

REPORT PROGETTO S10/L5

29/03/2024



Prepared By:
Ayman Hani

TRACCIA

Con riferimento al file Malware_U3_W2_L5 presente all'interno della cartella

«Esercizio_Pratico_U3_W2_L5» sul desktop della macchina virtuale dedicata per l'analisi dei malware, rispondere ai seguenti

quesiti:

vengono importate dal file eseguibile?

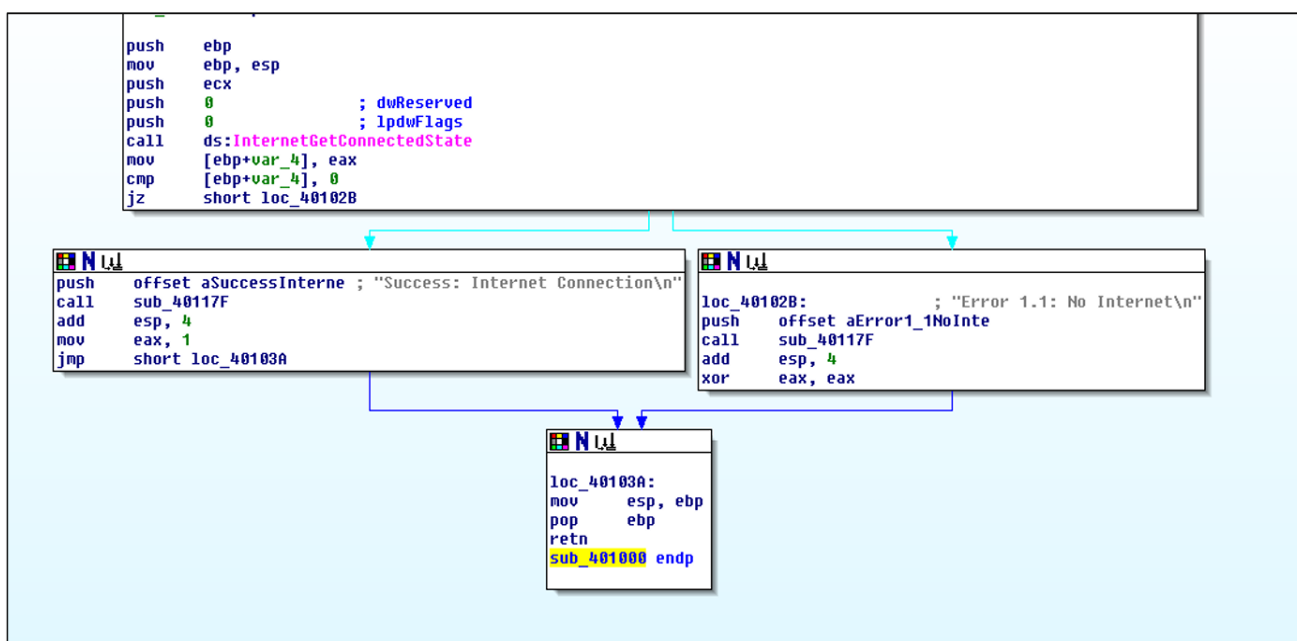
1. Quali librerie

2. Quali sono le sezioni di cui si compone il file eseguibile del malware?

Con riferimento alla figura in slide 3, risponde ai seguenti quesiti: 3. Identificare i costrutti noti (creazione dello stack, eventuali cicli, altri costrutti)

4. Ipotezzare il comportamento della funzionalità implementata 5. BONUS fare tabella con significato delle singole righe di codice assembly

