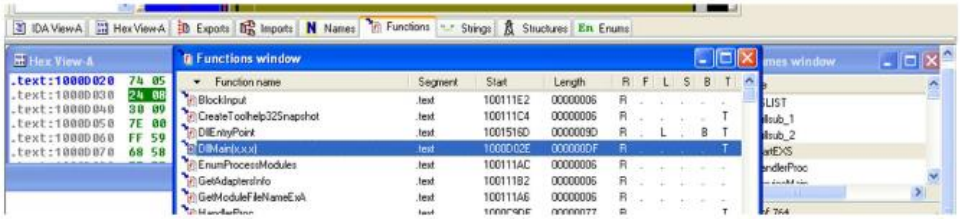
M6 D6

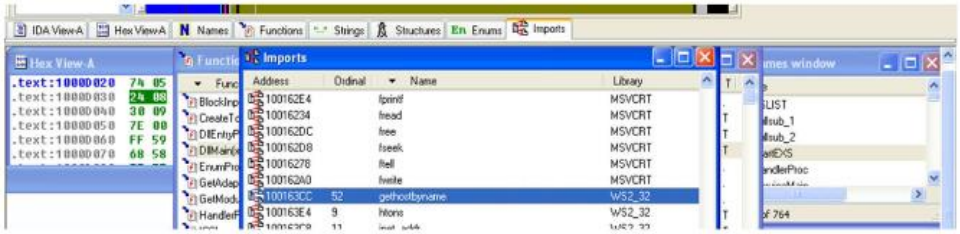
ESERCIZIO

ANALISI STATICA AVANZATA CON IDA

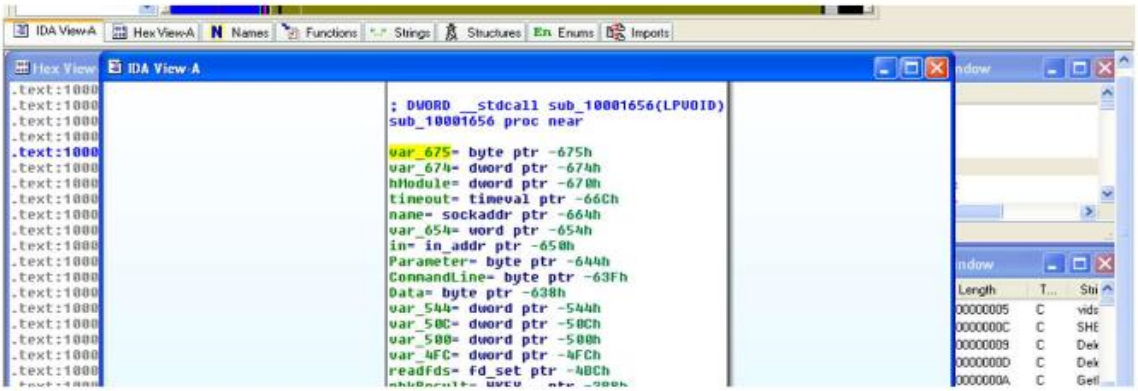
Identificazione dell'indirizzo della funzione **dllmain**.

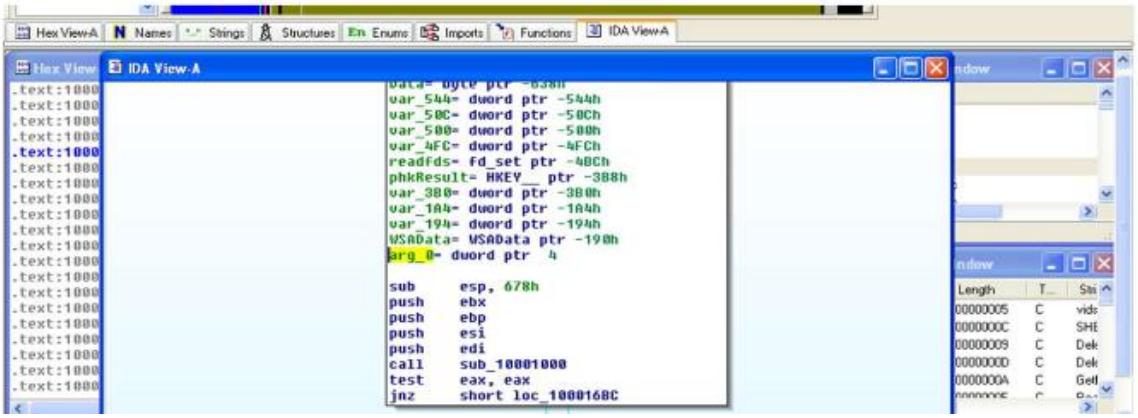


Identificazione della funzione **gethostbyname**.



