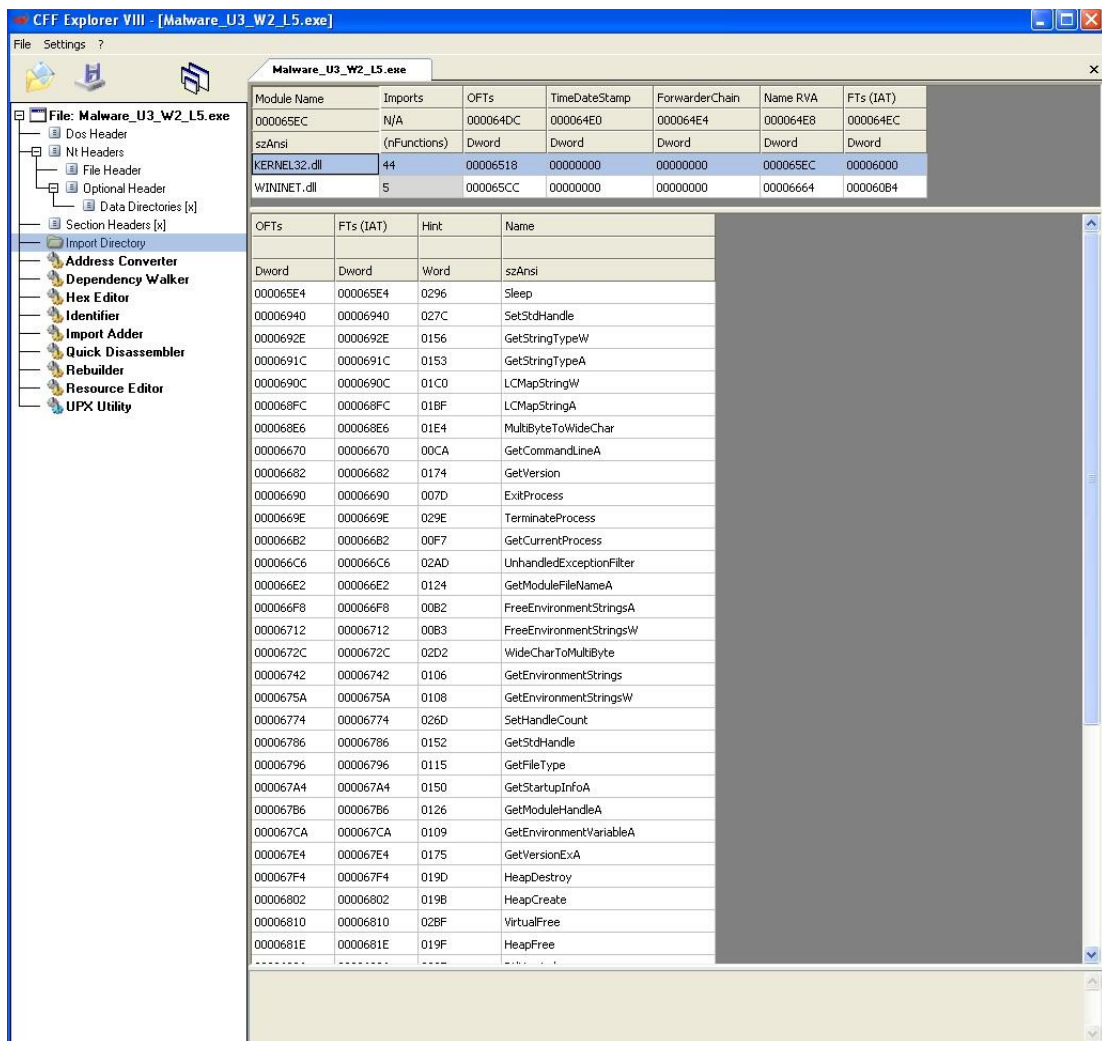


# Progetto

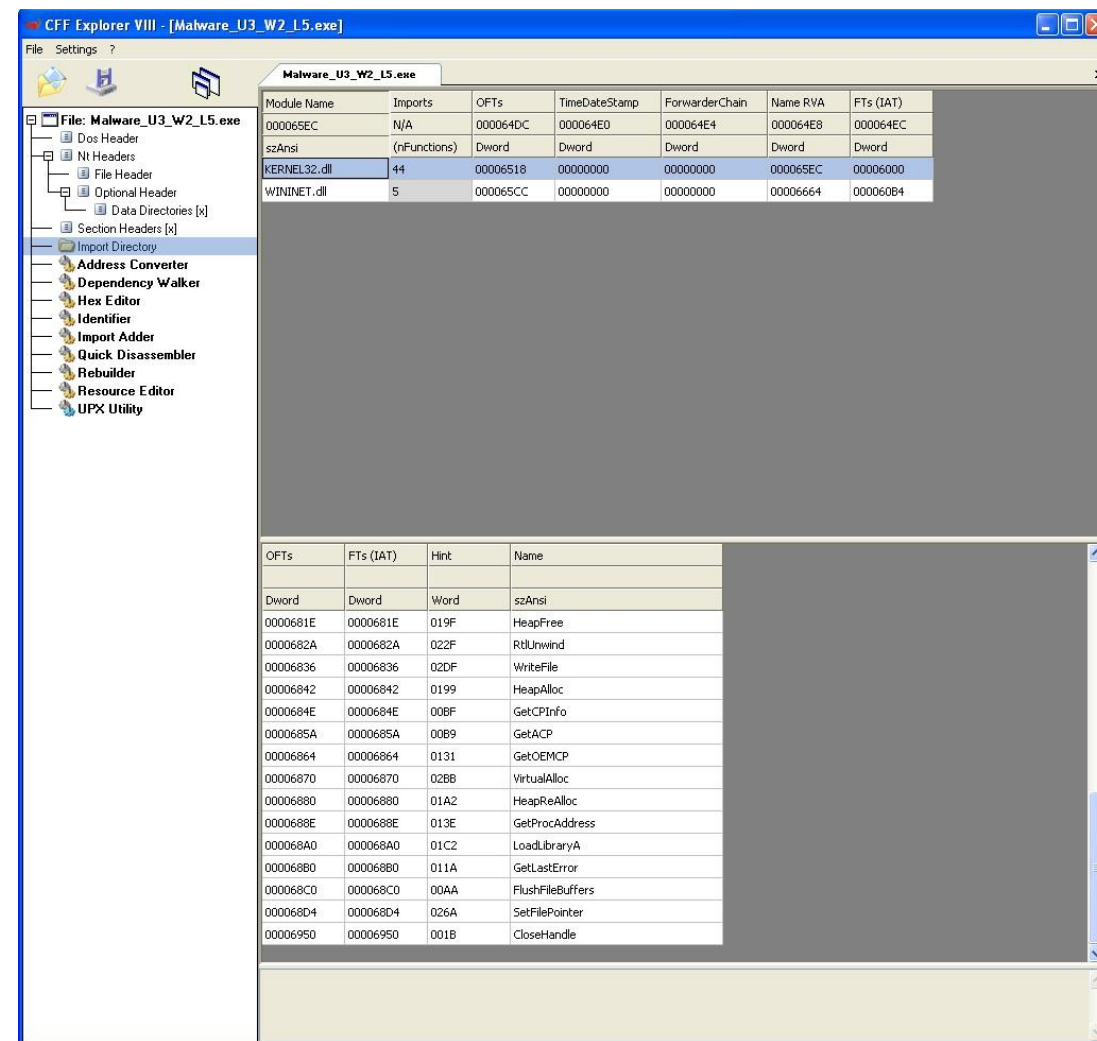
