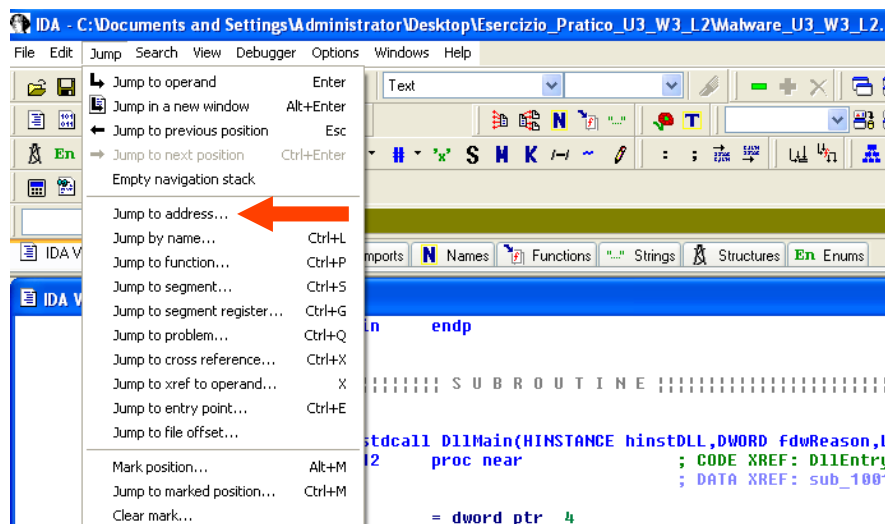




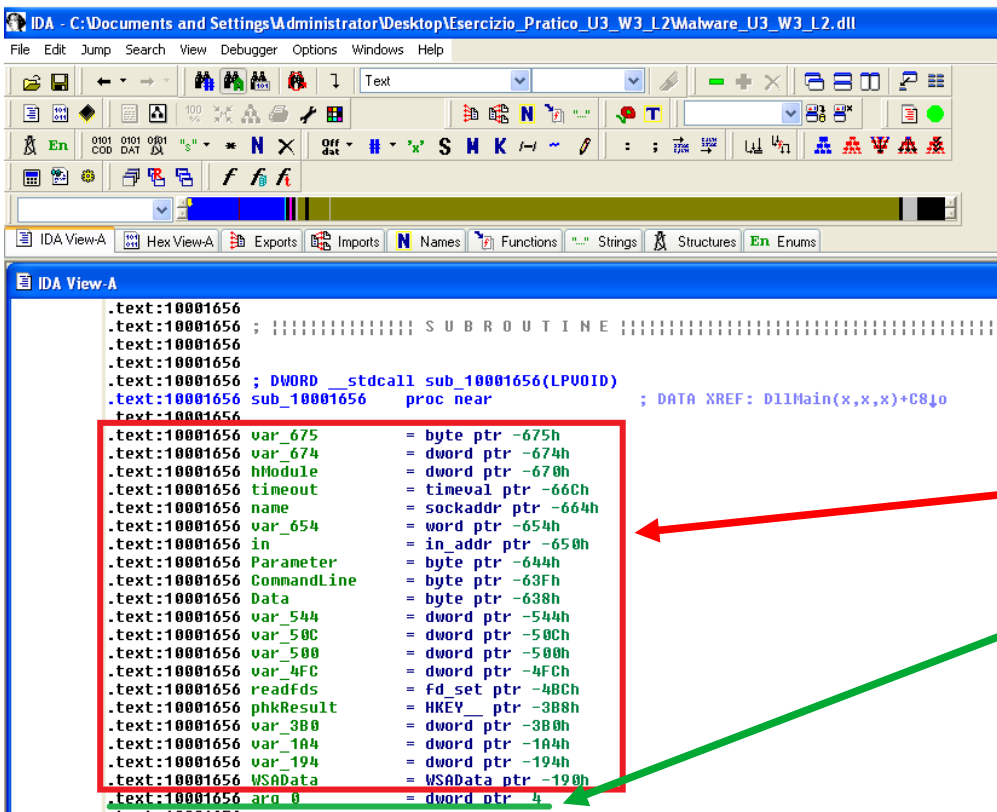
Come possiamo vedere dall'immagine qui sopra tale funzione è localizzata all'indirizzo di memoria 0x100163CC.

