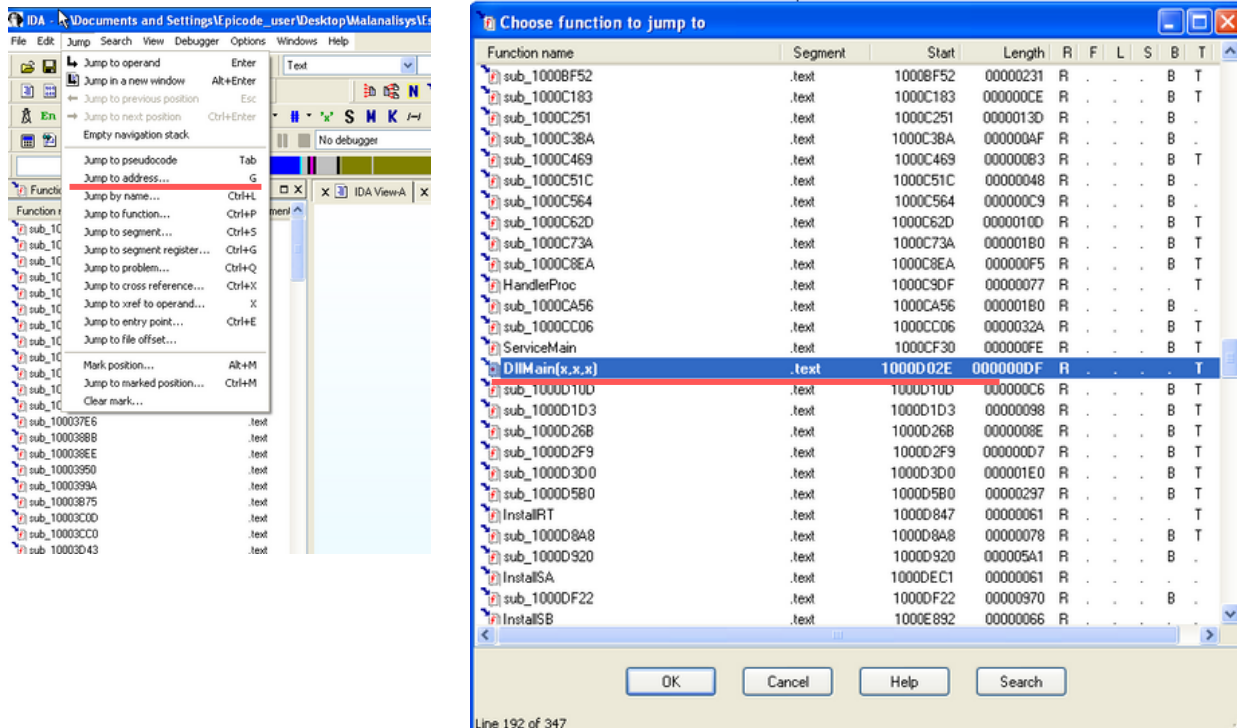


1. Individuazione dell'indirizzo della funzione DLLMain

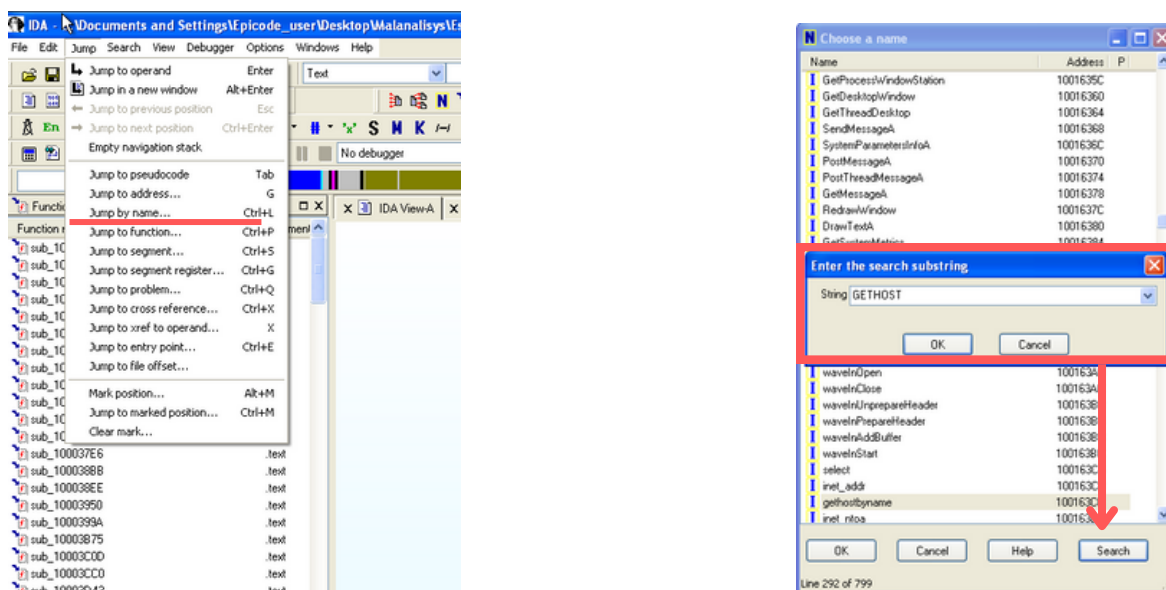
Inizialmente individuiamo l'indirizzo della funzione DLLMain. Per farlo, apriamo il menù “Jump”, “Jump to function” e cerchiamo la funzionalità “Search”:

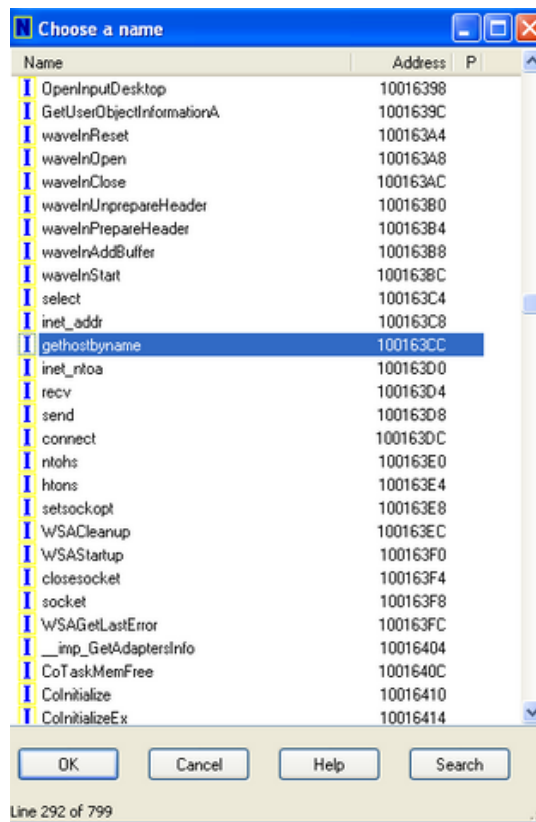


Abbiamo identificato la funzione DLLMain; l'indirizzo di memoria ad essa associato è 1000D02E.

2. Individuazione dell'indirizzo di import della funzione gethostbyname

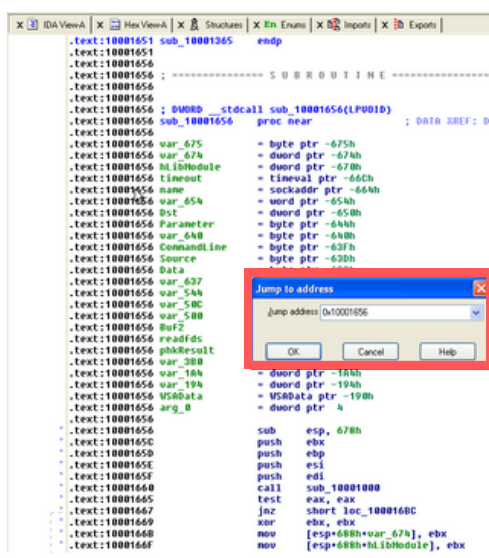
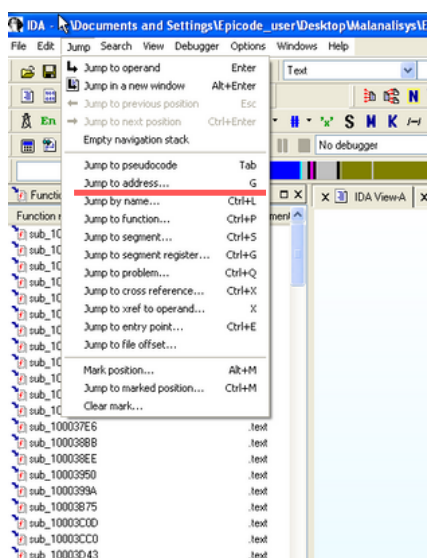
Adesso individuo la funzione gethostbyname, presente tra le funzioni importate dall'eseguibile. Scelgo funzionalità jump by name e ricercare il nome della funzione cliccando su “Search”:





Ho individuato la funzione ricercata, presente all'indirizzo di memoria 1001063CC

3. Quantificazione delle variabili locali e dei parametri della funzione alla locazione di memoria 0x10001656



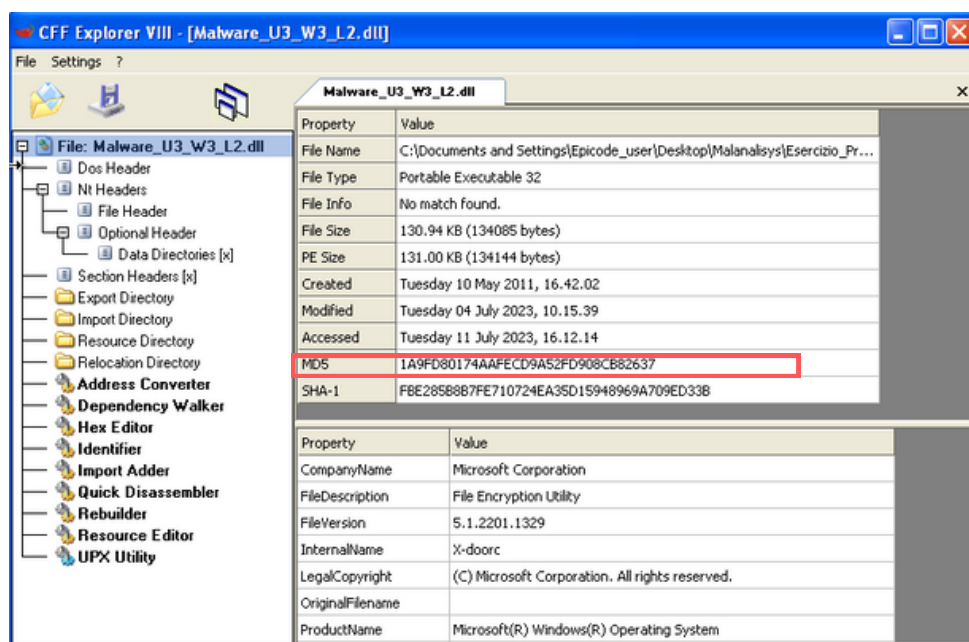
```

.text:10001651 sub_10001365 endp
.text:10001651
.text:10001656 ; ===== SUBROUTINE =====
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656 proc near ; DATA XREF: DllMain(x,x,x)+C810
.text:10001656
.text:10001656 var_675 = byte ptr -675h
.text:10001656 var_674 = dword ptr -674h
.text:10001656 hLibModule = dword ptr -670h
.text:10001656 timeout = timeval ptr -66Ch
.text:10001656 name = sockaddr ptr -664h
.text:10001656 var_654 = word ptr -654h
.text:10001656 Dst = dword ptr -650h
.text:10001656 Parameter = byte ptr -644h
.text:10001656 var_640 = byte ptr -640h
.text:10001656 CommandLine = byte ptr -63Fh
.text:10001656 Source = byte ptr -63Dh
.text:10001656 Data = byte ptr -638h
.text:10001656 var_637 = byte ptr -637h
.text:10001656 var_544 = dword ptr -544h
.text:10001656 var_50C = dword ptr -50Ch
.text:10001656 var_500 = dword ptr -500h
.text:10001656 Buf2 = byte ptr -4FCh
.text:10001656 readfds = fd_set ptr -4BCh
.text:10001656 phkResult = byte ptr -388h
.text:10001656 var_380 = dword ptr -380h
.text:10001656 var_1A4 = dword ptr -1A4h
.text:10001656 var_194 = dword ptr -194h
.text:10001656 VSAData = VSADData ptr -190h
.text:10001656 arg_0 = dword ptr 4
.text:10001656
.text:10001656 sub esp, 678h
.text:10001656 push ebx
.text:10001656 push ebp
.text:10001656 push esi
.text:10001656 push edi
.text:10001660 call sub_10001000
.text:10001665 test eax, eax
.text:10001667 jnz short loc_1000168C
.text:10001669 xor ebx, ebx
.text:1000166B mov [esp+688h+var_674], ebx
.text:1000166F mov [esp+688h+hLibModule], ebx

```

4. Considerazioni macro-livello circa il comportamento del malware

Inizialmente trovo l'hash del malware con CFF EXPLORER



Una volta trovato l'hash del file lo inserisco su virus total

eb1079bd96b0cc19c38b76342113a0966aad47518f1a7535eebffaadb4a

59 / 70

59 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

eb1079bd96b0cc19c38b76342113a0966aad47518f1a7535eebffaadb4a

X-doorc

Size 130.94 KB Last Analysis Date 11 days ago

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY (19)

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.idcaf.r06cc08f321 Threat categories trojan Family labels idcaf r06cc08f321

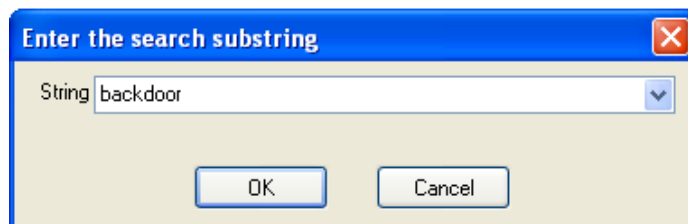
Security vendors' analysis Do you want to automate checks?

Vendor	Detection	Vendor	Detection
Acronis (Static ML)	Suspicious	AhnLab-V3	Backdoor/Win32.Agent.R9408
Alibaba	Backdoor/Win32/Idcaf.9f3a5556	ALYac	Backdoor.XIV
Antiy-AVL	Trojan@backdoor/Win32.Agent	Arcabit	Backdoor.XIV
Avast	Win32:Agent-OLM [Trj]	AVG	Win32:Agent-OLM [Trj]
Avira (no cloud)	BD5/Agent.twe.134160	BitDefender	Backdoor.XIV
ClamAV	Win.Trojan.idcaf-9937585-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)

59 vendors su 70 dicono che è un file malevolo.

Come possiamo vedere nella figura precedente il file è una backdoor

Dopo l'analisi di virus total ho provato a cercare la parola backdoor nelle stringhe



Function name	Segment	Address	Length	Type	String
00401000	text	00401000	1	C	GetDiskFreeSpaceEx
00401004	text	00401004	1	C	"MHz"
00401008	text	00401008	1	C	HARDWARE\DESCRIPTION\System\CentralProcessor\0
0040100C	text	0040100C	1	C	default
00401010	text	00401010	1	C	GroupInfo
00401014	text	00401014	1	C	HostInfo
00401018	text	00401018	1	C	SOFTWARE\Microsoft\Windows\CurrentVersion
0040101C	text	0040101C	1	C	Fail To Create Snap Shot
00401020	text	00401020	1	C	Virus(1)Enter Current Directory Error Update Failed
00401024	text	00401024	1	C	Virus(2)Get DLL FileName Error Update Failed
00401028	text	00401028	1	C	Virus(3)Move "x" To "y" Failed Perhaps Other Process Updating
0040102C	text	0040102C	1	C	Virus(4)Resume "x" To "y" Failed Update Failed
00401030	text	00401030	1	C	Virus(5)Resume "x" To "y" Successfully Update Failed
00401034	text	00401034	1	C	Virus(6)Get New FileName Error Update Failed
00401038	text	00401038	1	C	Virus(7)Update Successfully Will Take Effect Until Next Reboot
0040103C	text	0040103C	1	C	Virus(8)New FileName As Old FileName
00401040	text	00401040	1	C	Virus(9)Resume "x" To "y" Successfully Update Failed
00401044	text	00401044	1	C	Virus(10)Move "x" To "y" Failed Update Failed
00401048	text	00401048	1	C	Virus(11)Copy "x" To "y" Successfully
0040104C	text	0040104C	1	C	Virus(12)Get New FileName "x"
00401050	text	00401050	1	C	Virus(13)Move "x" To "y" Successfully
00401054	text	00401054	1	C	ubak
00401058	text	00401058	1	C	Virus(14)Get DLL FileName "x"
0040105C	text	0040105C	1	C	Virus(15)Enter Current Directory "x"
00401060	text	00401060	1	C	*\@BackDoor Serve Update Setup\Ver...
00401064	text	00401064	1	C	main
00401068	text	00401068	1	C	exit
0040106C	text	0040106C	1	C	stop
00401070	text	00401070	1	C	shutdown
00401074	text	00401074	1	C	sleep
00401078	text	00401078	1	C	reboot
0040107C	text	0040107C	1	C	Default
00401080	text	00401080	1	C	Virus(16)
00401084	text	00401084	1	C	version\default
00401088	text	00401088	1	C	EXPLORER.EXE
0040108C	text	0040108C	1	C	EXPLORER.EXE
00401090	text	00401090	1	C	Path
00401094	text	00401094	1	C	SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\VED-PLD...
00401098	text	00401098	1	C	...

