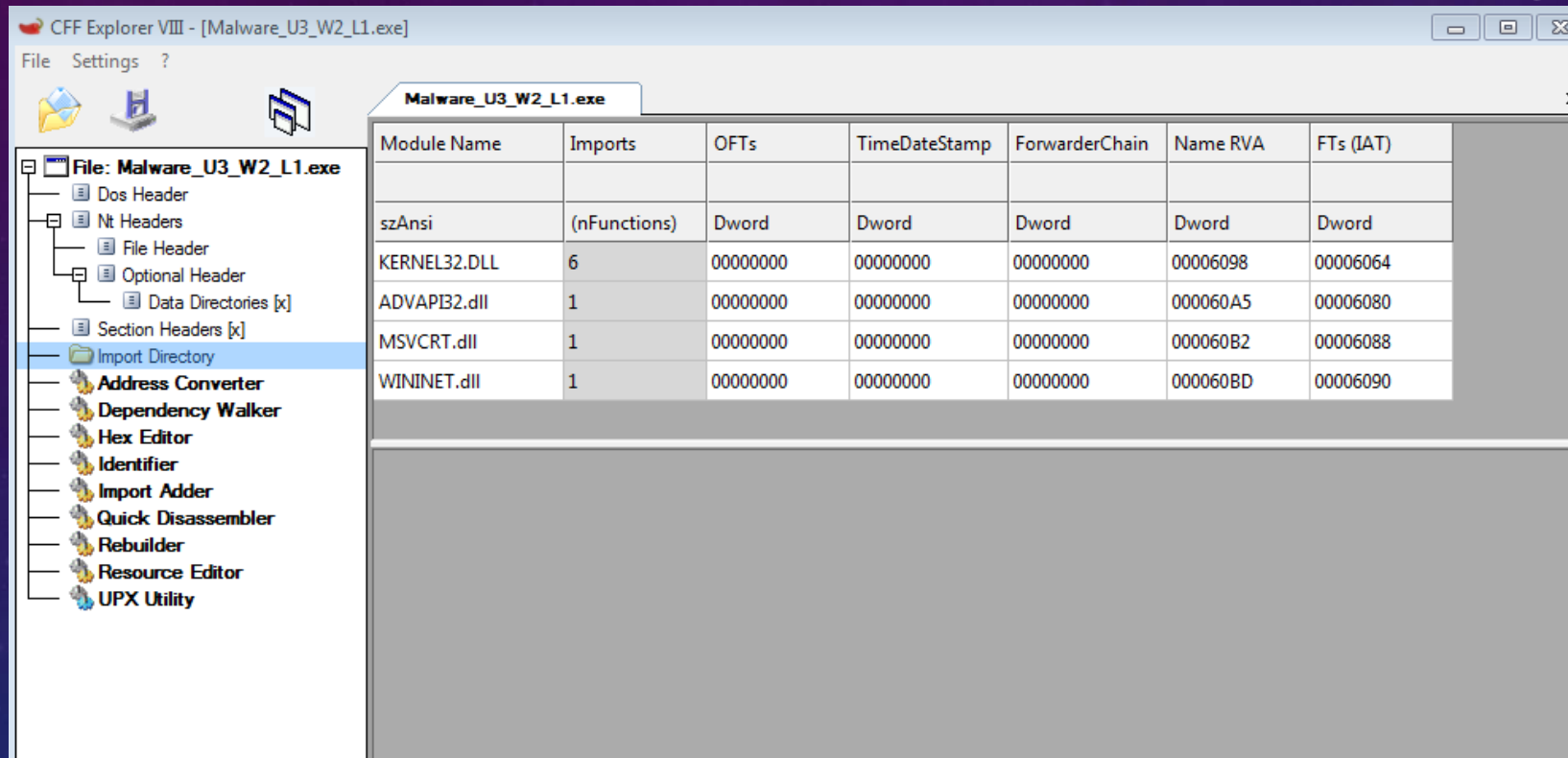


The background is a dark blue gradient with a subtle pattern of white dots. On the left side, there are several concentric circles and a large circular scale with degree markings from 140 to 260. Some of the circles have arrows indicating a clockwise direction. The text is positioned on the right side of the image.

MALWARE ANALYSIS

S10/L1

NELL'ESERCIZIO DI OGGI ANDIAMO AD ESEGUIRE UN ANALISI STATICA BASICA VEDIAMO LE LIBRERIE CHE VENGONO IMPORTARE CON LE LORO CARATTERISTICHE, LE SEZIONI DI CUI SI COMPONE IL MALWARE CON LE RELATIVE DESCRIZIONI, INFINE FACCIAMO UNA CONSIDERAZIONE RIGUARDO ALL'ANALISI E ALLE INFORMAZIONI RACCOLTE.



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

Utilizziamo il programma «CFF Explorer» per eseguire il file «Esercizio_Pratico_U3_W2_L1», che ci è stato fornito e proseguiamo con l'analisi dei malware

CFF EXPLORER CI MOSTRA NELLA CARTELLA DIRECTORY CHE IL MALWARE CHE ABBIAMO ESEGUITO IMPORTA QUATTRO LIBRERIE, OVVERO:

Malware_U3_W2_L1.exe						
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

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

«SECTION HEADER» CI MOSTRA LE SEZIONI DEL MALWARE

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
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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000030	00	00	00	00	00	00	00	00	00	00	00	E0	00	00	00	00à...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	è. .í! , Lí!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is.program.canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t.be.run.in.DOS.
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode...\$.....
00000080	E3	C1	65	8F	A7	A0	0B	DC	A7	A0	0B	DC	A7	A0	0B	DC	šÁe \$ šŮš šŮš šŮ
00000090	4F	BF	01	DC	AC	A0	0B	DC	24	BC	05	DC	A6	A0	0B	DC	Ō Ů- šŮšš Ů! šŮ
000000A0	4F	BF	0F	DC	A5	A0	0B	DC	A7	A0	0B	DC	A3	A0	0B	DC	ŌšŮš šŮš šŮš šŮ
000000B0	A7	A0	0A	DC	BC	A0	0B	DC	C5	BF	18	DC	A2	A0	0B	DC	\$ Ůš šŮšš Ůš šŮ

Il malware dunque è composto da 3 sezioni «UPX0», «UPX1», «UPX2»
ma non riusciamo a capire che sezione sono, il vero nome viene nascosto.

CONSIDERAZIONI FINALI DOPO L'ANALISI

Abbiamo visto che questo malware non ci consente di recuperare molte informazioni con l'analisi statica basica, quindi si tratta di un malware potenzialmente avanzato.

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000A98	N/A	0000A00	0000A04	0000A08	0000A0C	0000A10
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

Tra le funzioni importate infatti troviamo «LoadLibrary e GetProcAddress», che possono essere sfruttate per nascondere l'attività dannosa. Sono utilizzate da malware per caricare in modo dinamico il codice dannoso all'interno di un processo in esecuzione e per ottenere puntatori a funzioni all'interno di queste librerie per eseguire operazioni dannose, come il furto di informazioni o il danneggiamento del sistema.