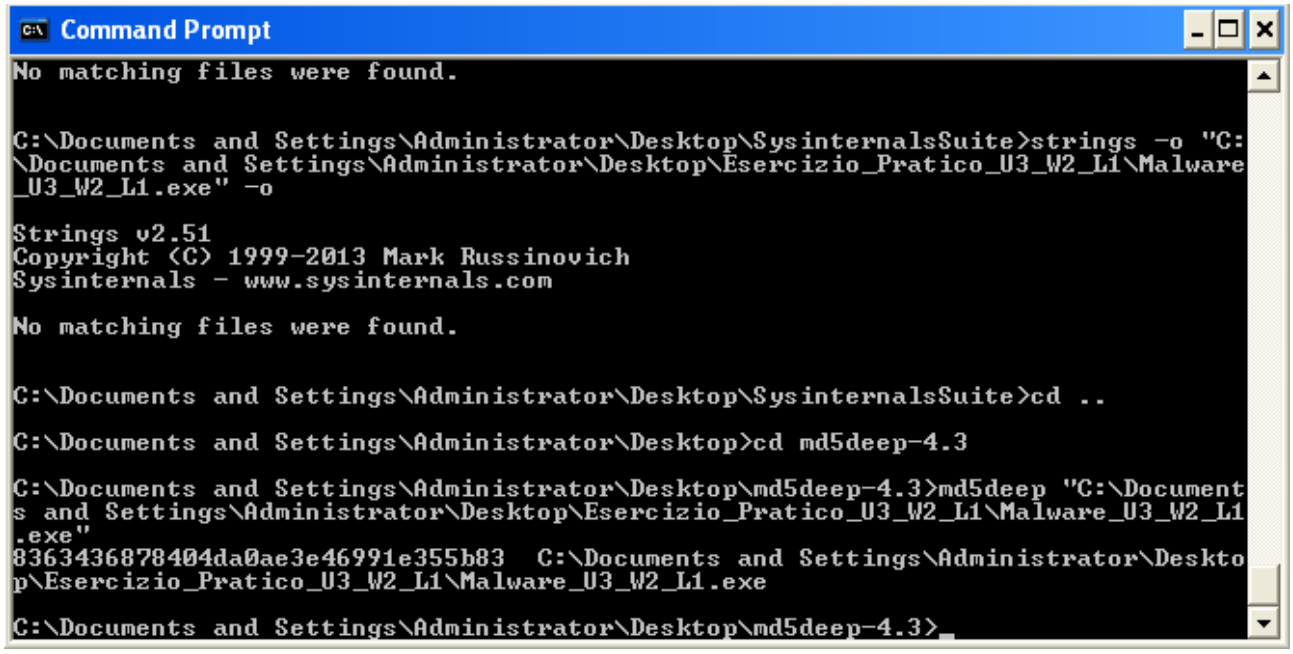
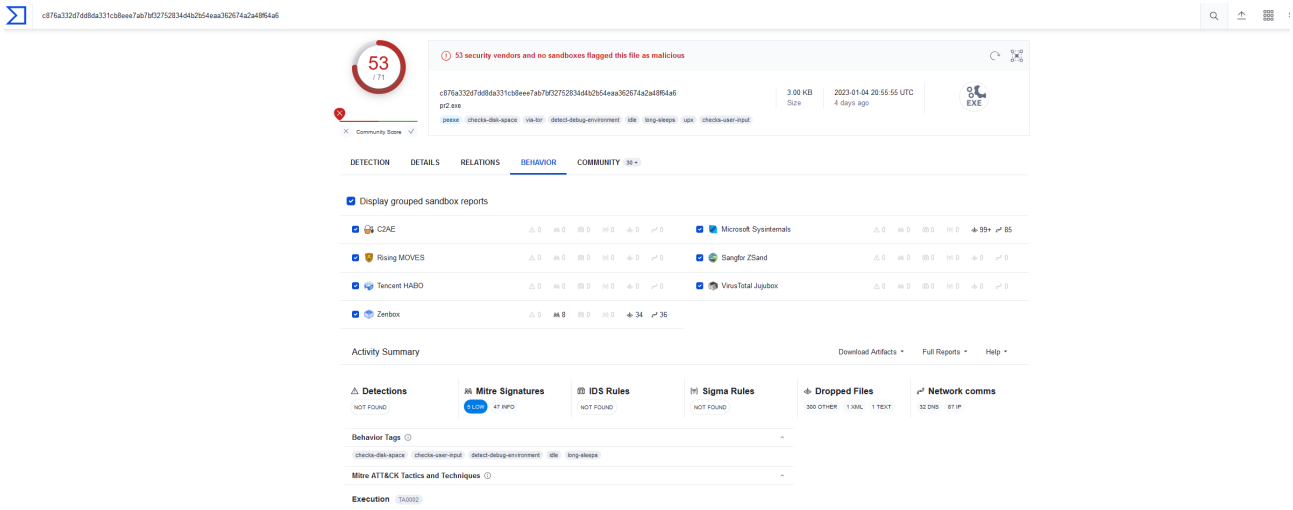
ANALISI STATICA BASICA

