EPICODE

CYBERSECURITY COURSE

BY MAX ALDROVANDI

17/05/2024

Web-site: https://epicode.com/it

Locality:
Via dei Magazzini Generali,
6 Roma, Lazio 00154, IT

PRACTICE EXERCISE S10/L1

Track:

Exercise Static Analysis With reference to the executable file contained in the "Exercise_Practice_U3_W2_L1" folder on the Desktop of your virtual machine dedicated to malware analysis, answer the following questions:

- Indicate the libraries imported by the malware, providing a description for each of them

- Indicate the sections of which the malware is composed, providing a description for each of them

- Add a final consideration about the malware under analysis based on the information gathered

Basic static analysis

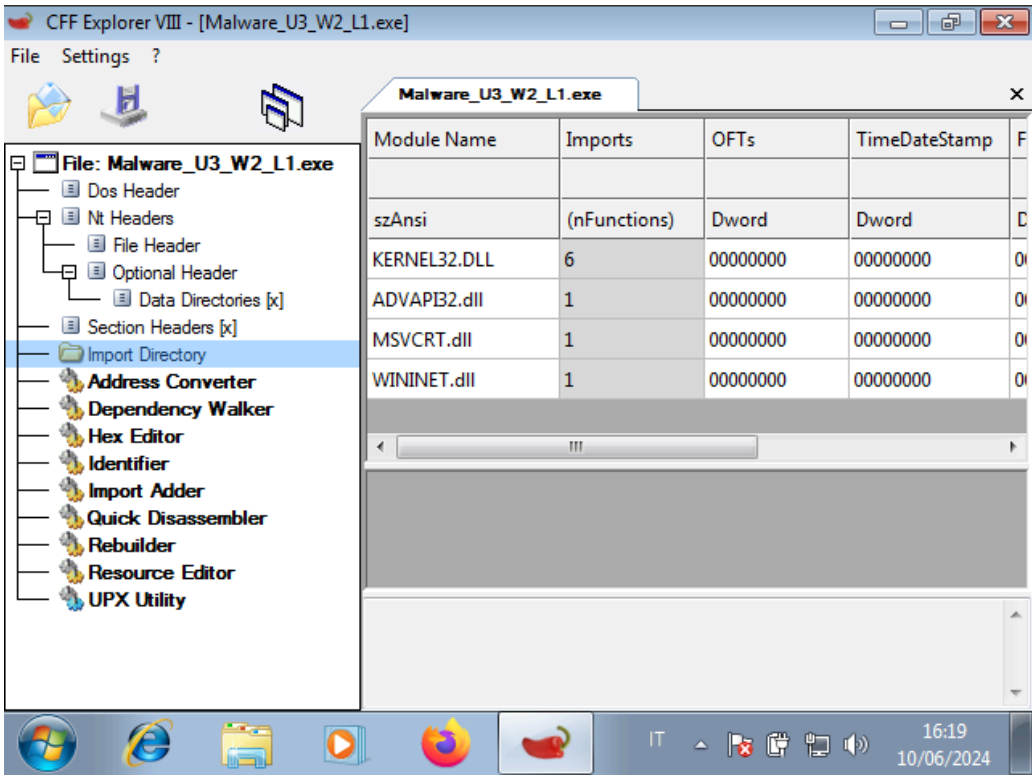
Using **CFF Explorer**, we see from the import directory section that the **U3_W2_L1 malware** imports **4 libraries**:

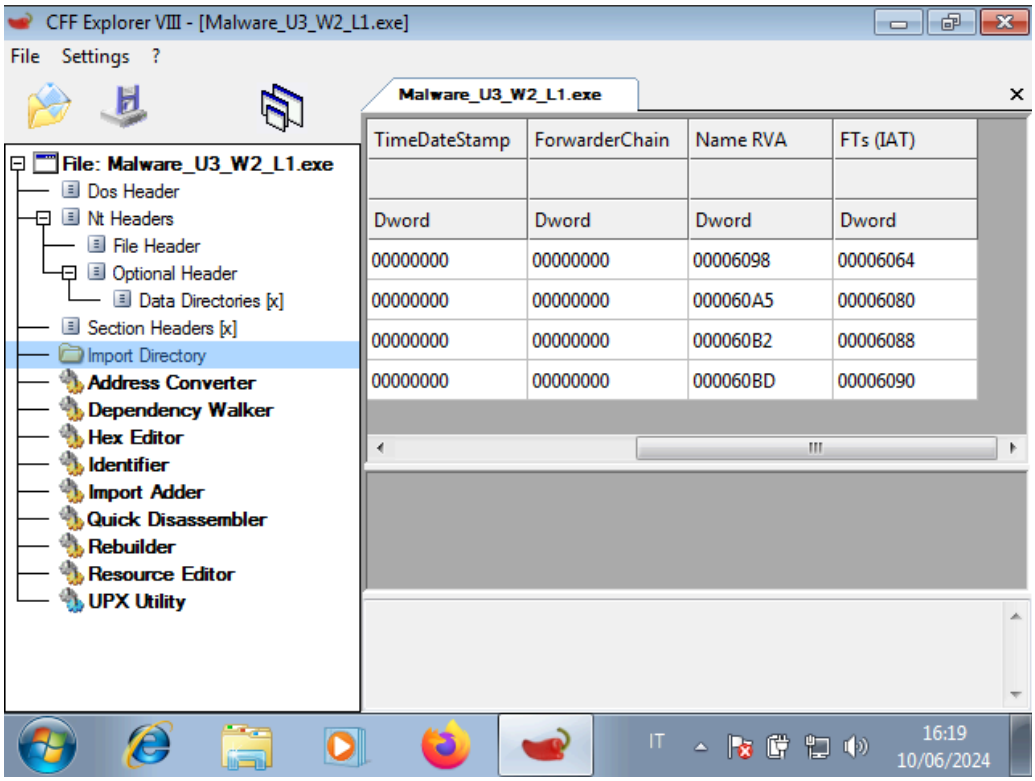
- Kernel32.dll, which includes the core functions of the operating system

