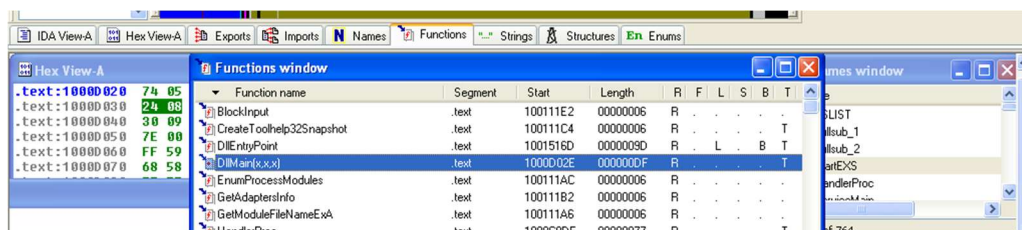
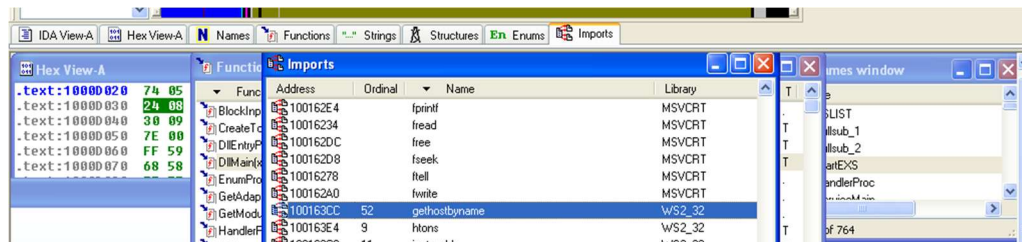


Identificazione dell'indirizzo della funzione **dllmain**.

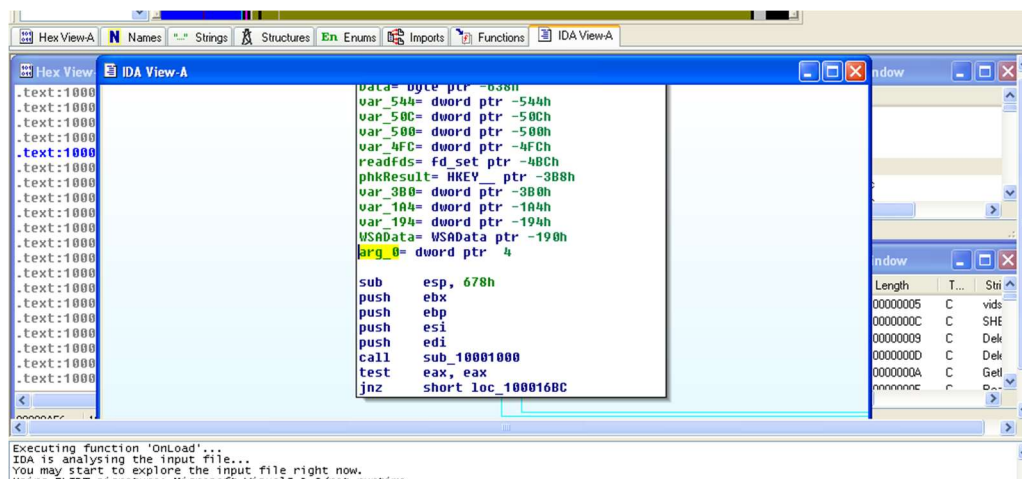
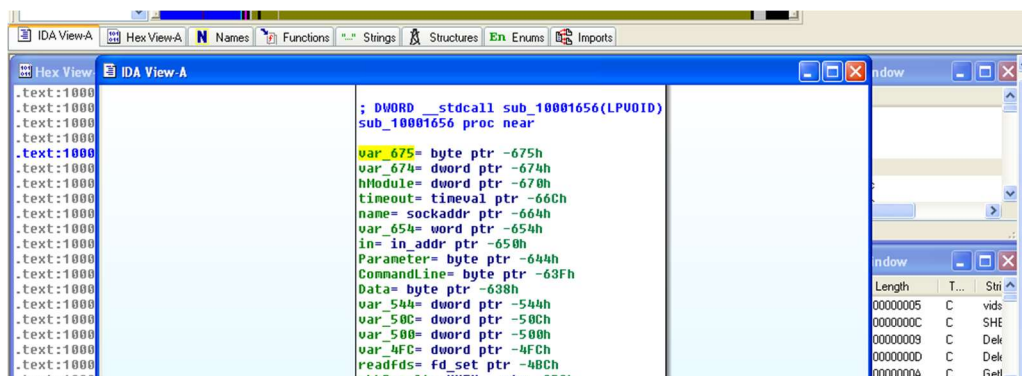


Identificazione della funzione **gethostbyname**.



