

S10-L1

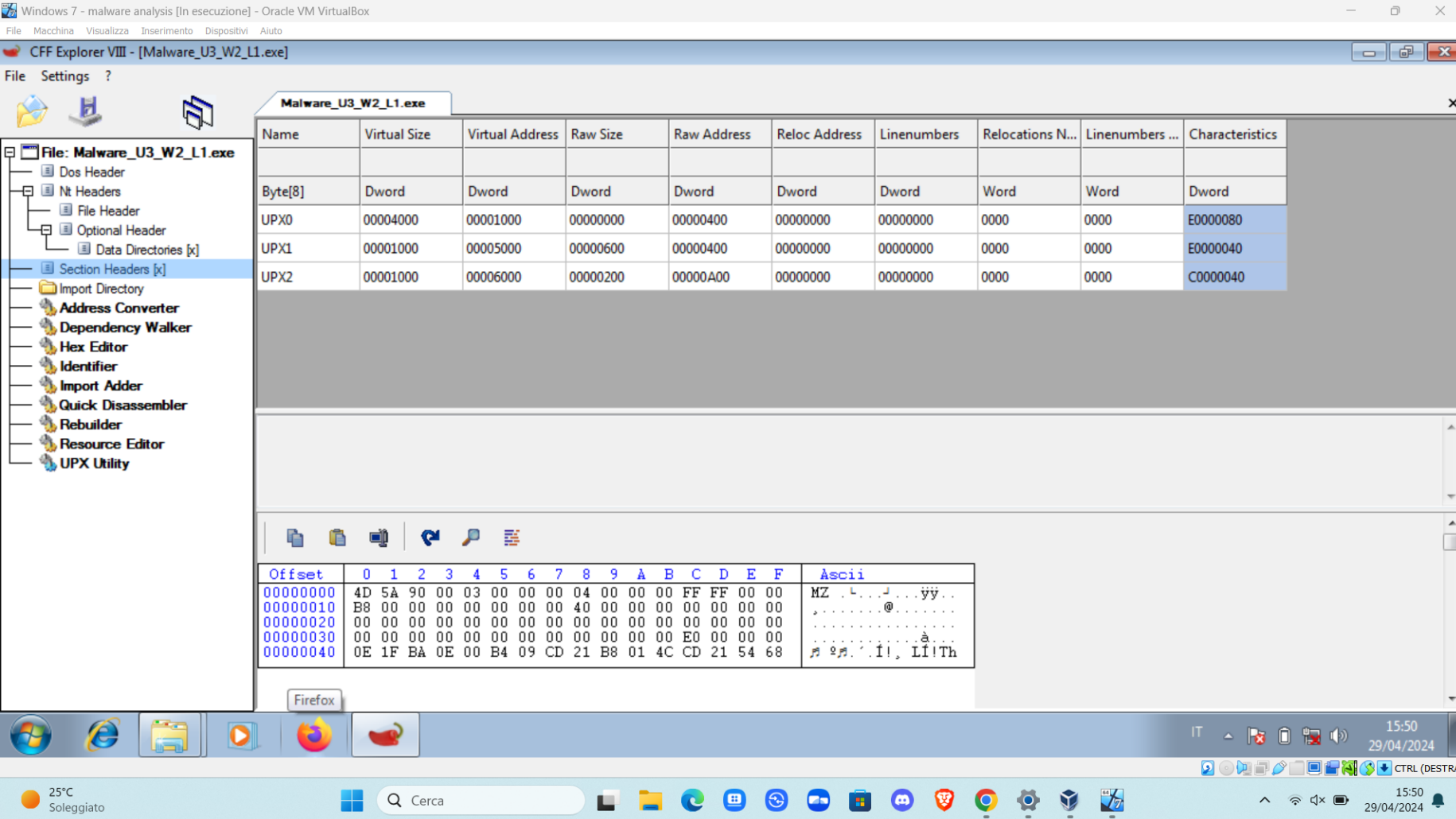
File: Malware\_U3\_W2\_L1.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Module Name	Imports	OFs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

Come possiamo vedere sono state importate le seguenti librerie:

- Kernel32.dll**, che include le funzioni core del sistema operativo
- Advapi32.dll**, che include le funzione per interagire con registri e servizi Windows
- MSVCRT.dll**, libreria scritta in C per la manipolazione scritte o allocazione memoria
- Wininet.dll**, include le funzione per implementare i servizi di rete come ftp, ntp, http



Come possiamo vedere dall' immagine non possiamo risalire alle sezioni del malware. Sembra che le abbia mascherate