

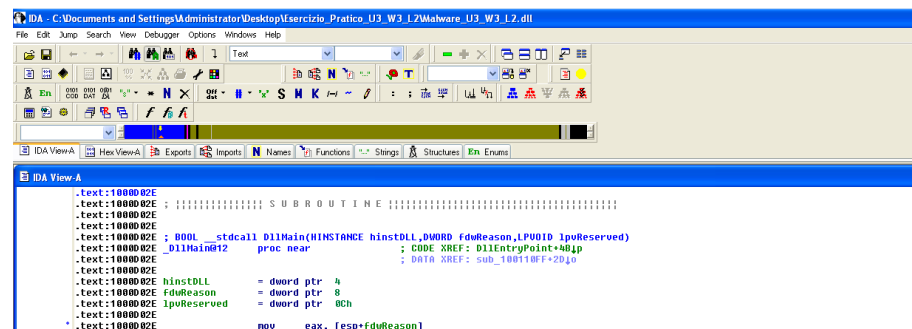
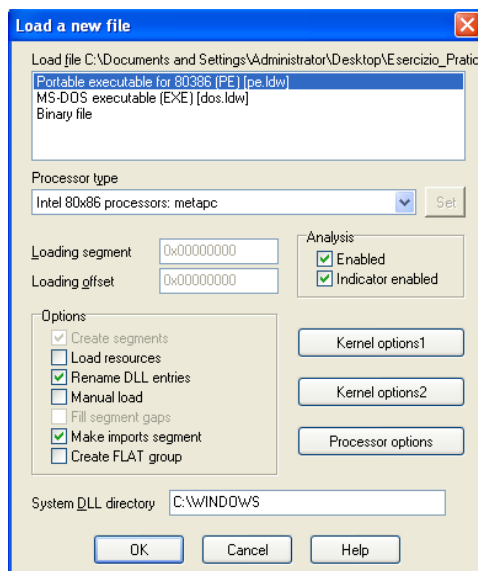
TASK:

Con riferimento al malware “Malware_U3_W3_L2” presente sulla macchina Windows XP rispondere ai seguenti quesiti:

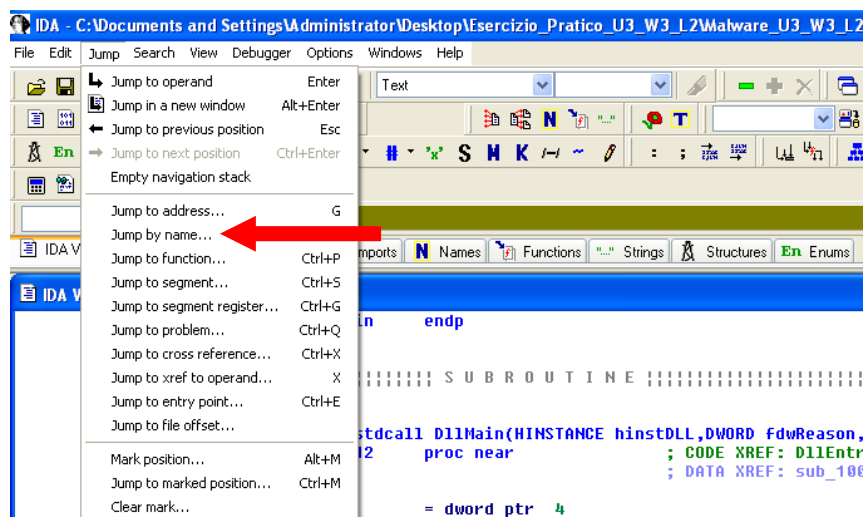
1. Individuare L’indirizzo della funzione DllMain
2. Dalla scheda “imports” individuare la funzione “gethostbyname”. Qual’è l’indirizzo dell’import’
3. Quante sono le variabili locali della funzione alla locazione di memoria “0x10001656”?
4. Quante sono invece i parametri della funzione al punto 3?
5. 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 following components:

- Title Bar:** IDA - C:\Documents and Settings\Administrator\Desktop\Pratico_U3_W3_L2\Malware_U3_W3_L2.dll
- Menu Bar:** File Edit Jump Search View Debugger Options Windows Help
- Toolbar:** Standard IDA tools like Open, Save, Undo, Redo, etc.
- View Bar:**
 - IDA View-A (Selected)
 - Hex View-A
 - Exports
 - Imports
 - Names
 - Functions
 - Strings
 - Structures
 - Enums
- Main Window (IDA View-A):** Displays assembly code for the `ServiceMain` function at address `0000002B`. The code includes comments and variable declarations. A red rectangle highlights the following section:

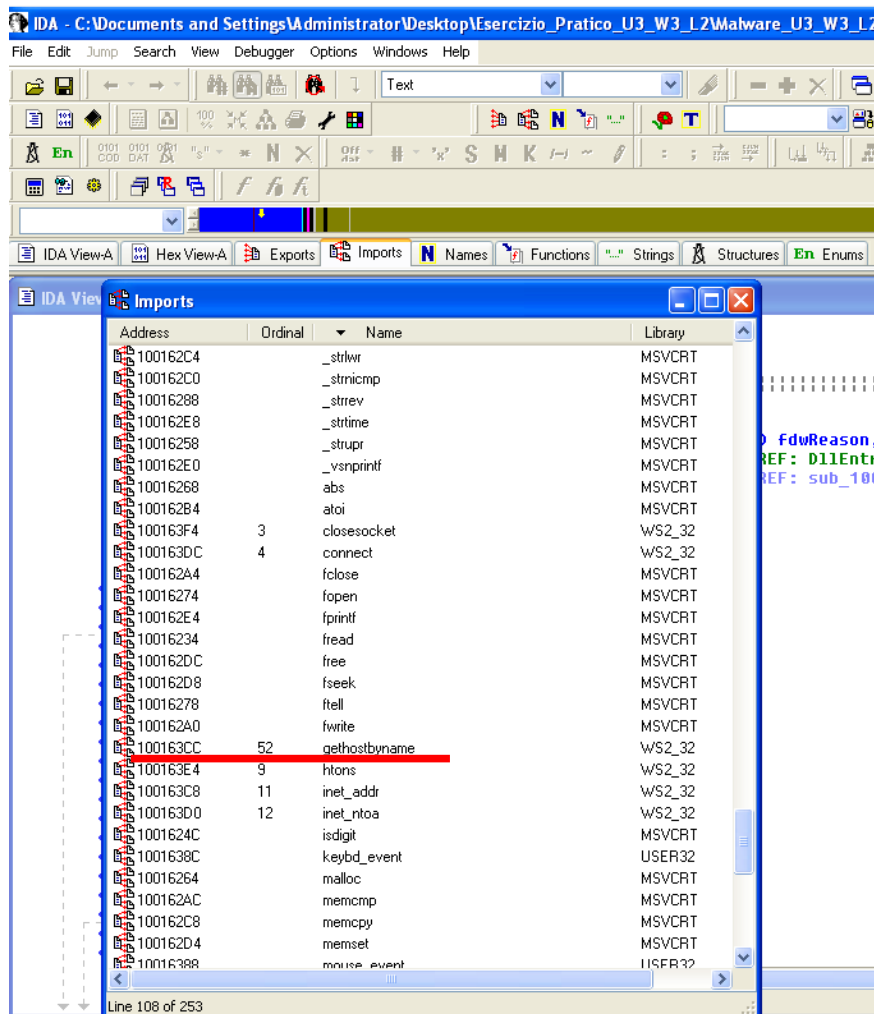

```

.text:1000002E ; |:::::::::::::::::: SUBROUTINE ::::::::::|
.text:1000002E ;
.text:1000002E ;
.text:1000002E ; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPUVOID lpvReserved)
.text:1000002E _DllMain@12 proc near ; CODE XREF: DllEntryPoint+48bp
.text:1000002E ; DATA XREF: sub_100110FF+2d0
.text:1000002E
.text:1000002E hinstDLL = dword ptr 4
.text:1000002E fdwReason = dword ptr 8
.text:1000002E lpvReserved = dword ptr 0Ch
.text:1000002E
.text:1000002E mov eax, [esp+fdwReason]