Recupero delle informazioni su un malware tramite l'analisi statica basica.

Quando si analizza un potenziali malware il primo passo da fare è di assicurarsi che sia di fatto un malware. Ogni file ha una propria firma di conseguenza anche i malware hanno una propria firma. Per calcolare l'hash di un file possiamo utilizzare l'utility "**md5deep**" presente sulla nostra macchina windows.



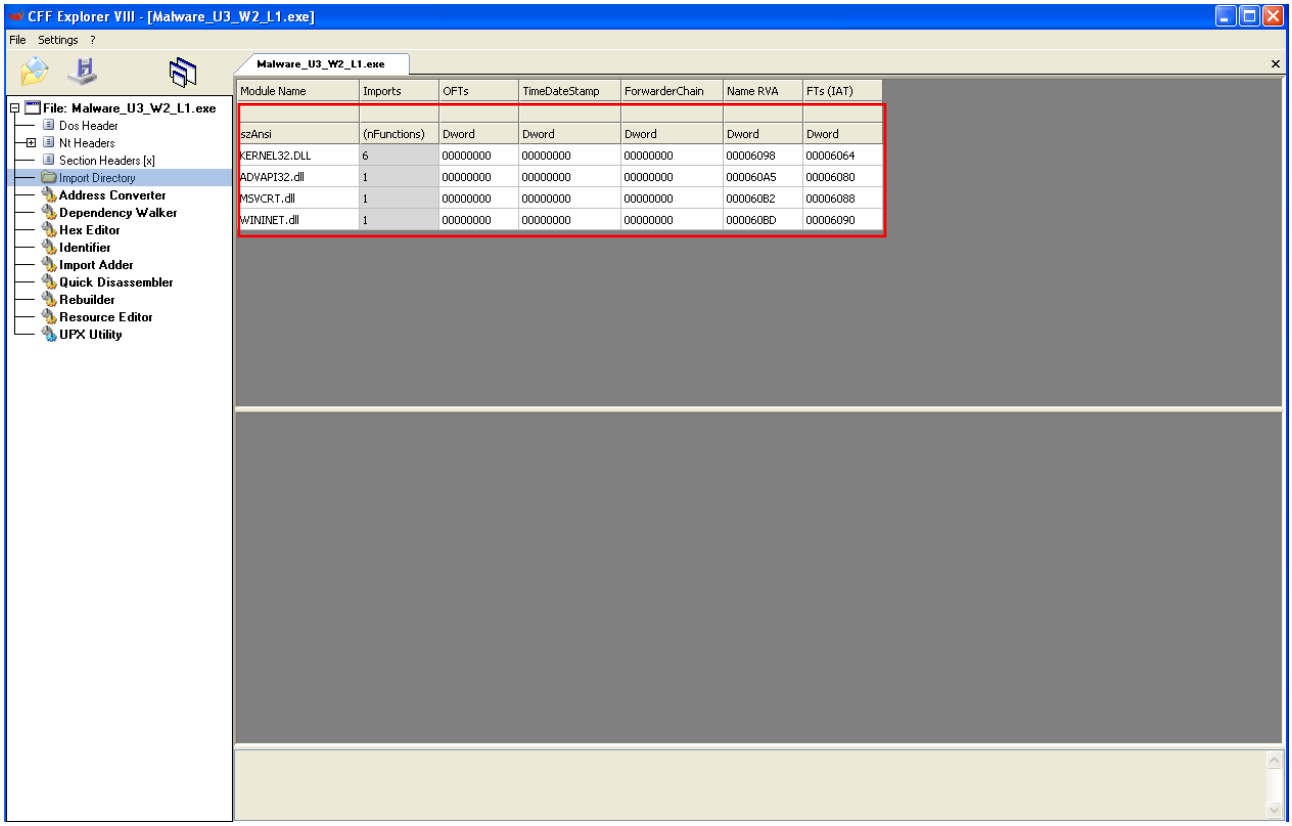
Hash file eseguibile viene inserita sul sito https://www.virustotal.com. La prima cosa che notiamo è lo score negativo. Da qui possiamo dedurre che il nostro file rappresenta un malware.



