

## COSTRUTTI NOTI DEL SEGUENTE PROGRAMMA IN ASSEMBLY

-Creazione dello stack

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

-Chiamata di funzione. I parametri sono passati sullo stack tramite le istruzioni push

```
push ecx
push 0 ;dwReserved
push 0 ;ldpwFlags
call ds:InternetGetConnectedState
```

```
mov [ebp+var_4],eax
```

-Ciclo IF

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

```
push offset aSucesssInterne ; "Success: internet Connection\n"
call sub_40105f
add  esp,4
mov  eax,1
jmp  short loc_40103A
```

-ELSE

```
loc_40102B: ; "Error 1,1 : No Internet\n"
push offset aError1_1NoInte
call sub_40117F
add  esp,4
xor  eax,eax
```

```
loc_40103A:
mov  esp,ebp
pop  ebp
retn
sub_401000 endp
```

## ANALISI DEL PROGRAMMA ASSEMBLY (FUNZIONALITA' ED FUNZIONAMENTO DEL CODICE)

1-push ebp ;Istruzione che porta il processore ad inserire il valore "ebp" nello stack

2-mov ebp,esp ;Istruzione che porta il processore a copiare il valore di "esp" nel registro "ebp". Questa e' una operazione comune per la creazione di uno stack.

3-push ecx ;Istruzione per inserire il registro "ecx" nello stack, potrebbe essere usato come parametro nella funzione successiva.

4-push 0 ;dwReserved ;Parametro 2

5-push 0 ;ldpwFlags ;Parametro 3

6-call ds:InternetGetConnectedState ;chiama la funzione "InternetGetConnectedState", se la funzione restituisce un valore diverso da 0 il sistema e' connesso altrimenti no.

7-mov [ebp+var\_4],eax ;Copia il valore di ritorno della funzione nella variabile [ebp+var\_4].

8-cmp [ebp+var\_4],0

9-jz short loc\_40102B ;IF questaistruzione confronta il valore restituito dalla funzione "InternetGetConnectedState" con 0

10-push offset aSucessInterne ; "Success: internet Connection\n"

11-call sub\_40105f

12-add esp,4

13-mov eax,1

14-jmp short loc\_40103A ;Queste istruzioni vengono eseguite nel caso di successo alla connessione ad internet,"eax" viene impostato ad 1 ed il programma salta ad "loc\_40103A

15-loc\_40102B: ;"Error 1,1 : No Internet\n"

16-push offset aError1\_1NoInte

17-call sub\_40117F

18-add esp,4

19-xor eax,eax

20-loc\_40103A: ;Queste istruzioni vengono eseguite nel caso di errore,"eax viene azzerato ed il programma salta ad "loc\_40103A.Xor E' un operatore logico che restituisce in uscita VERO(1) solo se gli ingressi sono diversi tra di loro.

21-mov esp,ebp

22-pop ebp

23-retn ;Queste istruzioni servono a ripristinare lo stack e tornare quindi al chiamante

24-sub\_401000 endp ;endp(end procedure)

Le righe:16-,17- e 10- sono responsabili di stampare un messaggio di notifica dello stato di connessione a internet le opzioni sono "Success/Error".

Analizzando il codice, sembra che il programma controlli se il sistema è connesso a Internet e poi stampi un messaggio di successo o di errore a seconda del risultato.

## Analisi del malware Esercizio\_Pratico\_U3\_W2\_L5

Analizzando il programma (analisi statica base) con il tool md5deep abbiamo ottenuto l'informazione che il programma malevolo eseguibile e' dedicato ad un sistema 32 bit quindi non e' eseguibile sulla nostra macchina windows 7 64 bit,successivamente con il tool CFF si vanno ad analizzare le librerie importate che in questo caso sono:KERNEL32.dll e ed WININET.dll,conoscendo dunque le librerie importate sempre con il tool CFF ne studieremo l'ascii e le sezioni si puo' cosi definire la natura del malware.