```

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

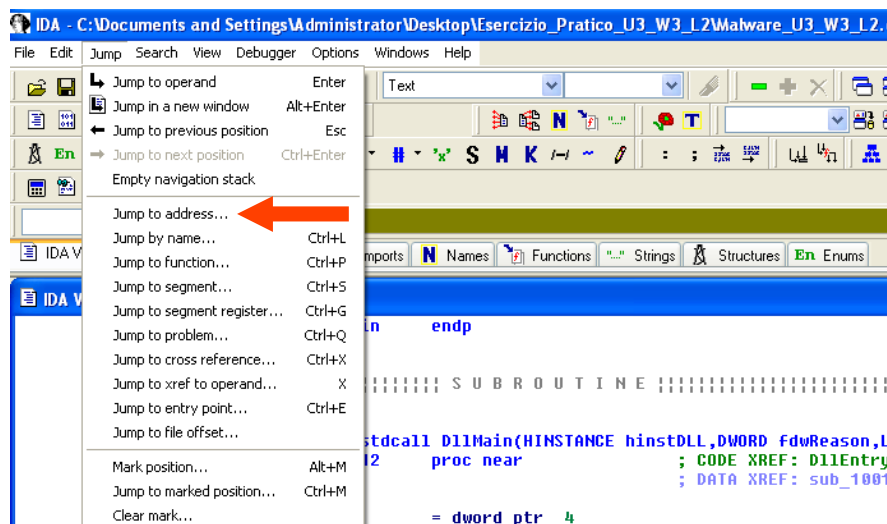




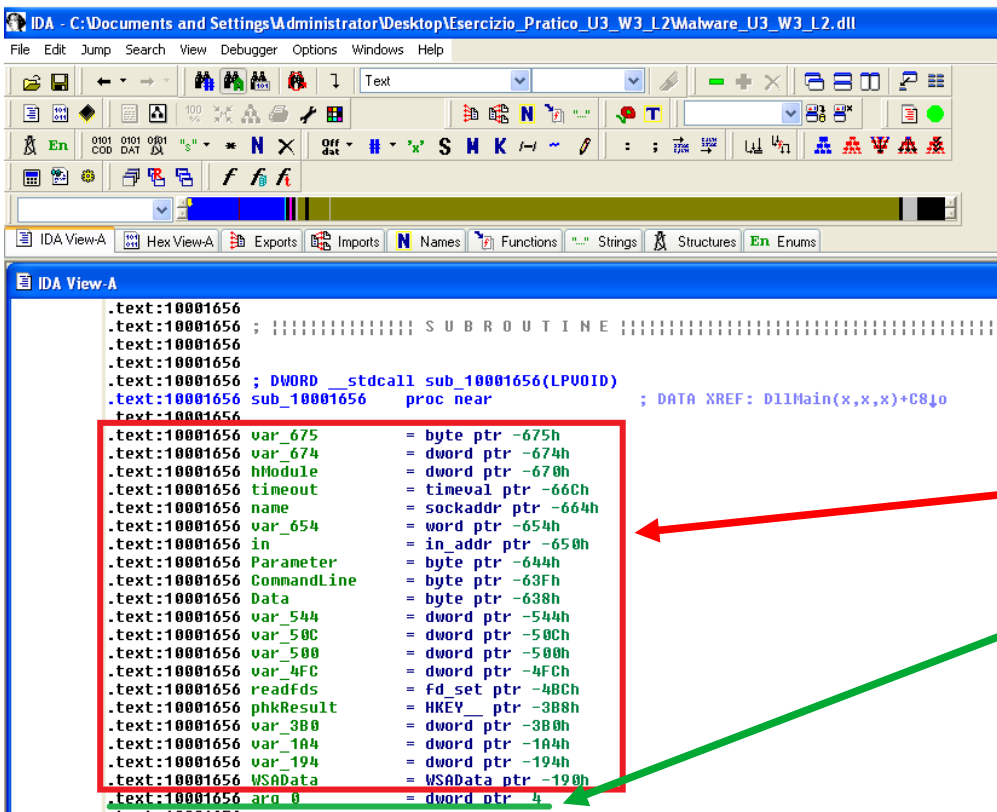
Come possiamo vedere dall'immagine qui sopra tale funzione è localizzata all'indirizzo di memoria 0x100163CC.

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:

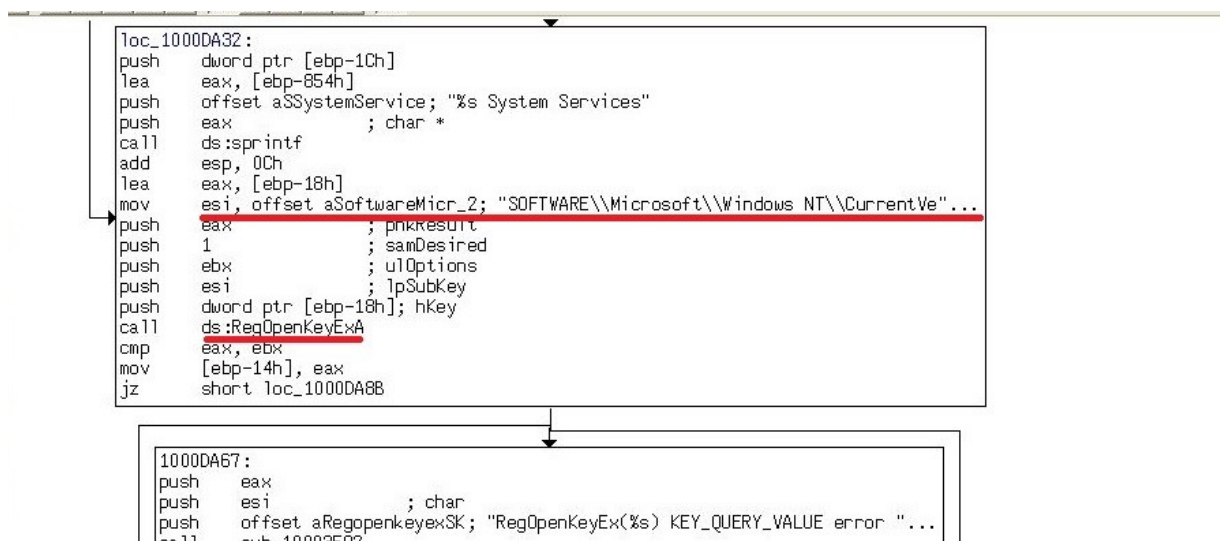
| | | | | |
|-------|-------------------|----------|---|--|
| "..." | xdoors_d_10093F40 | 00000051 | C | \r\n[install Log:] &\r\n\r\ndetect vm :> &\r\n\r\nSSDT Rings:> &\r\n\r\nSSDT Ring0:> &\r\n\r\n\r\n |
| "..." | xdoors_d_10093F94 | 00000054 | C | \r\n\r\nHost connect Type :> %d\r\n\r\nHost Reconnect Time:> %d\r\n\r\nCURL Reconnect Time:> %d\r\n\r\n |
| "..." | xdoors_d_10093AF8 | 00000055 | C | \r\n\r\n(3) Move '%s' To '%s' Failed,Perhaps Other Process UpdateingUpdated Same Module\r\n\r\n |
| "..." | xdoors_d_10093D74 | 00000067 | C | \r\n\r\n\r\n*****\r\n\r\n[BackDoor Server Update Setup]\r\n\r\n*****\r\n\r\n\r\n |
| "..." | xdoors_d_10093740 | 000000AD | C | Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, |
| "..." | xdoors_d_10095B44 | 00000118 | C | Hi,Master [%d/%d/%d %d:%d:%d]\r\n\r\nWellCome Back...Are You Enjoying Today?\r\n\r\n\r\nMachine UpTime [%.-2d 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 a\$svchost_exe;"svchost.exe" |
| .text:1000CB8F | push offset a\$svchost_exe;"svchost.exe" |
| .text:1000CD67 | push offset a\$svchost_exe;"svchost.exe" |
| .text:1000DAD3 | mov dword ptr [ebp-38h], offset aRegQueryValue;"RegQueryValueEx(Svchost" |
| .text:1000DB0C | push offset a\$youSpecifyService;"you specify service name not in Svchost"..." |
| .text:1000DBA8 | push offset BinaryPathName;"%SystemRoot%\System32\svchost.exe -k ne"..." |
| .text:1000DEC7 | mov dword ptr [ebp-5Ch], offset aRegQueryValue;"RegQueryValueEx(Svchost" |
| .text:1000E100 | push offset a\$youSpecifySe_0;"You Specify Service Name Not In Svchost"..." |
| .text:1000E31D | mov esi, offset a\$svchost_exe;"svchost.exe" |
| .text:1000EB68 | mov dword ptr [ebp-3Ch], offset aRegQueryValue;"RegQueryValueEx(Svchost" |
| .text:1000EBA1 | push offset a\$youSpecifyServ;"you specify service name not in Svchost"..." |
| .text:1000F860 | push offset a\$svchost_exe;"svchost.exe" |
| .text:1000FD52 | push offset a\$svchost_exe;"svchost.exe" |
| xdors_d_10094468 | ; char a\$svchost_exe[] |
| xdors_d_100950E8 | BinaryPathName db "%SystemRoot%\System32\svchost.exe -k netsvcs",0 |
| xdors_d_10095170 | a\$youSpecifyServ db "you specify service name not in Svchost\netsvcs, must be one of " |
| xdors_d_1009518C | aRegQueryValue db "RegQueryValueEx(Svchost\netsvcs)",0; DATA XREF: sub_1000D920 |
| xdors_d_10095214 | aSoftwareMicr_2 db "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost",0 |
| xdors_d_100954BC | a\$youSpecifySe_0 db "You Specify Service Name Not In Svchost\netsvcs, must be one of " |

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:

