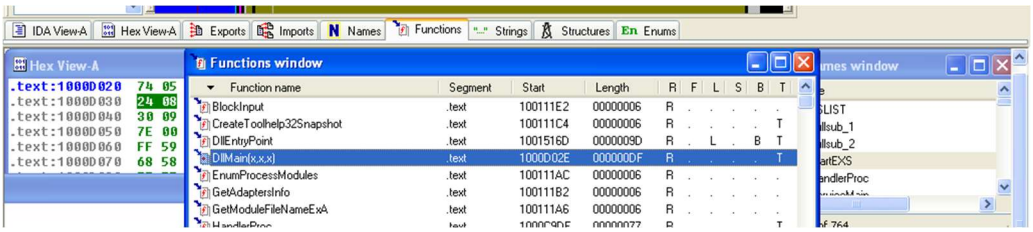
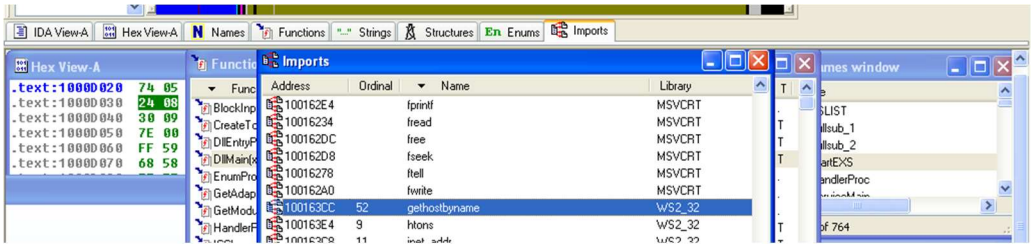
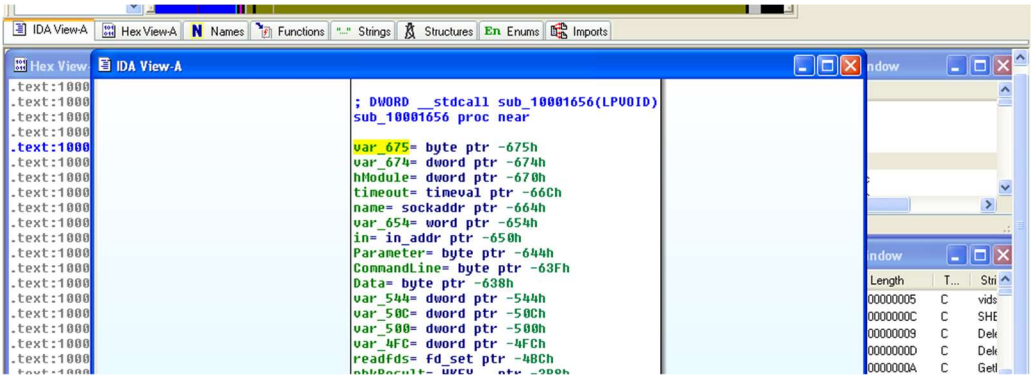
Identificazione dell'indirizzo della funzione **dllmain**.

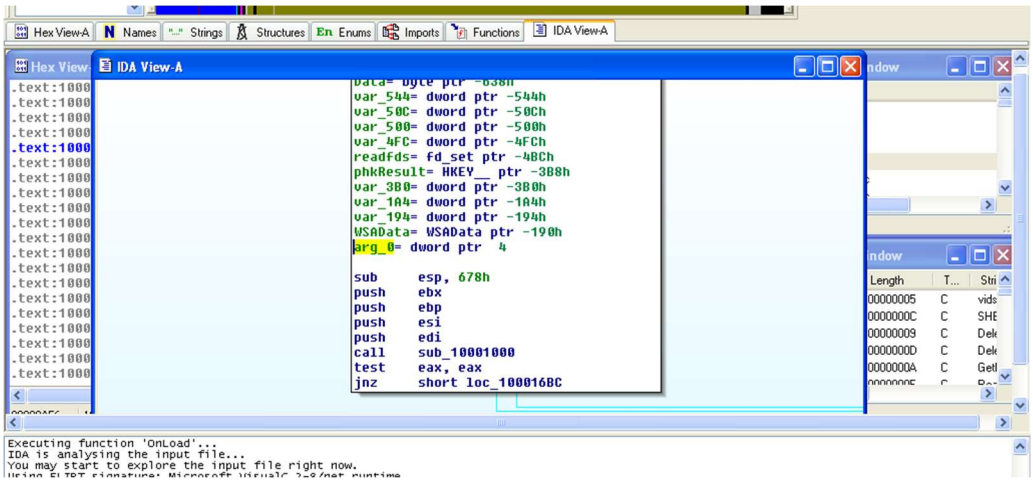


Identificazione della funzione **gethostbyname**.



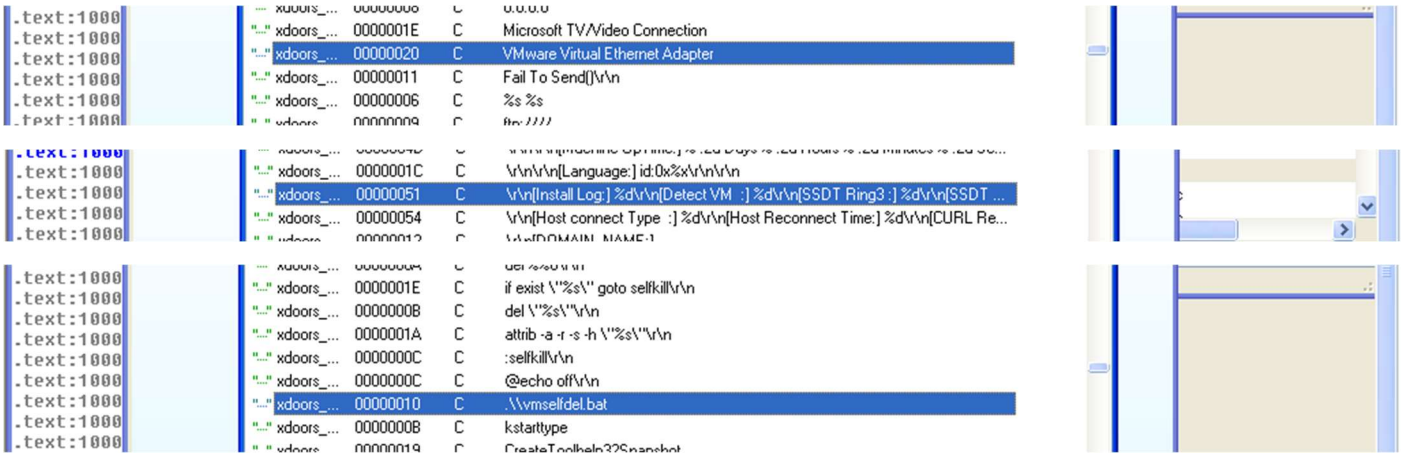
Variabili e parametri della funzione in locazione di memoria a **0x10001656**.
Le variabili locali hanno un **offset negativo**, mentre il parametro ha **offset posivito**.





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.