FASE 1

Nella prima parte delle analisi anndiamo a vedere quali tipi di librerie il nostro malware importa.

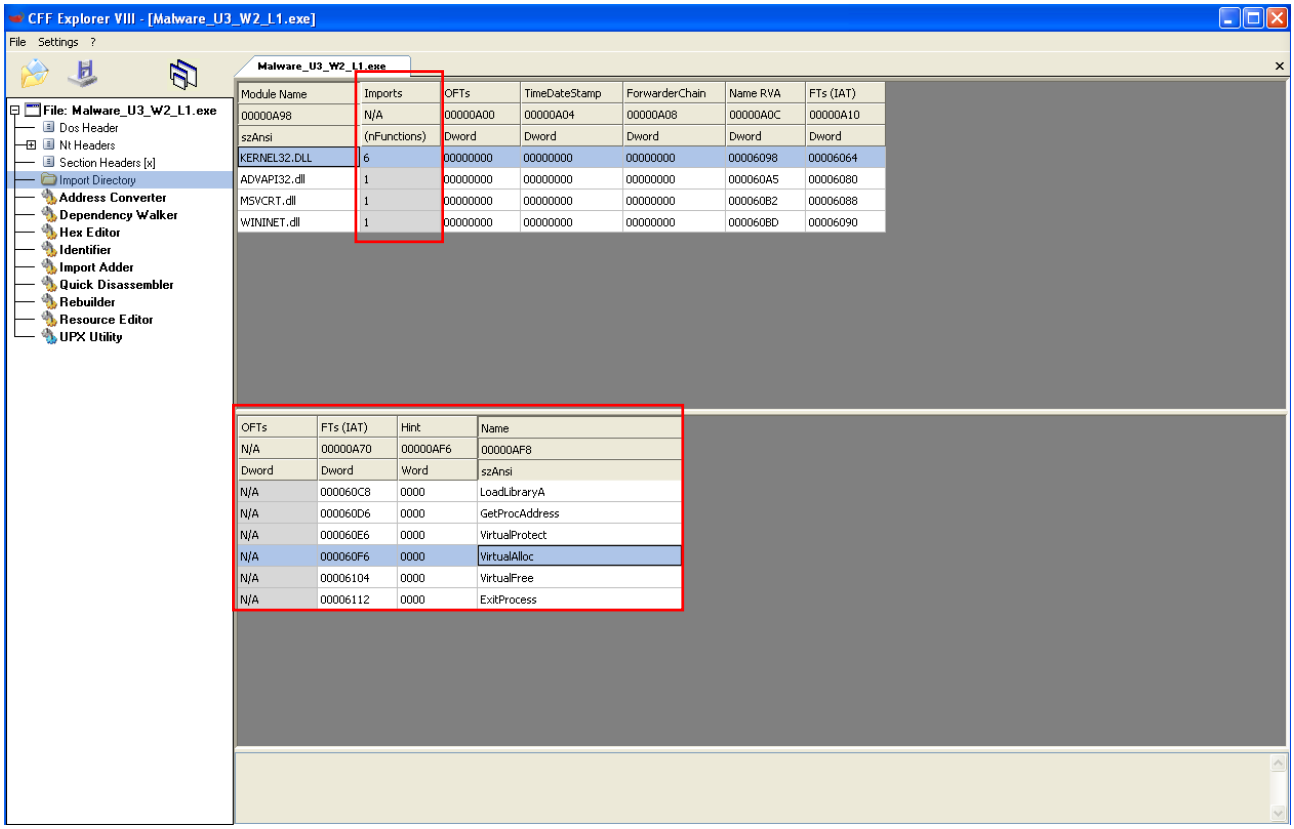
Grazie all'utility "**CFF Explorer**" possiamo analizzarle nel dettaglio.



