

S10-L1

by Andreoli Michael & Hmich Otman

Referring to the executable file contained in the "Esercizio_Pratico_U3_W2_L1" folder located on the Desktop of your virtual machine dedicated to malware analysis, answer the following questions:

List the libraries imported by the malware, providing a description for each of them.

List the sections that make up the malware, providing a description for each of them.

Add a final consideration on the malware under analysis based on the information collected.

CFF Explorer

CFF Explorer is a freeware suite offering a comprehensive Portable Executable (PE) editor, CFF Explorer, alongside a process viewer. CFF Explorer itself provides in-depth analysis and modification capabilities for PE files, including support for 32-bit and 64-bit architectures. Key functionalities include:

Detailed PE Structure Exploration: Examine headers, sections, imports, exports, and resources of PE files.

Editing and Customization: Modify metadata fields and flags, enabling customization of program behavior.

Advanced Functionality: Tools like a disassembler, hex editor, import adder, and scripting language empower advanced editing and analysis.

.NET Support: CFF Explorer is the first PE editor with full support for editing .NET internal structures and resources.

Overall, CFF Explorer caters to programmers and reverse engineers seeking a feature-rich solution for PE file analysis and modification.

Import Directory

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	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

A **DLL (Dynamic Link Library)** is a toolbox for computer programs. It contains tools (functions and data) that many programs can use at once, instead of each program having its own copy. This saves space and memory. If a program needs to open a file. There's a DLL with a "file open" tool inside. Many programs can use this same tool from the DLL, instead of each writing their own version.

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	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
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

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress
N/A	000060E6	0000	VirtualProtect
N/A	000060F6	0000	VirtualAlloc
N/A	00006104	0000	VirtualFree
N/A	00006112	0000	ExitProcess

KERNEL32.DLL: A fundamental Windows library. It provides basic functions, including memory management, process management, and thread execution. It

is imported by many operating system executable files.

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	ForwarderChain	Name RVA	FTs (IAT)
0000AA5	N/A	0000A14	0000A18	0000A1C	0000A20	0000A24
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

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006120	0000	CreateServiceA

ADVAPI32.dll: Handles user authentication, security token management, and access to the system registry. It is often imported by executable files that require elevated privileges or need to access protected resources.

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	ForwarderChain	Name RVA	FTs (IAT)
0000AB2	N/A	0000A28	0000A2C	0000A30	0000A34	0000A38
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

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006130	0000	exit

MSVCRT.dll: The standard C runtime library for Windows. It provides basic functions for input/output, string management, and mathematics. It is imported by almost all Windows executable files that use the C or C++ programming languages.

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	ForwarderChain	Name RVA	FTs (IAT)
00000ABD	N/A	00000A3C	00000A40	00000A44	00000A48	00000A4C
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

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006136	0000	InternetOpenA

WININET.dll: Provides functions for Internet access, such as sending and receiving HTTP requests and downloading files. It is imported by executable files that need to connect to the Internet.

Section Headers

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

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

From an initial attempt to open with CFF, we were unable to retrieve the section names, so we used the UPX utility to decompress the malware and analyze it again.

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000	40000040
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040

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

Now we can see the parts of the malware, .text, .rdata, .data;

.text This is the part of the code that will be executed by the CPU.

.rdata This is the section that contains information about the imported libraries.

.data Contains the global variables that the code will act upon.

We can conclude that the malware in question could potentially be very dangerous if executed. It calls code from the most important system libraries and could thus have access to the machine's files, manage its memory, access user data, and, once the code is executed, it could also send all collected information to a potential attacker using network libraries.