PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

TUTORIAL S10L1

IANNONE LUCA
ALESSIO D’OTTAVIO
GIUSEPPE PIGNATELLO
FRANCESCO PIO SCOPECE

DRAFT

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

Traccia:

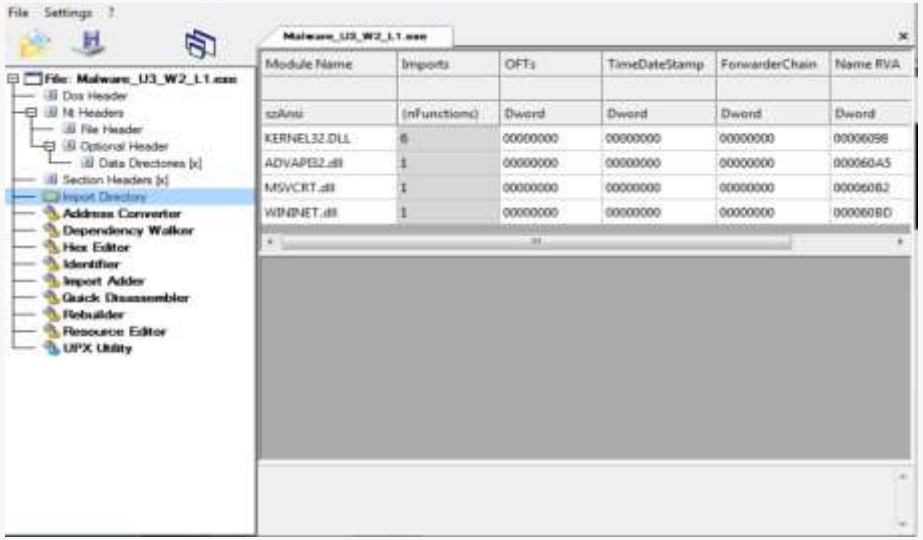
Con riferimento al file eseguibile contenuto nella cartella «**Esercizio_Pratico_U3_W2_L1**» presente sul Desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Indicare le **librerie importate** dal malware, fornendo una **descrizione** per ognuna di esse
- Indicare le **sezioni** di cui si compone il malware, fornendo una **descrizione** per ognuna di essa
- Aggiungere una **considerazione finale** sul malware in analisi in base alle informazioni raccolte

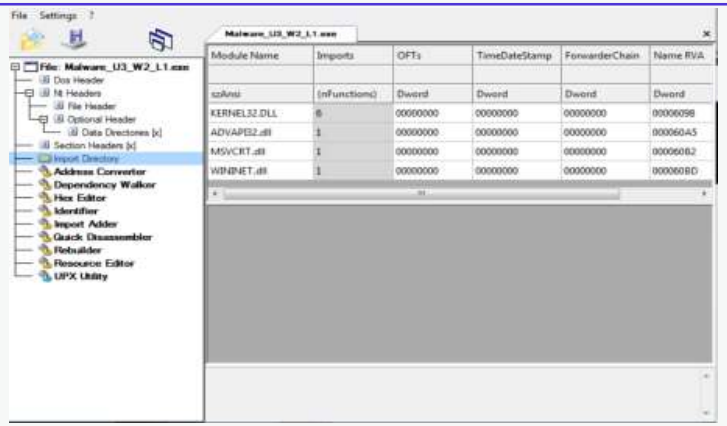
PROGRESS

LIBRARY ANALYSIS

Starting from the beginning, we do the following:
1 - OPENING THE WINDOWS 7 MACHINE TO BE EXAMINED
2 – LET'S OPEN THE SOFTWARE MALWARE ANALISYS FOLDER
3 – WE USE THE CFF EXPLORER VIII TOOL
4 – ONCE OPENED, SELECT THE MALWARE TO BE ANALYZED



As we can see from the image on the right, the libraries used by the malicious program are 4, and are as follows:
KERNEL32.DLL
ADVAP32.DLL
MSVCRT.DLL
WINNET.DLL
These libraries are visible inside the "Import Directory" folder
N.B.
IN THE NEXT SLIDE WE WILL SEE SPECIFICALLY WHAT THE LIBRARIES IN QUESTION DO IN A GENERIC WAY.