LIBRERIE

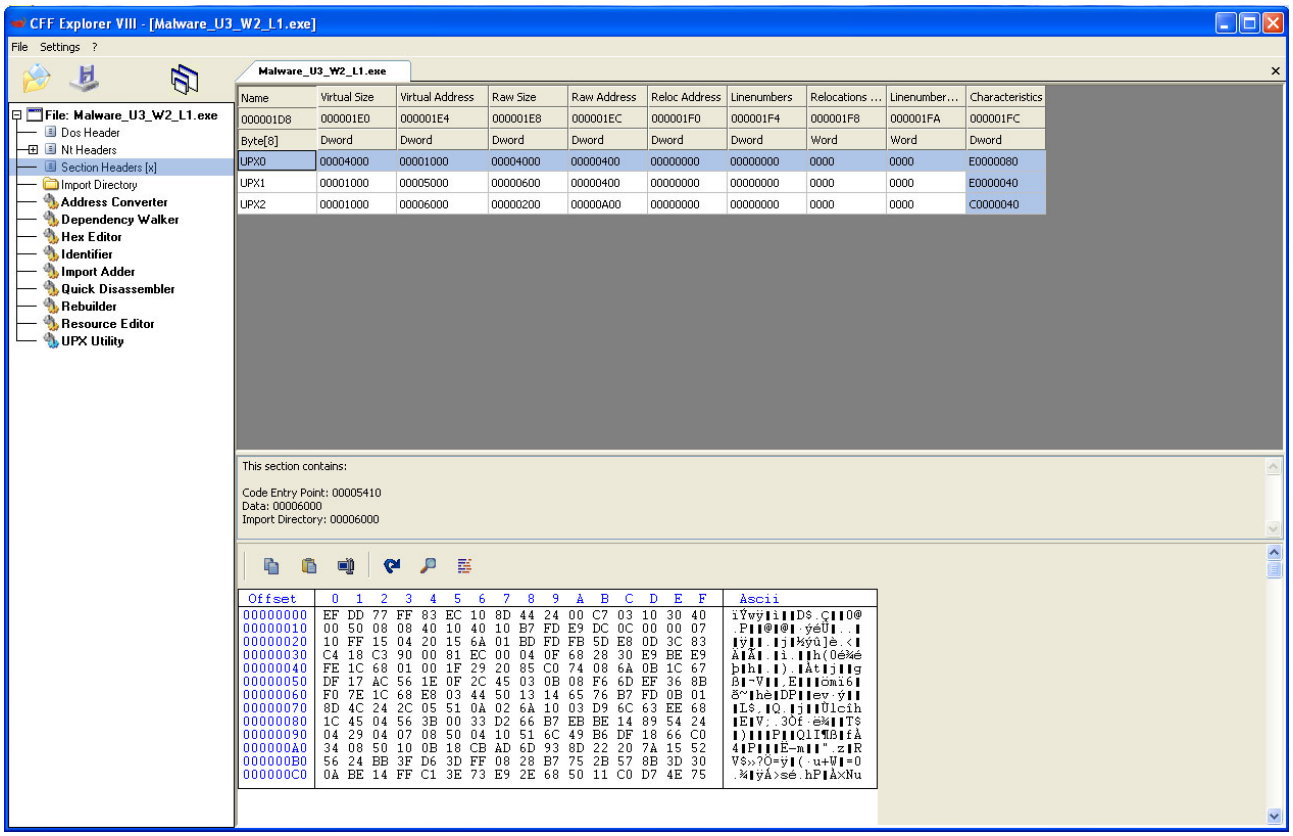
- **KERNELL32.DLL** – Libreria con funzioni principali per interagire con il Sistema Operativo
- **ADVAPI32-DLL** – Libreria con funzioni per interagire con servizi e registri del Sistema Operativo
- **MSVCRT.DLL** – Libreria con funzioni per allocazione di memoria, chiamate input/output
- **WINNET.DLL** - Libreria con funzioni per protocolli di rete HTTP/FTP/NTP