3-4)

Ho utilizzato sempre il comando jump ma questa volta sono andato a cercare l'indirizzo di memoria di mio interesse: 0x10001656



Una volta effettuato questo jump ho ottenuto questa schermata:



Nel riquadro rosso possiamo vedere le **variabili locali** della funzione, mentre sottolineato in verde l'unico **argomento** della funzione.

5)

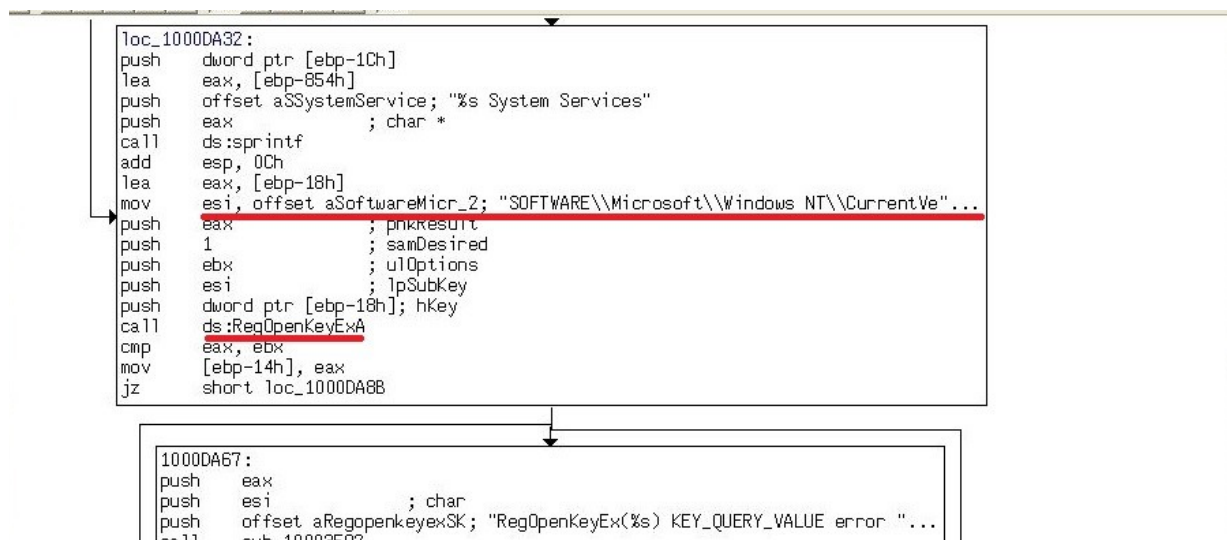
Dall'analisi del codice, coadiuvata dall'utilizzo di [virustotal.com](https://www.virustotal.com), sono giunto alla conclusione che questo malware si occupa di creare una backdoor nella macchina infetta. A sostegno di questa mia ipotesi ho riscontrato questa stringa nel codice:

"	xdoors_d:10093f40	00000051	C	%n\n[install Log:] %d\n\n[detect VM :] %d\n\n[SSD : Rings :] %d\n\n[SSD : Rings :] %d\n\n\n
"	xdoors_d:10093f94	00000054	C	%n\n[Host connect Type :] %d\n\n[Host Reconnect Time:] %d\n\n[CURL Reconnect Time:] %d\n\n
"	xdoors_d:10093afc	00000055	C	%n\n(3) Move '%s' To '%s' Failed,Perhaps Other Process UpdateingUpdated Same Module%n\n
"	xdoors_d:10093d74	00000067	C	%n\n\n% %n\nBackDoor Server Update Setup%n\n% %n\n\n
"	xdoors_d:10093f70	000000AD	C	Accept: image/gif, image/x-bitmap, image/jpeg, application/javascript, application/x-shockwave-flash, application/vnd.ms-excel,
"	xdoors_d:10095844	00000118	C	Hi,Master [%d/%d/%d %d:%d:%d]%n\nWelcome Back...Are You Enjoying Today?%n\n\nMachine UpTime [%d Days

Inoltre ho riscontrato una manipolazione del servizio svchost.exe per porre il processo in background per essere meno rintracciabile:

Occurrences of: svchost		
Address	Instruction	
.text:100070C3	push	offset aSvchost_exe ; "svchost.exe"
.text:1000C8BF	push	offset aSvchost_exe ; "svchost.exe"
.text:1000CD67	push	offset aSvchost_exe ; "svchost.exe"
.text:1000DAD3	mov	dword ptr [ebp-38h], offset aRegQueryValueEx(Svchost
.text:1000DB0C	push	offset aYouSpecifyServ ; "you specify service name not in Svchost"...
.text:1000DBA8	push	offset BinaryPathName ; "%SystemRoot%\System32\svchost.exe -k ne"...
.text:1000E0C7	mov	dword ptr [ebp-5Ch], offset aRegQueryValueEx(Svchost
.text:1000E100	push	offset aYouSpecifySe_0 ; "You Specify Service Name Not In Svchost"...
.text:1000E31D	mov	esi, offset aSvchost_exe ; "svchost.exe"
.text:1000E668	mov	dword ptr [ebp-3Ch], offset aRegQueryValueEx(Svchost
.text:1000EBA1	push	offset aYouSpecifyServ ; "you specify service name not in Svchost"...
.text:1000F860	push	offset aSvchost_exe ; "svchost.exe"
.text:1000FD52	push	offset aSvchost_exe ; "svchost.exe"
xdoors_d_10094468	; char aSvchost_exe[]	
xdoors_d_100950E8	BinaryPathName db "%SystemRoot%\System32\svchost.exe -k netsvcs".0	
xdoors_d_10095170	aYouSpecifyServ db 'you specify service name not in Svchost\netsvcs, must be one of f'	
xdoors_d_100951BC	aRegQueryValueEx db 'RegQueryValueEx(Svchost\netsvcs).0 ; DATA XREF: sub_1000D920	
xdoors_d_10095214	aSoftwareMicr_2 db 'SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost'.0	
xdoors_d_100954BC	aYouSpecifySe_0 db 'You Specify Service Name Not In Svchost\netsvcs, must be one of f'	

Ottiene la persistenza andando a modificare le chiavi di registro come possiamo vedere dall'immagine qui sotto:



E inoltre penso che vada ad aprire una remote shell data:

```

.text:10010100      cmp     dword_1000E304, ebx
.text:1001010E      jz      short loc_100101D7
.text:100101D0      push    offset aCmd_exeC ; "\\cmd.exe /c "
.text:100101D5      jmp     short loc_100101DC

.text:100101D7 ; -----
.text:100101D7 loc_100101D7:
.text:100101D7      push    offset aCommand_exeC ; "\\command.exe /c "
.text:100101DC      loc_100101DC:
.text:100101DC      lea     eax, [ebp+CommandLine]

```

## IDA View-A

```
xdoors_d:10095B20 aCommand_exeC db '\command.exe /c ',0 ; DATA XREF: sub_1000FF58:loc_100101D7↑o
• xdoors_d:10095B31 align 4
• xdoors_d:10095B34 aCmd_exeC db '\cmd.exe /c ',0 ; DATA XREF: sub_1000FF58+278↑o
• xdoors_d:10095B41 align 4
• xdoors_d:10095B44 ; char aHiMasterDDDDDD[]
xdoors_d:10095B44 aHiMasterDDDDDD db 'Hi,Master [%d/%d/%d %d:%d:%d]',0Dh,0Ah
xdoors_d:10095B44 ; DATA XREF: sub_1000FF58+145↑o
xdoors_d:10095B44 db 'Welcome Back...Are You Enjoying Today?',0Dh,0Ah
xdoors_d:10095B44 db 0Dh,0Ah
xdoors_d:10095B44 db 'Machine UpTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Secon'
xdoors_d:10095B44 db 'ds]',0Dh,0Ah
xdoors_d:10095B44 db 'Machine IdleTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Seco'
xdoors_d:10095B44 db 'nds]',0Dh,0Ah
xdoors_d:10095B44 db 0Dh,0Ah
xdoors_d:10095B44 db 'Encrypt Magic Number For This Remote Shell Session [0x%02x]',0Dh,0Ah
xdoors_d:10095B44 db 0Dh,0Ah,0
xdoors_d:10095C5C ; char asc_10095C5C[]
xdoors_d:10095C5C asc_10095C5C: ; DATA XREF: sub_1000FF58+4B↑o
xdoors_d:10095C5C ; sub_1000FF58+3E1↑o
• xdoors_d:10095C5C dw 3Eh
xdoors_d:10095C5C unicode 0, <>,0
• xdoors_d:10095C60 align 200h
xdoors_d:10095C60 xdoors_d ends
xdoors_d:10095C60
xdoors_d:10095C60
xdoors_d:10095C60 end DllEntryPoint
```