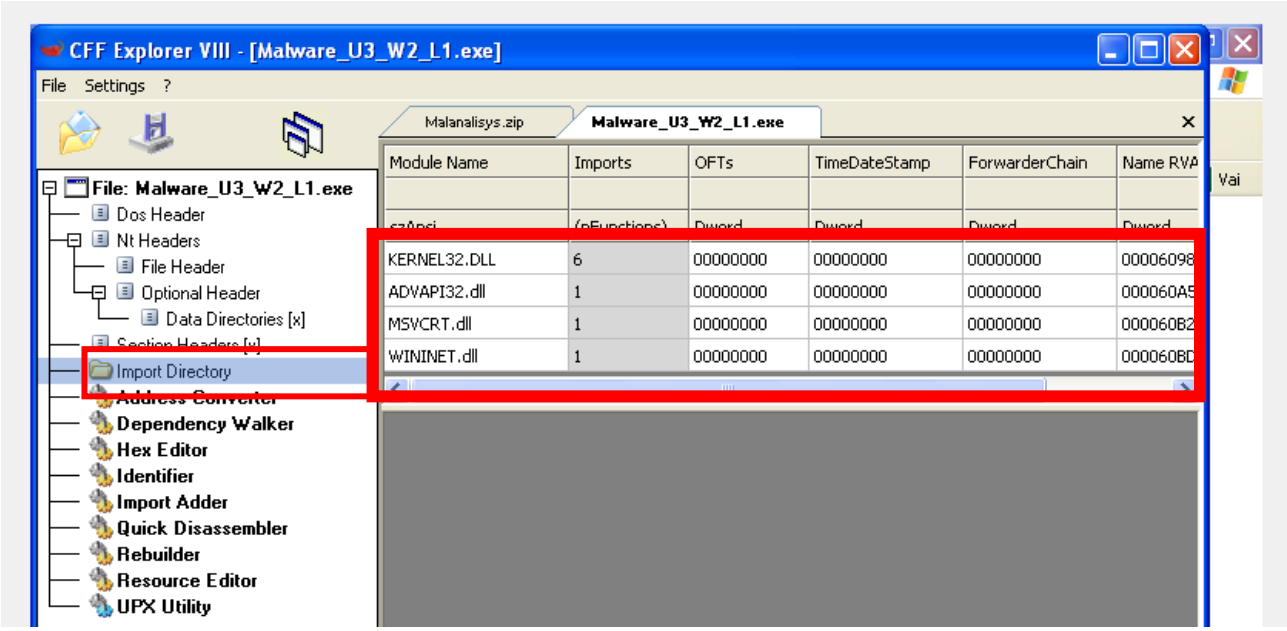
ANALISI STATICA BASICA

Ho aperto **CFF EXPLORER VIII**, selezionando la tab **IMPORT DIRECTORY** per vedere e librerie importate nel malware:

- **KERNEL32.DLL**: libreria usata per le funzioni principali per interagire con il sistema operativo. Un malware potrebbe sfruttare tale libreria per manipolare i file e per accedere la gestione della memoria
- **ADVAPI32.dll**: libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft, tramite la quale un malware potrebbe creare nuovi account utente, accedere al registro di sistema e crittografare o decrittografare dati sensibili;