FASE 2

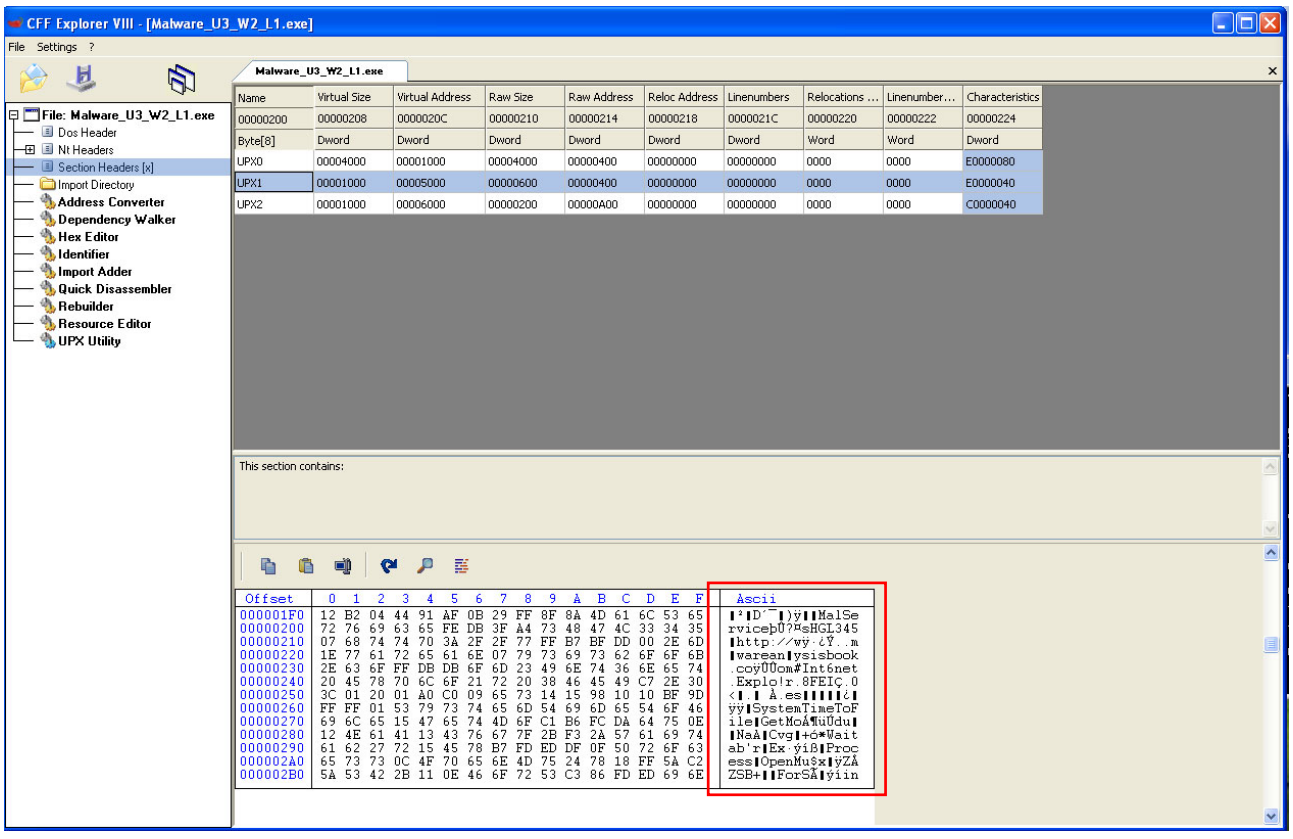


All’interno delle librerie possiamo vedere che tipi di funzioni il nostro malware può utilizzare.