Figura 1

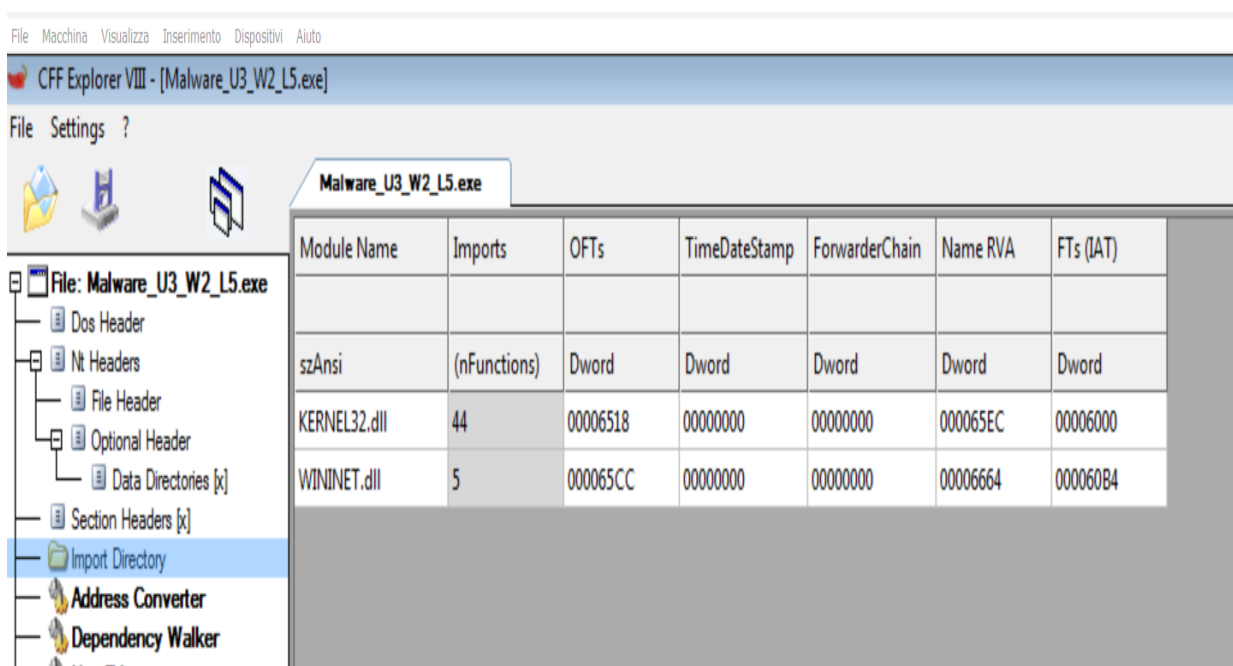


INDICE

1. Librerie importate
2. Sezioni del malware
3. Identificazione dei costrutti
4. Comportamento della funzionalità implementata

LIBRERIE IMPORTATE

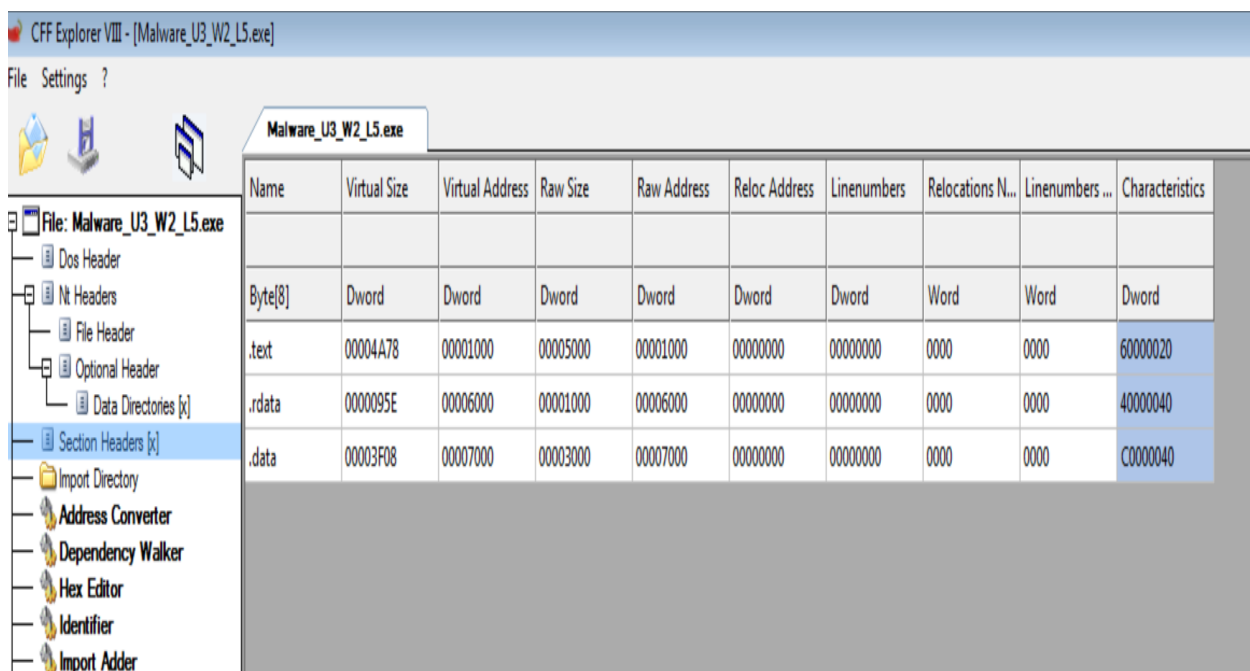
Utilizziamo CFF explorer per controllare le librerie importate del file eseguibile e cliccando l'opzione "Import directory" scopriamo che le librerie importate dal file eseguibile sono **Kernel32.dll** e **WININET.dll**:



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

SEZIONI DEL MALWARE

Sempre utilizzando CFF explorer verifichiamo le sezioni di cui si compone il file cliccando su "section headers" visualizzando : test,rdata,data



CFF Explorer VIII - [Malware_U3_W2_L5.exe]

File Settings ?

Malware_U3_W2_L5.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	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

File: Malware_U3_W2_L5.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

IDENTIFICAZIONE DEI COSTRUTTI

Questo blocco di istruzioni fa riferimento alla creazione dello stack

```
push    ebp
mov     ebp, esp
```

Questo invece è un costrutto condizionale «IF»

```
cmp     [ebp+var_4], 0
jz      short loc_40102B
```

Infine abbiamo il costrutto di rimozione dello stack

```
mov     esp, ebp
pop     ebp
```

Comportamento della funzionalità implementata

Questa funzionalità controlla se su una macchina è presente la connessione ad internet, Il costrutto IF verifica se il parametro restituito dalla funzione **getinternetconnectstate** è uguale a 0, e in questo caso verrà scritto **no internet** completando l'esecuzione altrimenti nel caso in sia diverso da 0 allora verrà scritto **succes: internet connection**.