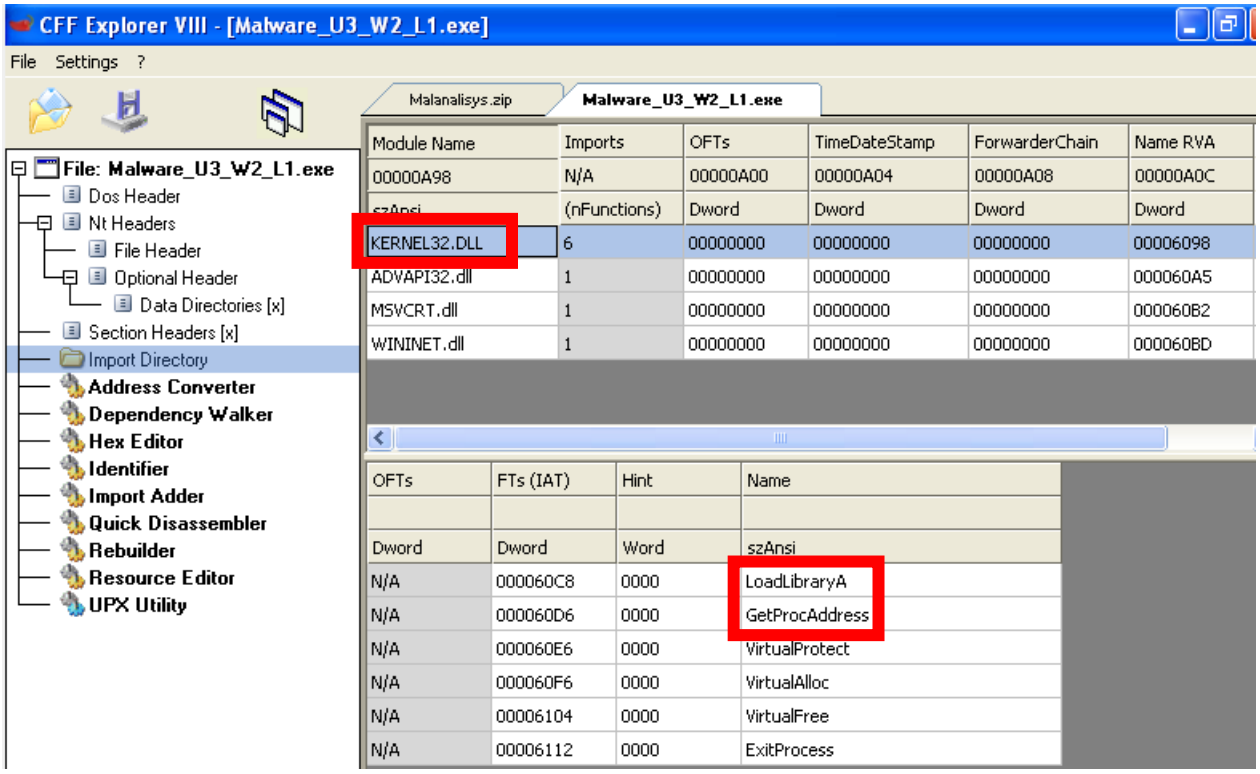
- **MSVCRT.dll:** libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C. Tramite questa libreria un malware potrebbe sfruttare delle vulnerabilità presenti o per eseguire codice malevolo;

- **WININET.dll:** libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come http, FTP, NTP. Un malware potrebbe sfruttare tale libreria per comunicare con server remoti, scaricare e caricare file, inviare dati sensibili…

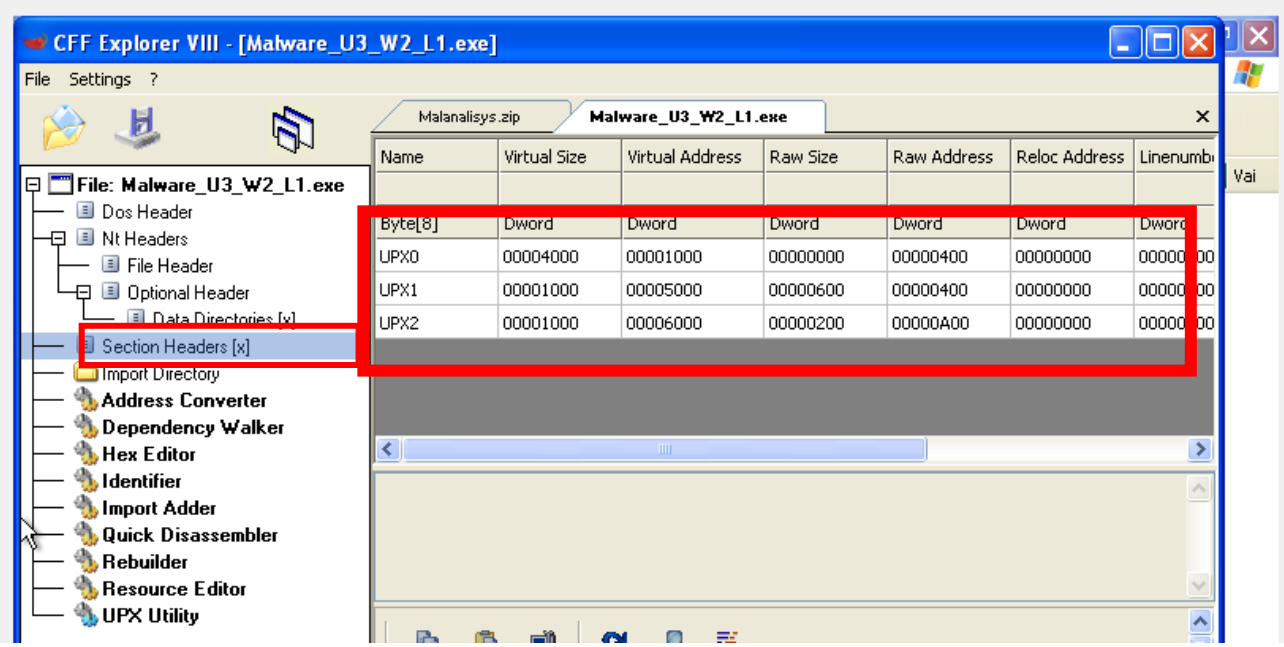


Selezionando la libreria KERNEL 32.DLL ho notato che al suo interno vi sono le funzioni **LoadLibraryA** e **GetProcAddress**, che permettono di importare le funzioni della libreria a **tempo di esecuzione (runtime**). **Ciò significa che l'eseguibile richiama la libreria solo quando ha bisogno di utilizzare una specifica funzione.**

Questo è un comportamento tipico dei malware, i quali, attraverso questo meccanismo, cercano di risultare meno invasivi e rilevabili.