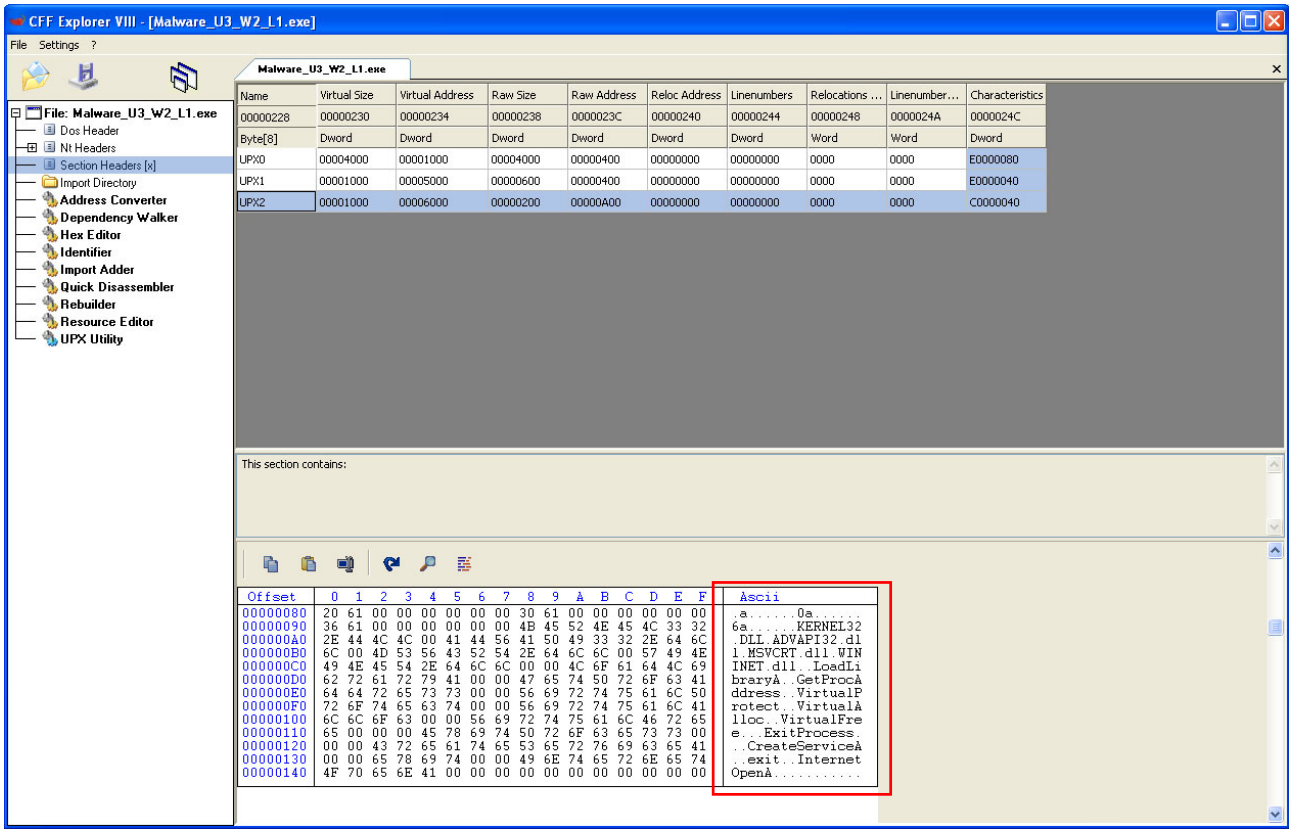
L'Header del formato PE ci fornisce altre informazioni. Qui possiamo vedere **UPX0 – UPX1 – UPX2**



Quelle che ci interessano sono **UPX1 – UPX2**



UPX1- **.data** – la sezione data contiene dati/variabili globali del programma. Le variabili globali non sono definite allì'interno di un contesto bensi sono disponibili da qualsiasi parte del programma



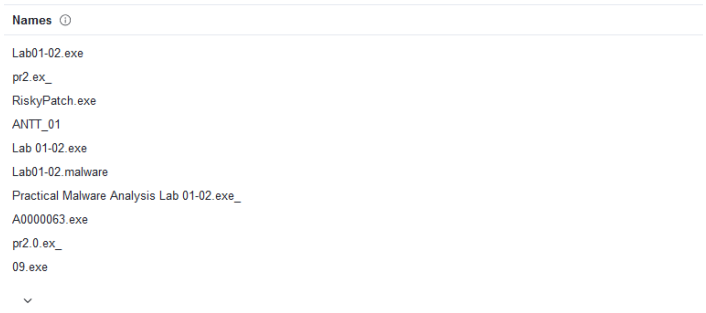
UPX2 - **.rdata** – richiamo alle librerie e alle funzioni importate dall'eseguibile

FASE 3

Una ricerca più approfondita su virus total ci permette di dire che il file analizzato è un **Trojan** (malware che si nasconde all'interno di un altro programma apparentemente utile e innocuo. L'utente, eseguendo o installando quest'ultimo programma, attiva inconsapevolmente anche il codice del trojan nascosto)

Possiamo vedere che al suo interno ha delle librerie che permettono di modificare grafica, registri di sistemi, protocolli di rete.

MD5 – Virus Total - https://www.virustotal.com/gui/file/c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6/details



Altri nomi con cui è stato "segnalato"