



S11L2

Individuare indirizzo di funzione

DLLMain

Function name	Segment	Start	Length	R	F	L	S	B	T	=
PSLIST	.text	10007025	00000040	R	T	.
Module32Next	.text	100111CA	00000006	R	T	.
Module32First	.text	100111D0	00000006	R	T	.
InstallSB	.text	1000E892	00000066	R	T	.
InstallSA	.text	1000DEC1	00000061	R	T	.
InstallRT	.text	1000D847	00000061	R	T	.
ICSendMessage	.text	100113DC	00000006	R	T	.
ICOpen	.text	100113E2	00000006	R	T	.
ICImageCompress	.text	100113CA	00000006	R	T	.
ICCompress	.text	100113D0	00000006	R	T	.
ICClose	.text	100113D6	00000006	R	T	.
HandlerProc	.text	1000C9DF	00000077	R	T	.
GetModuleFileNameExA	.text	100111A6	00000006	R
GetAdaptersInfo	.text	100111B2	00000006	R
EnumProcessModules	.text	100111AC	00000006	R
DLLMain(x.x.x)	.text	1000D02E	000000DF	R	T	.
DllEntryPoint	.text	1001516D	0000009D	R	.	L	.	B	T	.
CreateToolhelp32Snapshot	.text	100111C4	00000006	R	T	.

L'indirizzo della funzione gethostbyname è: 100163CC

IDA - C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W3_L2\Malware_U3_W3_L2.dll - [Imports]

File Edit Jump Search View Debugger Options Windows Help

Text

IDA View-A Hex View-A Exports Imports Names Functions Strings Structures Enums

Address	Ordinal	Name	Library
100162E4		fprintf	MSVCRT
10016234		fread	MSVCRT
100162DC		free	MSVCRT
100162D8		fseek	MSVCRT
10016278		ftell	MSVCRT
100162A0		fwrite	MSVCRT
100163CC	52	gethostbyname	WS2_32
100163E4	9	htons	WS2_32
100163C8	11	inet_addr	WS2_32
100163D0	12	inet_ntoa	WS2_32
1001624C		isdigit	MSVCRT
1001638C		keybd_event	USER32

Individuate le variabili locali (19 in totale) e i parametri (1 in totale ovvero arg0) all'indirizzo 0x10001656

Hex View-A | Exports | Imports | Names | Functions | Strings | Structures | Enums

```
.text:10001656
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656      proc near                                ; DATA XREF: DllMain(x,x,x)+C8↓o
.text:10001656
.text:10001656 var_675           = dword ptr -675h
.text:10001656 hModule           = dword ptr -670h
.text:10001656 timeout           = timeval ptr -66Ch
.text:10001656 name              = sockaddr ptr -664h
.text:10001656 var_654           = word ptr -654h
.text:10001656 in               = in_addr ptr -650h
.text:10001656 Parameter         = byte ptr -644h
.text:10001656 CommandLine       = byte ptr -63Fh
.text:10001656 Data              = byte ptr -638h
.text:10001656 var_544           = dword ptr -544h
.text:10001656 var_50C           = dword ptr -50Ch
.text:10001656 var_500           = dword ptr -500h
.text:10001656 var_4FC           = dword ptr -4FCh
.text:10001656 readfds           = fd_set ptr -4BCh
.text:10001656 buf               = byte ptr -3B8h
.text:10001656 var_3B0           = dword ptr -3B0h
.text:10001656 var_1A4           = dword ptr -1A4h
.text:10001656 var_1A4           = dword ptr -1A4h
```

La tipologia del Malware è una Backdoor

Hex View-A | Exports | Imports | Names | Functions | Strings | Structures | Enums

```
.text:1000437C    push    eax                ; lpBuffer
.text:1000437D    push    edi                ; nBufferLength
.text:1000437E    call    ds:GetCurrentDirectoryA
.text:10004384    mov     esi, ds:sprintf
.text:1000438A    lea     eax, [ebp+buf]
.text:10004390    push    offset aBackdoorServer ; "\r\n\r\n*****\r\n[Ba"...
.text:10004395    push    eax                ; char *
.text:10004396    call    esi ; sprintf      ; char aBackdoorServer[]
.text:10004398    mov     ebx, [ebp+s]       aBackdoorServer db 0Dh,0Ah           ; DATA XREF: sub_100042DB+B5fo
.text:1000439B    lea     eax, [ebp+buf]     db 0Dh,0Ah
.text:100043A1    push    eax                db '*****',0Dh,0Ah
.text:100043A2    push    ebx                db '[BackDoor Server Update Setup]',0Dh,0Ah
.text:100043A3    call    sub_100038BB       db '*****',0Dh,0Ah
.text:100043A8    add     esp, 10h          db 0Dh,0Ah,0
.text:100043AB    lea     eax, [ebp+PathName]
.text:100043B1    push    eax                ; lpPathName
.text:100043B2    call    ds:SetCurrentDirectoryA
.text:100043B8    test    eax, eax
.text:100043BA    jz      loc_100046E1
.text:100043C0    lea     eax, [ebp+PathName]
.text:100043C6    push    eax
.text:100043C7    lea     eax, [ebp+buf]
```

00003790 | 10004390: sub_100042DB+B5fo

Information from the database: All idle | Down | Pick: 7CB