PRATICA S11L2

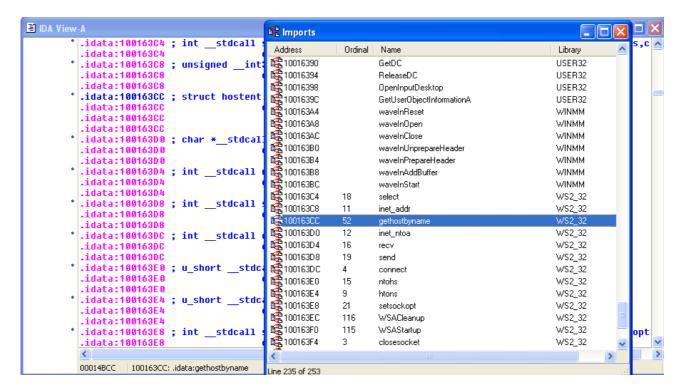
1) Individuare l'indirizzo della funzione DLLMAIN

Possiamo individuare la funzione richiesta dalla tab "names" di IDA pro:

```
DA View-A
             Name
                                                                                                                                                           PSLIST
                                                                                                                                                           nullsub 1
             .text:1000D02E
            nullsub_2
                                 StartEXS
                                                                                                                                                           HandlerProc
                                                                                                                                                           ServiceMain
                                                      = dword ptr
= dword ptr
= dword ptr
                                                                                                                                                           DllMain(x,x,x)
             .text:1000D02E
                                                                                                                                                           InstallRT
             text:1000002E TuwReserved
text:1000002E
text:1000002E
text:10000032
                                                                       ACh
                                                                                                                                                           InstallSA
                                                                eax, [esp+fdwReason]
                                                                                                                                                        Line 7 of 764
                                                                loc 1000D107
             .text:1000D033
                                                      inz
                                                                eax, [esp+hinstDLL]
ebx
ds:hModule, eax
eax, off_10019044
             .text:1000D039
                                                                                                                                                                                             .text:1000D03D
.text:1000D03E
.text:1000D043
.text:1000D048
                                                                                                                                                         Address
                                                                                                                                                                                        String
                                                                                                                                                                    Length
                                                                                                                                                          " .rdata:1
                                                                                                                                                                    00000005
                                                                esi eax, 8Dh edi edi eax ; ch strlen ebx, ds:CreateThread esi, ds:_strnicmp edi, edi ecx eax, eax
                                                                esi
                                                                                                                                                                                       SHELL32.dll
                                                                                                                                                           .rdata:1..
                                                                                                                                                                    0000000C
             .text:1000D049
                                                      add
                                                                                                                                                           .rdata:1.
                                                                                                                                                                    00000009
                                                                                                                                                                                       DeleteDC
             .text:1000D04C
.text:1000D04D
.text:1000D04E
.text:1000D053
                                                      push
push
call
                                                                                                                                                           .rdata:1..
                                                                                                                                                                    0000000D
                                                                                                                                                                                       DeleteObjec
                                                                                                                                                                                       GetDIBits
                                                                                                                                                           .rdata:1.
                                                                                                                                                                    ΠΠΠΠΠΠΔ
                                                                                                                                                           .rdata:1.
                                                                                                                                                                    0000000F
                                                                                                                                                                                       RealizePalet
             .text:1000D059
                                                                                                                                                           .rdata:1.
                                                                                                                                                                    ODDOOD
                                                                                                                                                                                       SelectPaletti
             .text:1000D05F
                                                                                                                                                                    0000000F
                                                                                                                                                                                       GetStock0b
                                                                                                                                                           .rdata:1..
                                                                                                                                                           .rdata:1..
                                                                                                                                                                    0000000B
                                                                                                                                                                                       GetObjectA
            0000C42E 1000D02E: DllMain(x,x,x)
```

Dallo screen vediamo che l'indirizzo è 1000D02E

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



Selezionando la funzione richiesta, possiamo vedere che il suo indirizzo è 100163CC. Dalla documentazione di windows online possiamo recuperare le informazioni sul funzionamento di tale funzione, che restituisce un indirizzo ip dato un nome host appartenente ad un host database.

3) Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?

Inseriamo l'indirizzo indicato nel campo "jump to address" presente sulla scheda in alto. Le variabili utilizzate dalla funzione sono quelle in figura:

```
DA View-A
                                                                                                                           .text:10001656
           .text:10001656 ; DWORD
                                         stdcall sub 10001656(LPV0ID)
           .text:10001656 sub_10001656
                                                                             ; DATA XREF: DllMain(x,x,x)+C810
                                               proc near
           .text:10001656
           .text:10001656 var_675
                                                = byte ptr -675h
           .text:10001656
                            var_674
                                                = dword ptr -674h
           .text:10001656 hModule
                                                = dword ptr -670h
                                                = timeval ptr -66Ch
= sockaddr ptr -664h
= word ptr -654h
           .text:10001656 timeout
           .text:10001656 name
           .text:10001656 var_654
                                                = in_addr ptr -650h
           .text:10001656 in
                                                = byte ptr -644h
= byte ptr -63Fh
           .text:10001656 Parameter
           .text:10001656 CommandLine
           .text:10001656 Data
                                                = byte ptr -638h
= dword ptr -544h
           .text:10001656 var_544
.text:10001656 var_50C
.text:10001656 var_500
                                                = dword ptr -50Ch
                                                = dword ptr -500h
                                                = dword ptr -4FCh
           .text:10001656 var_4FC
                                                = fd_set ptr -4BCh
           .text:10001656 readfds
                                                = HKEY__ ptr -3B8h
           .text:10001656 phkResult
                                                = dword ptr -380h
= dword ptr -1A4h
           .text:10001656 var_3B0
           .text:10001656 var_1A4
.text:10001656 var_194
                                                = dword ptr -194h
           .text:10001656 WSAData
                                                = WSAData ptr -190h
```

4) Quanti sono, invece, i parametri della funzione sopra?

Sempre nella stessa scheda, vediamo che l'unico parametro è arg0:

```
.text:10001656 arg_0 = dword ptr 4
```

5) Dalla macro-analisi del codice, vediamo che il malware fa uso di diverse funzioni per utilizzare i socket di windows, gestire le comunicazioni di rete, leggere e modificare le chiavi di registro, connettersi ad un host remoto, inviare e ricevere dati. Aspettandosi quindi di ricevere comunicazioni in ingresso, si può presupporre che si tratti di una backdoor