The libraries mentioned are common Windows system libraries, often used for various programming purposes. Here is a brief description of each of them:

KERNEL32.dll:This is one of the core libraries of the Windows kernel. It contains many fundamental functions for managing memory, files, processes, and threads. It is widely used for low-level operations such as memory allocation, file management, and process and thread creation and management.

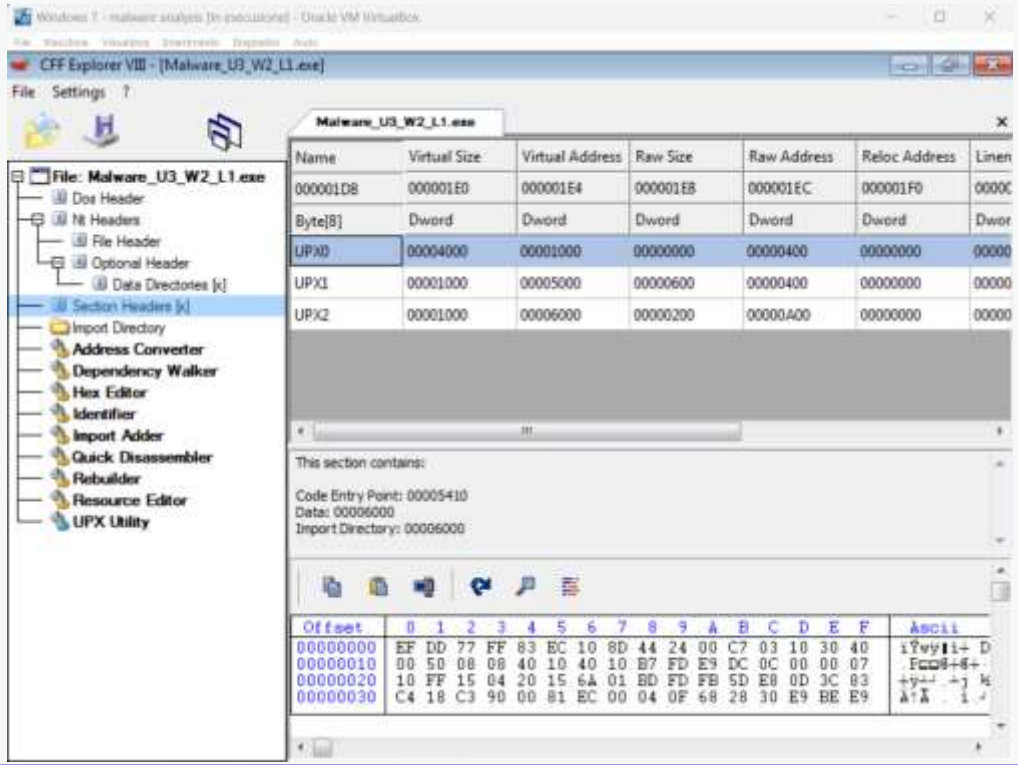
ADVAPI32.dll:This library provides many functions for interfacing with the registry, for managing user accounts and privileges, and for encrypting data. It is often used for security operations and account management, such as accessing the registry, managing Windows services, and accessing security objects.

MSVCRT.dll: This library provides many support features for programming in C/C++. It includes functions for memory management, string management, input/output, and more. It is commonly used for programs written in C or C++ and provides runtime functionality for applications developed with Microsoft Visual C++.

WININET.dll: This library provides functionality for accessing network resources on the Internet. It includes functions for managing HTTP, HTTPS, FTP, and other network operations. It is often used for developing applications that require network communications, such as web browsers, FTP clients, and other software that requires access to online resources.

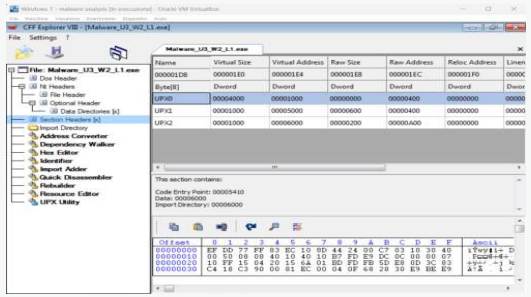
PROGRESS

INDICATION OF THE SECTIONS WHERE THE MALWARE IS COMPOSED AND THEIR DESCRIPTIONS



As we can see, the malware has hidden the real name of the sections, so it is not possible to go and see the name and automatically the sections with their descriptions.
Although not required by the track in the figure below, only and exclusively out of curiosity we went to make the real names visible through the function inside the CFF Explorer VIII tool (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
.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



The "LoadLibrary" is crucial when you want to dynamically load a DLL while running a Windows program.

The "GetProcAddress" is a fundamental function for obtaining pointers to functions within DLLs in Windows, thus allowing dynamic access and calling of functions flexibly while running the program.

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

The "kernel32.dll" and its "ExitProcess" function are an integral part of the Windows operating system and serve to manage the termination of processes safely and efficiently.

VirtualAlloc is a crucial feature for managing memory in a flexible and controlled manner in a Windows program.

VirtualProtect is a key feature for dynamically changing access permissions to a memory region in a Windows program.

VirtualFree is essential for managing memory in a dynamic and controlled way in a Windows program, complementing the memory allocation made by VirtualAlloc.

VirtualProtect is a key feature for dynamically changing access permissions to a memory region in a Windows program.

This is just one example

EXPLANATION

When using a dynamic library such as a DLL, you need to get a pointer to the function you intend to use within the DLL. "GetProcAddress" allows you to do just that.
The signature of the "GetProcAddress" function is as follows:

```
FARPROC GetProcAddress(
  HMODULE hModule,
  LPCSTR  lpProcName
);
```

•hModule: This is the manager of the DLL from which you want to get the address of the function.
•lpProcName: This is the name of the function whose address you want to get.
•This function returns a pointer to the code of the specified function, if it was found in the DLL; otherwise, it returns NULL.

The main purpose of the "kernel32.dll load library" is to load a DLL (Dynamic Link Library) into the current process. A DLL is a file that contains a collection of functions and resources that can be used by other programs.
The basic signature of the LoadLibrary function is as follows:

```
HMODULE LoadLibrary(
  LPCWSTR lpLibFileName
);
```

•lpLibFileName: This is the path or file name of the DLL you want to load.
•The function returns a handle to the loaded library (HMODULE), which can be used later to refer to the newly loaded DLL.
•When you call LoadLibrary, the operating system loads the specified DLL into memory and resolves all of its dependencies. This means that if the DLL you are loading depends on other DLLs, they will be automatically loaded and linked.
•LoadLibrary is widely used in Windows programs for accessing external functionality provided by dynamic libraries. Once a DLL is loaded, you can use the GetProcAddress function to get a pointer to a specific function within that DLL and then call that function.

VirtualAllo

It's especially useful when you need to allocate large blocks of memory, or when you need to specifically control memory allocation for certain purposes, such as executing dynamically generated code. Here is the basic signature of the VirtualAlloc function:

```
LPVOID VirtualAlloc(
  LPVOID lpAddress,
  SIZE_T dwSize,
  DWORD  flAllocationType,
  DWORD  flProtect
);
```

•lpAddress: Specifies the base address of the memory region to be allocated. If this parameter is NULL, the system automatically selects the base address.
•dwSize: Specifies the size, in bytes, of the memory region you want to allocate.
•flAllocationType: Specifies the type of memory allocation. It can be MEM_COMMIT to allocate memory and make it immediately available for use, MEM_RESERVE to reserve an address space for future memory allocation, or a combination of both.
•flProtect: Specifies the type of memory protection for the allocated region. This parameter determines whether memory can be read, written, or executed.
•The function returns a pointer to the allocated memory, or NULL if it fails.
•VirtualAlloc is widely used in situations where memory needs to be allocated in a dynamic and controlled manner, such as when creating new memory pages, allocating buffers for I/O operations, or creating executable memory areas for on-the-fly generated code.

CONCLUSION

It is an advanced malware that does not allow us to retrieve 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 malware that imports runtime libraries and effectively hides information about the upstream imported libraries.

THANKS FOR YOUR ATTENTION

BY

PHANTOM s.r.l
IMPOSSIBLE IS
OUR TARGET

IANNONE LUCA
ALESSIO D'OTTAVIO
GIUSEPPE PIGNATELLO
FRANCESCO PIO SCOPECE