Variabili e parametri della funzione in locazione di memoria a **0x10001656**.

Le variabili locali hanno un **offset negativo**, mentre il parametro ha **offset positivo**.



Tecniche di evasione e persistenza: Il malware è dotato di alcuni check che gli permettono di comprendere se viene eseguito in un ambiente virtualizzato; in caso positivo è programmato per cancellarsi automaticamente. La persistenza invece avviene attraverso la modifica del servizio **SVCHOST**.

Text	Process	PID	Operation	Path
.text:1000	xdoors_...	00000000	C	0.0.0.0
.text:1000	xdoors_...	0000001E	C	Microsoft TV/Video Connection
.text:1000	xdoors_...	00000020	C	VMware Virtual Ethernet Adapter
.text:1000	xdoors_...	00000011	C	Fail To Send[\r\n
.text:1000	xdoors_...	00000006	C	%s %s
.text:1000	xdoors_...	nnnnnnnq	C	Rev []]
.text:1000	xdoors_...	00000000	C
.text:1000	xdoors_...	0000001C	C	\r\n\r\n(Language:) id:0x\r\n\r\n\r\n
.text:1000	xdoors_...	00000051	C	\r\n[Install Log:] %d\r\n[Detect VM :] %d\r\n[SSDT Ring3:] %d\r\n[SSDT ...
.text:1000	xdoors_...	00000054	C	\r\n[Host connect Type :] %d\r\n[Host Reconnect Time:] %d\r\n[CURL Re...
.text:1000	xdoors_...	nnnnnnn?	C	V:\WINDOWS\NAME-1
.text:1000	xdoors_...	00000004	C	Get /set /val
.text:1000	xdoors_...	0000001E	C	if exist \"%s\" goto selfkill\r\n
.text:1000	xdoors_...	00000008	C	del \"%s\" \r\n
.text:1000	xdoors_...	0000001A	C	attrib -a -r -s -h \"%s\" \r\n
.text:1000	xdoors_...	0000000C	C	:selfkill\r\n
.text:1000	xdoors_...	0000000C	C	@echo off\r\n
.text:1000	xdoors_...	00000010	C	.\vmselfdel.bat
.text:1000	xdoors_...	00000008	C	kstartype
.text:1000	xdoors_...	00000019	C	CreateToolhelp??Snapshot

The screenshot displays the Immunity Debugger interface during a malware analysis session. The primary focus is on the Network tab, which lists several captured packets. Key details include:

- Packet 1:** Offset 0x00000007, Length 0x00000007, Protocol C, Details: FTP://
- Packet 2:** Offset 0x00000010, Length 0x00000010, Protocol C, Details: Content-Length: 115
- Packet 3:** Offset 0x00000012, Length 0x00000012, Protocol C, Details: [This is RNA]pics
- Packet 4:** Offset 0x0000002E, Length 0x0000002E, Protocol C, Details: [This is RDP]pics.practicalmalwareanalysis.com
- Packet 5:** Offset 0x0000004F, Length 0x0000004F, Protocol C, Details: [This is RIP]
- Packet 6:** Offset 0x00000010, Length 0x00000010, Protocol C, Details: [This is RPO]80
- Packet 7:** Offset 0x00000014, Length 0x00000014, Protocol C, Details: [This is DVM]
- Packet 8:** Offset 0x00000014, Length 0x00000014, Protocol C, Details: [This is SS2]
- Packet 9:** Offset 0x00000014, Length 0x00000014, Protocol C, Details: [This is SSD]
- Packet 10:** Offset 0x0000000F, Length 0x0000000F, Protocol C, Details: [This is LOG]0
- Packet 11:** Offset 0x00000010, Length 0x00000010, Protocol C, Details: [This is NTI]30
- Packet 12:** Offset 0x0000000D, Length 0x0000000D, Protocol C, Details: [This is CTI]
- Packet 13:** Offset 0x00000005, Length 0x00000005, Protocol C, Details: DAV

Below the network list, a console window shows the execution of various functions, including 'OnLoad' and 'Exit'. The bottom status bar indicates 'Line 483 of 746'.