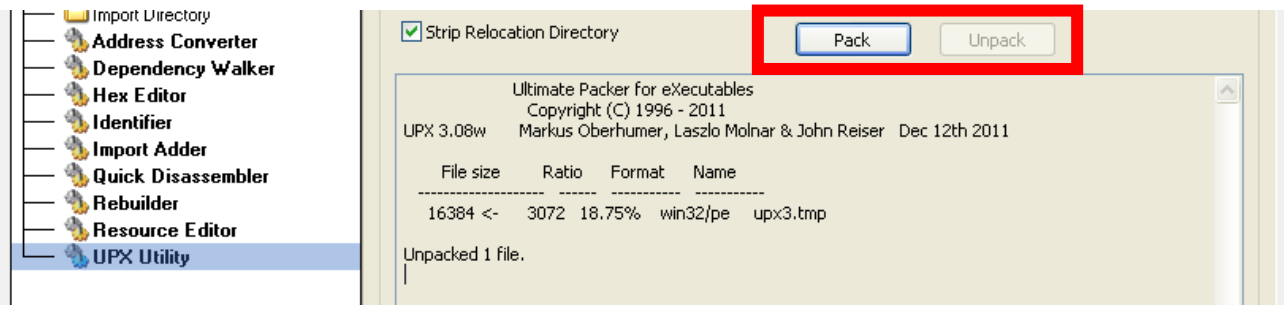


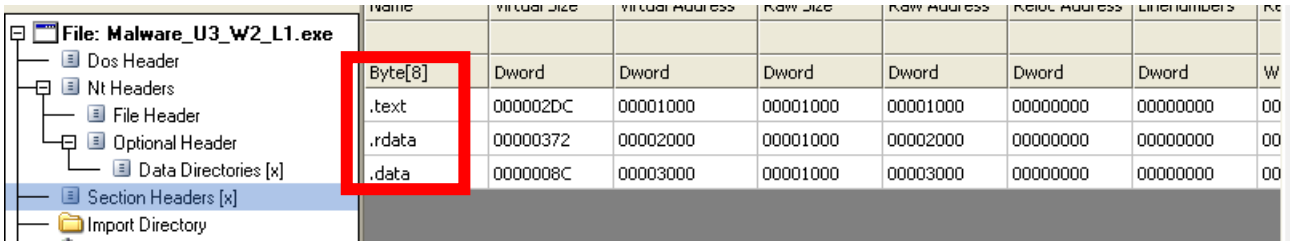
In seguito ho selezionato la tab **SECTION HEADERS**, dove ho identificato le sezioni **UPX0**, **UPX1** e **UPX2**.



Adesso spostiamoci sulla sezione **UPX Utiliity**: procedendo all'estrazione con "**unpack**" abbiamo accesso alle seguenti sezioni:

- **.text**: Questa sezione contiene le istruzioni, ovvero le righe di codice che la CPU eseguirà quando il software viene avviato. È la sezione principale di un file eseguibile, poiché contiene il codice effettivo che viene eseguito per far funzionare il programma. Tutte le altre sezioni contengono dati o informazioni di supporto per questa sezione.
- **.rdata**: Questa sezione contiene informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile. Qui vengono memorizzate le informazioni sui moduli esterni che l'eseguibile utilizza, come librerie di sistema o librerie condivise, e le funzioni che vengono importate o esportate per l'utilizzo all'interno del programma.
- **.data**: Questa sezione contiene dati e variabili globali del programma eseguibile. Le variabili definite in questa sezione sono accessibili da qualsiasi parte del programma, poiché sono globalmente dichiarate.

