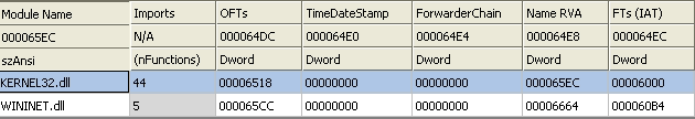
REPORT ANALISI MALWARE

In questo report verranno illustrati i passaggi atti a illustrare il funzionamento del seguente malware analizzato

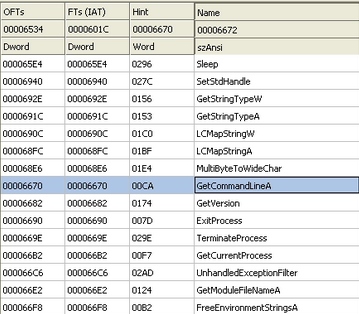
1.

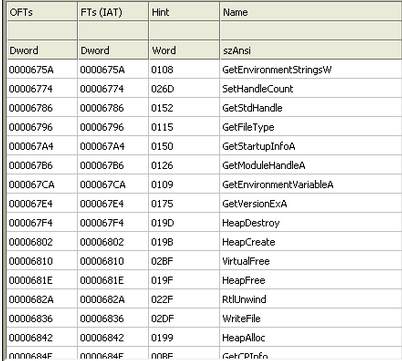
Le librerie caricate sono le seguenti KERNEL32.DLL e WININET.DLL

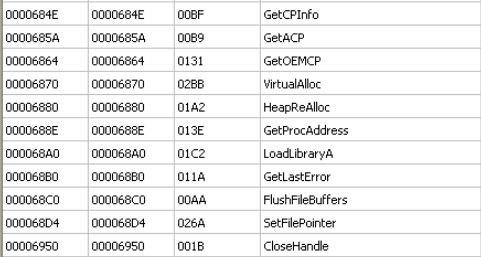
KERNEL32.DLL Contiene le funzioni principali per interagire con il sistema operativo ovvero manipolazione dei file e gestione della memoria.

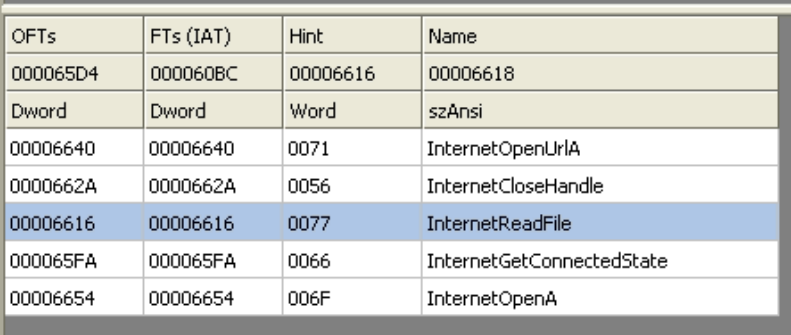
WININET.DLL Si occupa invece della gestione delle connessioni a internet

Nei seguenti screenshot sono raffigurate le istruzioni eseguite dalla libreria KERNEL32.DLL



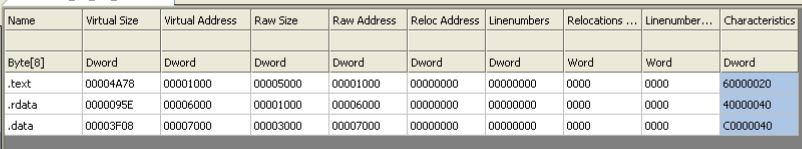






Queste sono le funzioni della libreria WININET32.DLL, che si occupano di creare una connessione ad internet verso la macchina vittima

2.

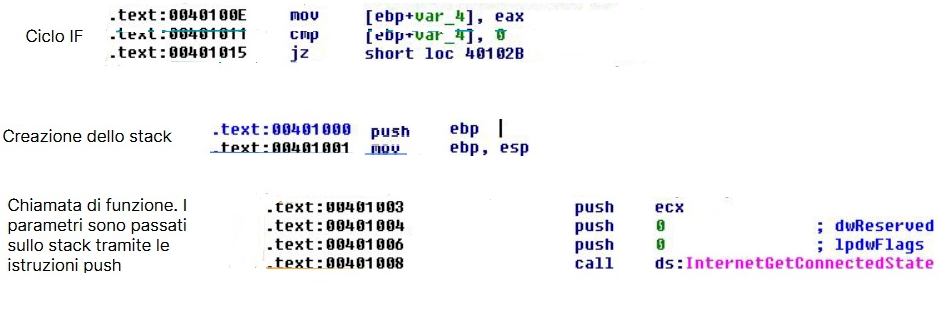


Qui sono raffigurate le sezioni di cui si compone il il malware ovvero:

.text: sezione che contiene righe di codice che la CPU eseguirà una volta avviato il software

.rdata: sezione che include informazioni riguardanti le librerie e le loro funzioni importate e poi esportate dall’eseguibile; .data: sezione che contiene le variabili globali e i dati del programma eseguibile, accessibili da qualsiasi funzione di esso.

3.



Nel seguente screenshot vengono identificati i costrutti noti

La funzionalità implementata all’interno del malware chiama la funzione internetgetconnectedstate. Se il valore è diverso da 0, significa che c’è una connessione attiva.

A giudicare dai comportamenti del malware, potrebbe trattarsi di un malware di tipo hijack, ovvero un malware in grado di rubare l’indirizzo ip della macchina vittima per poter eseguire attacchi Ddos, e reindirizza automaticamente la vittima alle pagine web malevoli scelte dagli attaccanti, quindi potrebbe trattarsi anche di un DRDOS. Inlotre si suppone sia una backdoor.