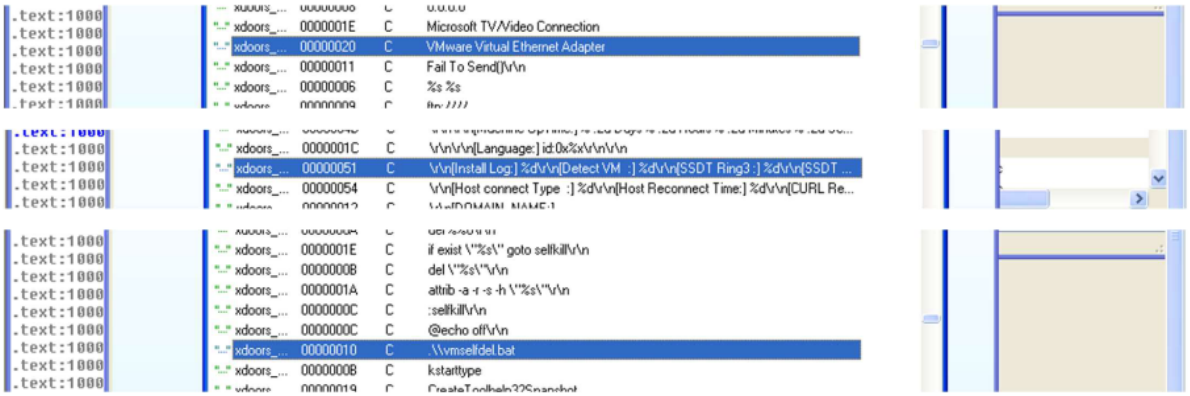
Variabili e parametri della funzione in locazione di memoria a **0x10001656**.
Le variabili locali hanno un **offset negativo**, mentre il parametro ha **offset posivito**.



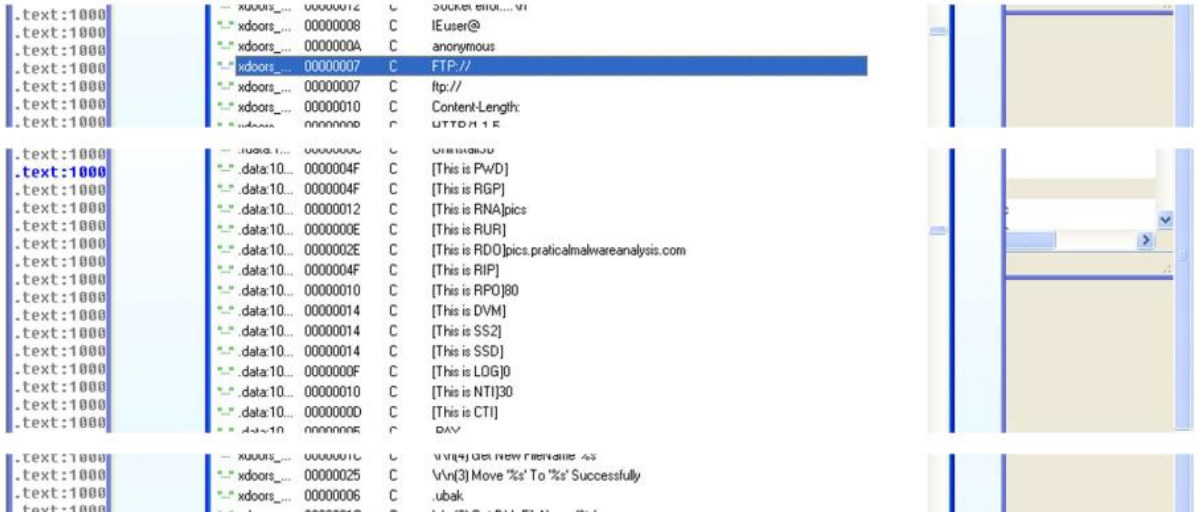


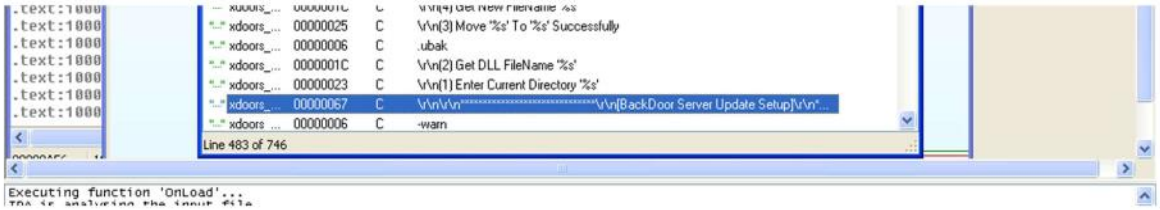
Da un'analisi più approfondita del codice decompilato si possono ricavare molte informazioni riguardo alla tipologia e al funzionamento del malware.

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**.



Tipologia: Dall'analisi si può notare che il malware è capace di prendere il controllo della rete attraverso una process injection, andando ad intaccare sia il processo **IEXPLORE.exe** che il servizio **FTP** in funzione sulla macchina e creando infine una **backdoor**. Tra le altre cose visibili dal codice è possibile ipotizzare che il malware sia in grado, probabilmente grazie ad una shell, di acquisire audio/video e prendere controllo dei processi della macchina bersaglio.




.text:1000
xdoors_... 00000025 C \r\n(3) Move '%s' To '%s' Successfully
xdoors_... 00000006 C .ubak
xdoors_... 0000001C C \r\n(2) Get DLL FileName '%s'
xdoors_... 00000023 C \r\n(1) Enter Current Directory '%s'
xdoors_... 00000067 C \r\n\r\n**********\r\n[BackDoor Server Update Setup]\r\n*...
xdoors_... 00000006 C -warn
Line 483 of 746
Executing function 'OnLoad'...


.text:1000
xdoors_... 00000008 C enmagic
xdoors_... 00000005 C exit
xdoors_... 00000005 C quit
xdoors_... 00000011 C \\command.exe /c
xdoors_... 0000000D C \\cmd.exe /c
xdoors_... 00000118 C Hi,Master [%d/%d/%d %d:%d:%d]\r\nWelCome Back...Are You Enjoying To...
Line 746 of 746