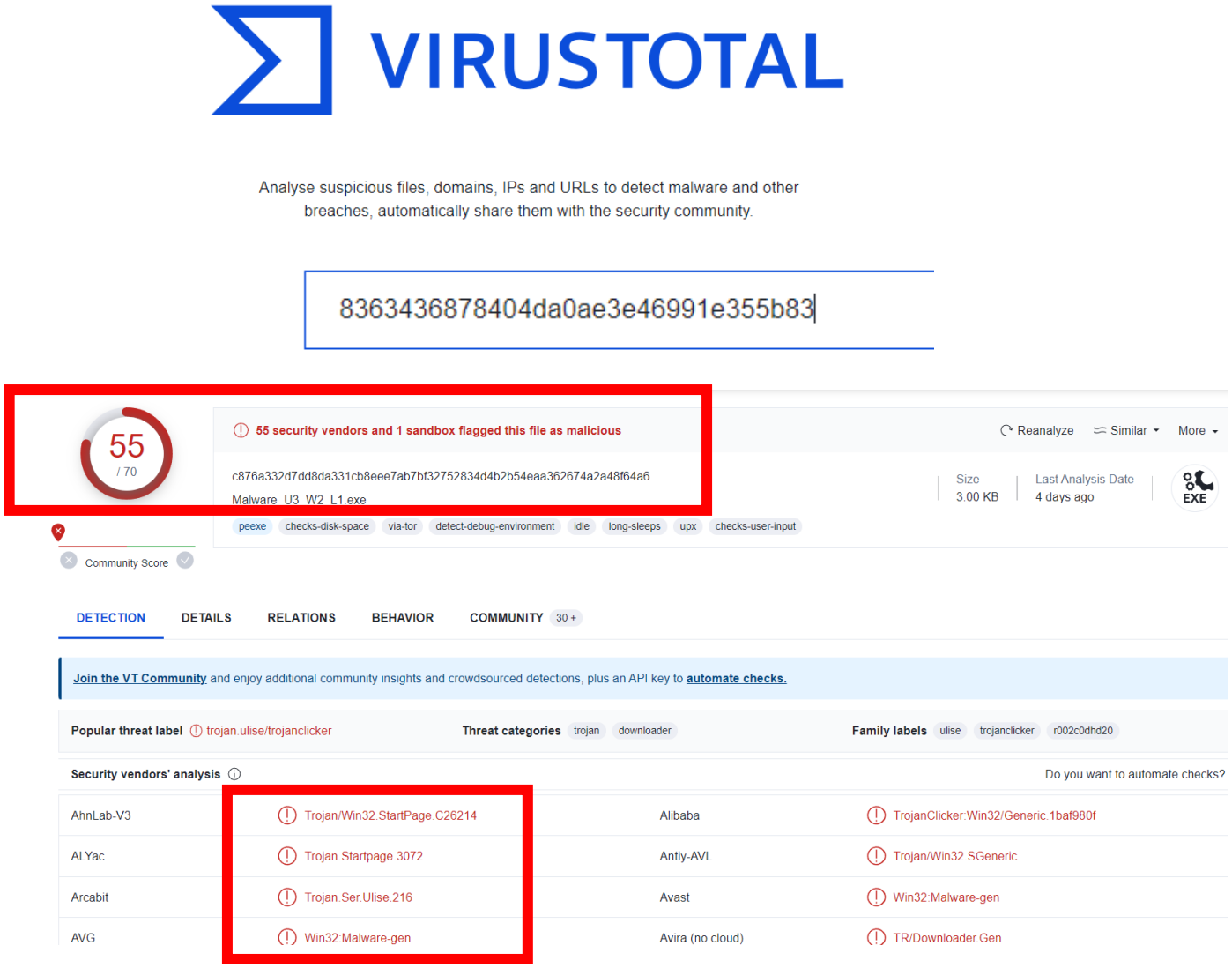




Ho scaricato md5deep su Windows XP, e tramite cmd ho preso l'hash del malware oggetto di interesse.

LINK DOWNLOAD: https://sourceforge.net/projects/md5deep/files/md5deep/md5deep-4.3/

Successivamente ho inserito su Virus Total l'hash ricavato grazie a MD5DEEP.



Risultato Virus Total: 53 vendors su 71 hanno identificato il malware come un tipo Trojan, comunicandoci per l'appunto la natura maligna del file oggetto di interesse.

Dai risultati delle analisi, possiamo trarre alcune conclusioni sul malware:

- Il malware è stato configurato **per utilizzare le connessioni di tipo HTTP/FTP/NTP** grazie all'importazione della libreria **Wininet.dll**. Questo suggerisce che **il malware potrebbe essere progettato per comunicare con server remoti, scaricare o caricare file o eseguire altre attività di rete utilizzando questi protocolli.**
- Il malware interagisce con il sistema operativo tramite la libreria **Kernel32.dll**. Questo indica che il malware utilizza funzioni di basso livello per accedere alle risorse del sistema, come la gestione dei file, la comunicazione con i processi e l'allocazione della memoria.
- L'analisi statica da sola non fornisce un quadro completo delle operazioni svolte dal malware. La presenza delle funzioni **LoadLibrary** e **GetProcAddress indica che il malware carica dinamicamente alcune funzioni durante l'esecuzione**. Pertanto, è necessaria un'analisi dinamica per ottenere ulteriori dettagli e osservare da vicino il comportamento del file.