C:\Windows\system32\cmd.exe

```
C:\Users\user\Desktop>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 88D2-1ECE
```

Directory di C:\Users\user\Desktop

```
20/01/2024  18:14    <DIR>          .
20/01/2024  18:14    <DIR>          ..
17/01/2024  17:50    <DIR>          MALWARE
17/01/2024  14:14                1.430 Mozilla Firefox.lnk
20/01/2024  18:14    <DIR>          Software Malware analysis
                  1 File          1.430 byte
                  4 Directory  22.706.679.808 byte disponibili
```

```
C:\Users\user\Desktop>cd Software Malware analysis
```

```
C:\Users\user\Desktop\Software Malware analysis>cd md5deep-4.3
```

```
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3>md5deep "C:\Users\user\Desktop\MALWARE\Esercizio_pratico_U3_W2_L5"
"md5deep" non è riconosciuto come comando interno o esterno,
un programma eseguibile o un file batch.
```

```
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3>md5deep-4.3 "\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L5"
md5deep-4.3" non è riconosciuto come comando interno o esterno,
un programma eseguibile o un file batch.
```

```
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3>md5deep \Users\user\Desktop\MALWARE\Esercizio_pratico_U3_W2_L5
"md5deep" non è riconosciuto come comando interno o esterno,
un programma eseguibile o un file batch.
```

```
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3>cd md5deep-4.3
```

```
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>md5deep \Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L5
```

```
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
```

```
md5deep: You probably want to use the 64-bit version of this program.
```

```
C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L5: No such file or directory
```

```
C:\Users\user\Desktop\Software Malware analysis\md5deep-4.3\md5deep-4.3>
```

modifica	Tipo	Dimensione
2024 17:48	Cartella di file	
2024 17:48	Cartella di file	
2024 17:48	Cartella di file	
2024 17:48	Cartella di file	
2024 17:48	Cartella di file	
2024 17:48	Cartella di file	

Windows 7  
Build 7601

La copia di Windows non è autentica

16:32  
29/03/2024

IT  Right Ctrl

CFF Explorer VIII - [Malware\_U3\_W2\_L5.exe]

File Settings ?

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
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Malware\_U3\_W2\_L5.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address
Byte[8]	Dword	Dword	Dword	Dword	Dword
.text	00004A78	00001000	00005000	00001000	00000000
.rdata	0000095E	00006000	00001000	00006000	00000000
.data	00003F08	00007000	00003000	00007000	00000000

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Asc

Cerca Soft...

Dimensione

tella di file

tella di file

tella di file

tella di file

tella di file

tella di file

tella di file

legamento 2 KB

legamento 1 KB

legamento 1 KB

legamento 2 KB

legamento 2 KB



CFF Explorer VIII - [Malware\_U3\_W2\_L5.exe]

File Settings ?

Malware\_U3\_W2\_L5.exe

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
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	0000
WININET.dll	5	000065CC	00000000	00000000	0000

Cerca Soft...

Dimensione

tella di file	
tella di file	
tella di file	
tella di file	
tella di file	
tella di file	
tella di file	
legamento	2 KB
legamento	1 KB
legamento	1 KB
legamento	2 KB
legamento	2 KB

CFF Explorer VIII - [Malware\_U3\_W2\_L5.exe]

File Settings ?

Malware\_U3\_W2\_L5.exe

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
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00006664	N/A	000064F0	000064F4	000064F8	000064FC	00006500
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
0000662A	0000662A	0056	InternetCloseHandle
00006616	00006616	0077	InternetReadFile
000065FA	000065FA	0066	InternetGetConnectedState
00006654	00006654	006F	InternetOpenA



CFF Explorer Ultima modifica: 17/01/2024 14:13  
Collegamento Dimensione: 1,57 KB

Data creazione: 17/01/2024 14:13

Windows 7

Build 7601

Questa copia di Windows non è autentica

16:36

29/03/2024

IT

Right Ctrl

ENG

GA

16:36

29/03/2024



Search



21°C  
Mostly cloudy