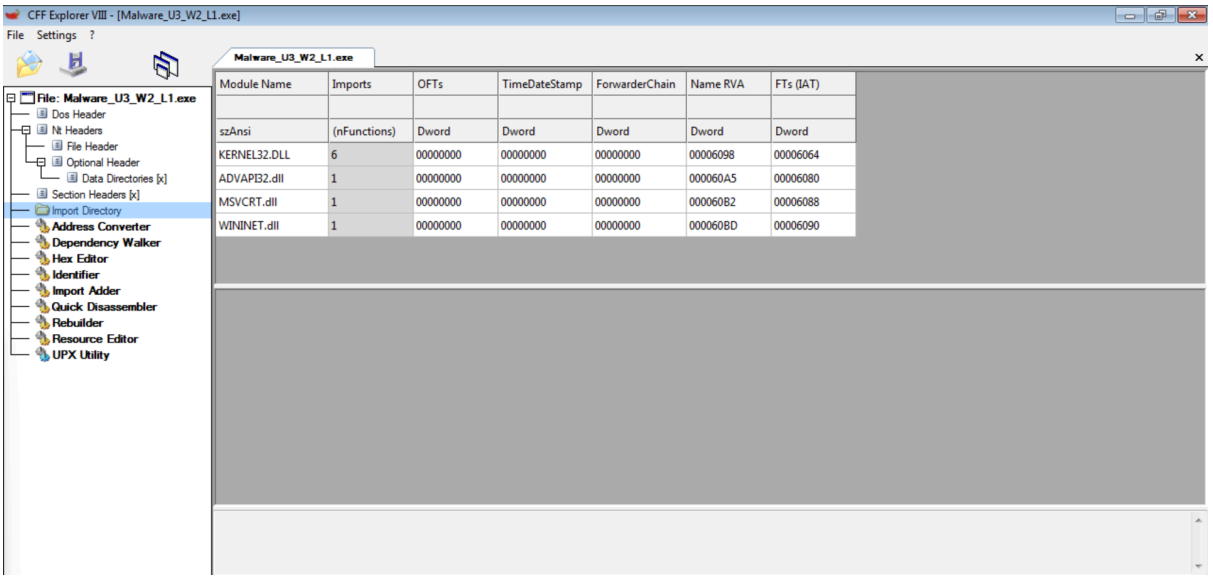
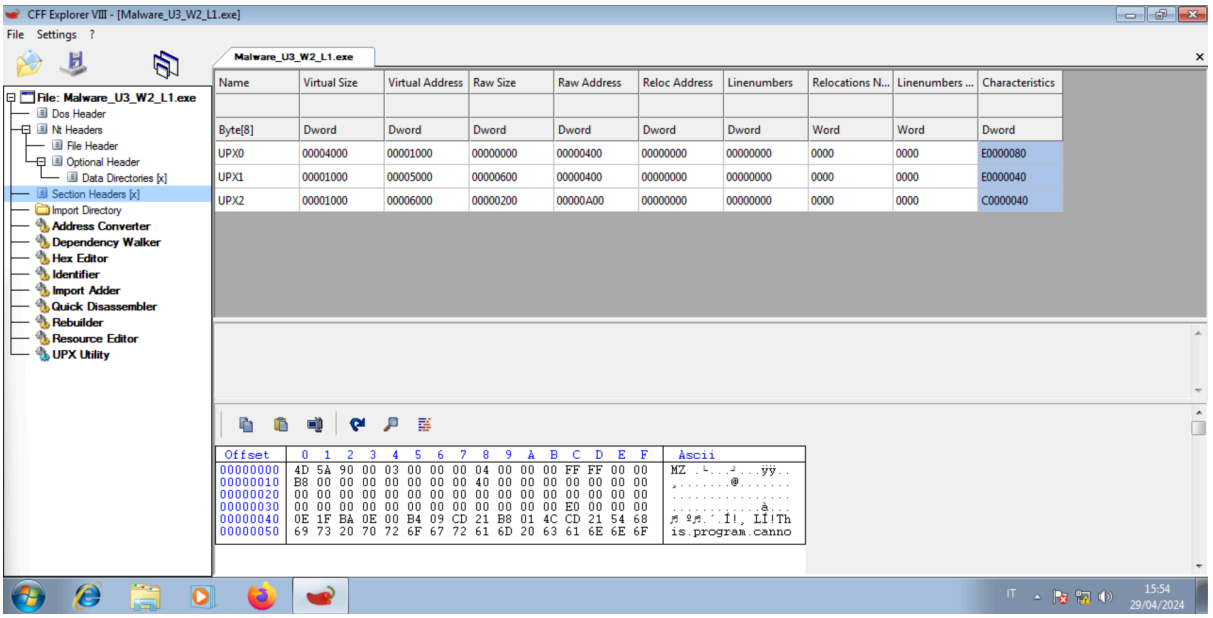
Librerie presenti nel malware



Kernel32.dll: contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.
Advapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo
MSVCRT.dll: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.
Wininet.dll:contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Sezioni presenti nel malware



Questo malware avanzato presenta sfide nell'analisi statica di base, poiché non fornisce molte informazioni sul suo comportamento. Questa conclusione è rafforzata dalla presenza di funzioni importanti come "LoadLibrary" e "GetProcAddress", suggerendo che il malware carichi librerie durante l'esecuzione, rendendo difficile identificare le librerie importate in fase di analisi preliminare.