Functions window

Function name	Segment
sub_10001000	text
sub_10001074	text
sub_10001365	text
sub_10001656	text
sub_1000208F	text
sub_10002CCE	text
sub_10003555	text
sub_10003552	text
sub_10003695	text
sub_100036C3	text
sub_100036FE	text
sub_10003728	text
sub_100037E6	text
sub_100038B8	text
sub_100038E6	text
sub_10003950	text
sub_1000399A	text
sub_10003B75	text
sub_10003C00	text
sub_10003C20	text
sub_10003D43	text
sub_10003DC6	text
sub_10003E8C	text
sub_10004249	text
sub_100042D8	text
sub_1000470A	text
sub_10004721	text
sub_10004738	text
sub_1000493A	text
sub_10004A03	text
sub_10004A81	text
sub_10004B01	text
sub_10004B0D	text
sub_10004C23	text
sub_10004C56	text
sub_10004C5C	text
sub_10004CFF	text
sub_10004DCA	text

IDA ViewA

Strings window

HexViewA

Structures

Enum

Imports

Exports

```
xdoors_d:10093D34 db '(2) Get DLL FileName ',27h,'3s',27h,0
xdoors_d:10093D50 ; char a1EnterCurrentD[]
xdoors_d:10093D50 a1EnterCurrentD db 00h,00h ; DATA XREF: sub_1000A2D0+1210
xdoors_d:10093D50 db '(1) Enter Current Directory ',27h,'3s',27h,0
xdoors_d:10093D73 align 4
xdoors_d:10093D74 ; char aBackdoorServer[]
xdoors_d:10093D74 aBackdoorServer db 00h,00h ; DATA XREF: sub_1000A2D0+B510
xdoors_d:10093D74 db 00h,00h
xdoors_d:10093D74 db '*****',00h,00h
xdoors_d:10093D74 db '[Backdoor Server Update Setup]',00h,00h
xdoors_d:10093D74 db '*****',00h,00h
xdoors_d:10093D74 db 00h,00h,0
xdoors_d:10093D80 align 4
xdoors_d:10093D80 ; char aWarn[]
xdoors_d:10093D80 aWarn db '-warn',0 ; DATA XREF: sub_1000A738+19810
xdoors_d:10093DE2 align 4
xdoors_d:10093DE2 ; char aErro[]
xdoors_d:10093DE2 aErro db '-erro',0 ; DATA XREF: sub_1000A738+18710
xdoors_d:10093DE4 align 4
xdoors_d:10093DE4 ; char aStop[]
xdoors_d:10093DE4 aStop db '-stop',0 ; DATA XREF: sub_1000A738+17610
xdoors_d:10093DE2 align 4
xdoors_d:10093DE2 ; char aShutdown_0[]
xdoors_d:10093DE2 aShutdown_0 db '-shutdown',0 ; DATA XREF: sub_1000A738:loc_1000A8710
xdoors_d:10093DE2 align 10h
xdoors_d:10093E00 ; char Caption[]
xdoors_d:10093E00 Caption db '0+0',0 ; DATA XREF: sub_1000A738+10710
xdoors_d:10093E00 ; sub_1000A738+10010
xdoors_d:10093E00 align 4
xdoors_d:10093E00 ; char aReboot_0[]
xdoors_d:10093E00 aReboot_0 db '-reboot',0 ; DATA XREF: sub_1000A738+ED10
xdoors_d:10093E10 ; char szDesktop[]
xdoors_d:10093E10 szDesktop db 'Default',0 ; DATA XREF: sub_1000A738+5910
xdoors_d:10093E10 ; StartEX+24410 ...
xdoors_d:10093E10 ; char szWinSta[]
xdoors_d:10093E10 szWinSta db 'WinSta0',0 ; DATA XREF: sub_1000A738+3010
xdoors_d:10093E20 ; char aWinStaDefault[]
xdoors_d:10093E20 aWinStaDefault db 'winsta0\default',0 ; DATA XREF: sub_1000A803+5D10
xdoors_d:10093E20 ; sub_1000A801+5D10
xdoors_d:10093E30 ; char aExplorer_exe[]
xdoors_d:10093E30 aExplorer_exe db 'EXPLORER.EXE',0 ; DATA XREF: sub_1000A803+1110
xdoors_d:10093E30 ; sub_1000A801+1110
xdoors_d:10093E30 align 10h
xdoors_d:10093E40 ; char aSIexplorer_exe[]
xdoors_d:10093E40 aSIexplorer_exe db 'SIEXPLORER.EXE',0 ; DATA XREF: sub_1000A801+9910
xdoors_d:10093E50 ; char aPath[]
```

}