- Advapi32.dll, which includes the functions to interact with Windows registers and services

- MSVCRT.dll, library written in C for manipulating written or memory allocation

- Wininet.dll, includes the functions to implement network services such as ftp, ntp, http

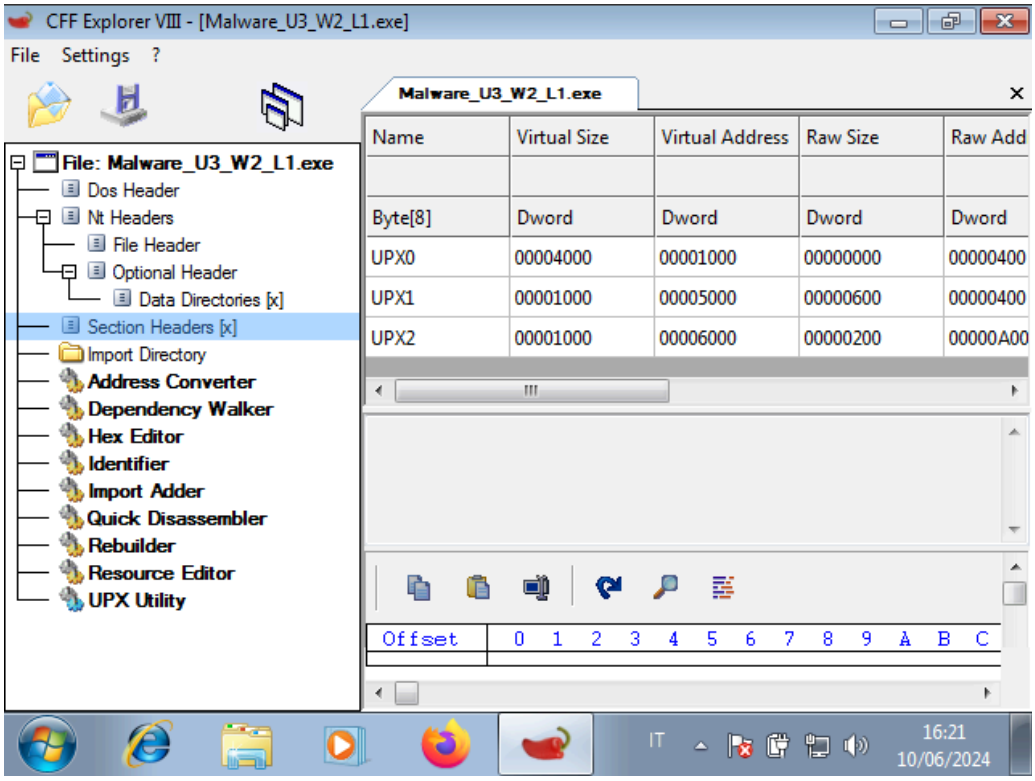

CFF Explorer VIII - [Malware_U3_W2_L1.exe]
File Settings ?
Malware_U3_W2_L1.exe
File: Malware_U3_W2_L1.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Module Name | Imports | OFTs | TimeDateStamp
szAnsi | (nFunctions) | Dword | Dword
KERNEL32.DLL | 6 | 00000000 | 00000000
ADVAPI32.dll | 1 | 00000000 | 00000000
MSVCRT.dll | 1 | 00000000 | 00000000
WININET.dll | 1 | 00000000 | 00000000
IT
16:19
10/06/2024


CFF Explorer VIII - [Malware_U3_W2_L1.exe]
File Settings ?
Malware_U3_W2_L1.exe
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
TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT)
Dword | Dword | Dword | Dword
00000000 | 00000000 | 00006098 | 00006064
00000000 | 00000000 | 000060A5 | 00006080
00000000 | 00000000 | 000060B2 | 00006088
00000000 | 00000000 | 000060BD | 00006090
IT
16:19
10/06/2024

Malware sections

From **CFF Explorer**, from the “section header” section we see that the executable consists of **3 sections**.

Unfortunately, it seems that the malware has hidden the real name of the sections, so we are unable to tell what kind of sections they are.



Final considerations

This is an advanced malware that does not allow us to recover much information about its behavior with basic static analysis.

This is supported by the fact that among the imported functions we find "**LoadLibrary** and **GetProcAddress**", which make us think of a malware that imports libraries at runtime (runtime) while actually hiding information about the imported libraries upstream.