-Analisi del Malware_U3_L2 utilizzando il tool IDA pro

1-Individuare l'indirizzo della funzione DLLMain
2-Dalla scheda <<imports>> individuare la funzione <<gethostbyname>> quale e' l'indirizzo dell'import?Cosa fa' la funzione?
3-Quante sono le variabili locali della funzione alla locazione memoria 0x10001656?
4-Quanti sono invece i parametri della funzione sopra?
5-Inserire altre considerazioni sul comportamento del malware

1-Per trovare L'indirizzo della funzione DLLMain utilizzeremo il tool IDA Pro e quindi caricando qui il Malware_U3_L2,utilizzeremo questo strumento per recuperare l'indirizzo della funzione main che sara':1000D02E.

BOOL__stdcall DLLMain(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpvReserved)

Un'entrata opzionale nel link della libreria dinamica DLL.Quando il sistema avvia o termina un processo o thread,chiama la funzione in punto di entrata per ogni DLL caricata usando il primo thread del processo.Il sistema chiama anche in punto di entrata per un DLL quando e' caricato o scaricato usando le funzioni LoadLibrary e FreeLibrary.
-HINSTANCE hinstDLL:handle to DLL module
-DWORD fdwReason:reason for calling function
-LPVOID lpvReserved:reserved

-PARAMETRI

-hinstDLL
HinstDLL e' un handle per il modulo DLL.Il valore e' l'indirizzo base del DLL.L'HINSTANCE del DLL e' uguale al HMODULE del DLL,quindi hinstDLL puo' essere usato per la chiamata di funzione che richiede un modulo handle.

-fdwReason
E' la ragione per cui il codice indica perche'la funzione in punto di entrata DLL e' chiamata.

-lpvReserved
Se fdwReason e' un DLL_PROCESS_ATTACH,lpvdReserved sara' NULL per caricamenti dinamici e non-NULL per caricamenti statici.
Se fdwReason e' DLL_PROCESS_DETACH,lpvReserved sara' NULL se la Freelibrary e' stata chiamata oppure se il caricamento del DLL e' fallito e sara' non-NULL se il proceso sta' terminando.

2-Aprendo la finestra degli imports localizzeremo la funzione <<gethostbyname>> all'indirizzo 100163CC(la funzione gethostbyname recupera le informazioni host corrispondenti a un nome host da un database).

3-20 variabili con offset negativo rispetto ad EBP

4-L'unico parametro parametro avente offset positivo rispetto ad EBP nella funzione e' <<arg_0>>.

5-Il malware recupera le informazioni dell'HOST.