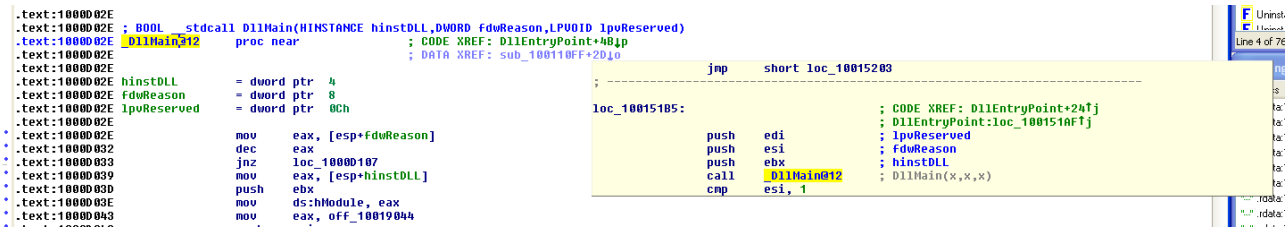
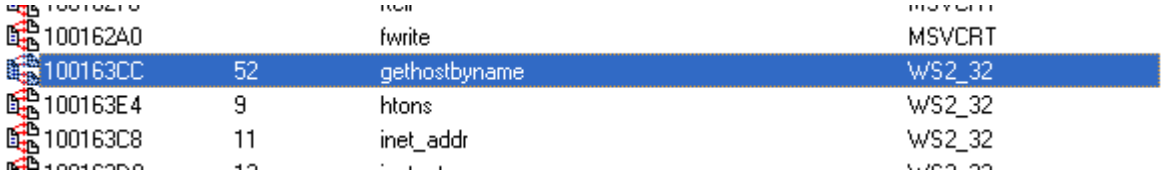
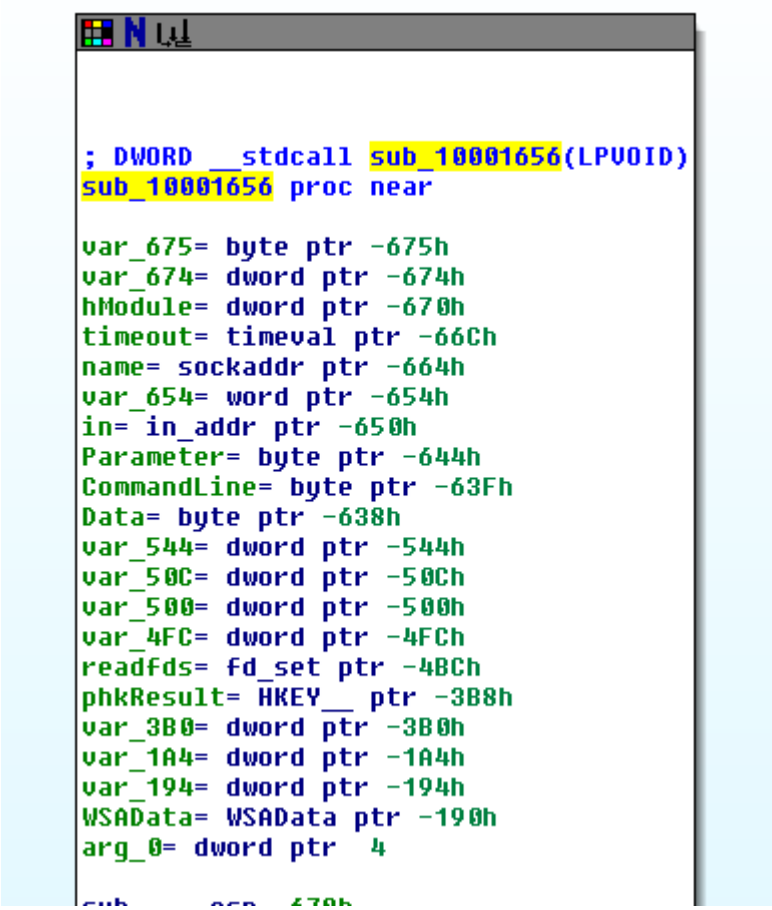
- Individuazione della funzione DLLmain

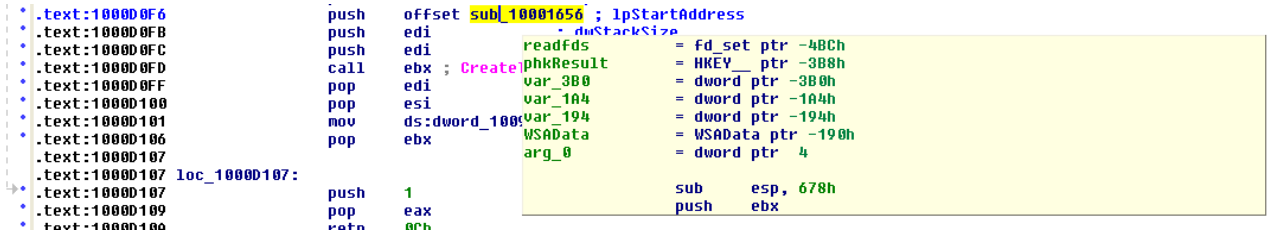


- Individuazione della funzione gethostbyname



- Individuazione delle variabili alla locazione di memoria 0x10001656





Considerazioni finali

Il Malware va ad intaccare i seguenti servizi:

IEXPLORE.exe e FTP

Inoltre crea una backdoor nel sistema.

Dal prossimo screen è possibile vedere inoltre come il malware sia programmato per controllare se l'ambiente in cui viene eseguito è una macchina virtuale o meno.