## Analisi Statica basica

Malware\_U3\_W2\_L5



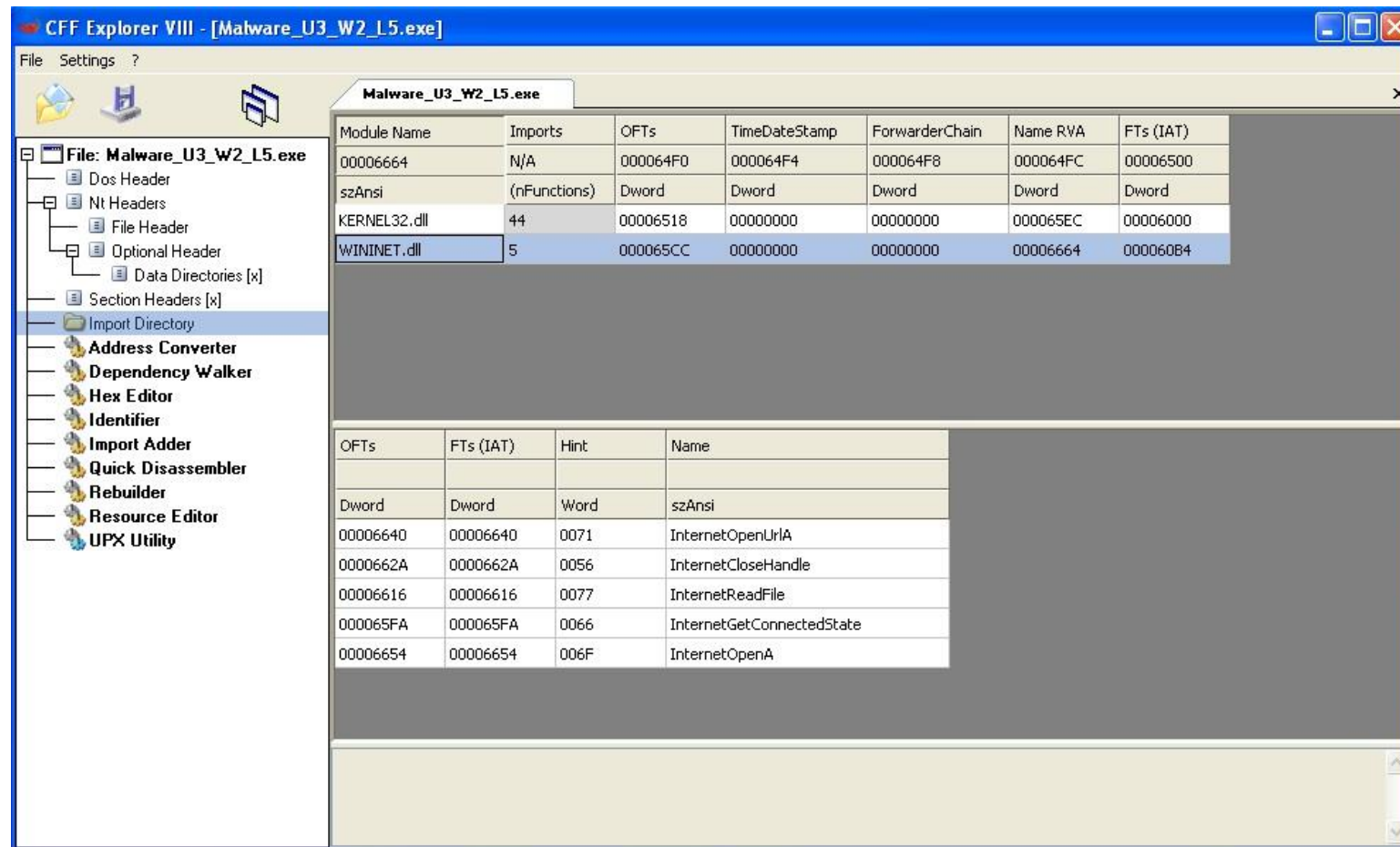
Libreria KERNEL32.DLL

Libreria contenente le funzioni principali per interagire con il sistema operativo.



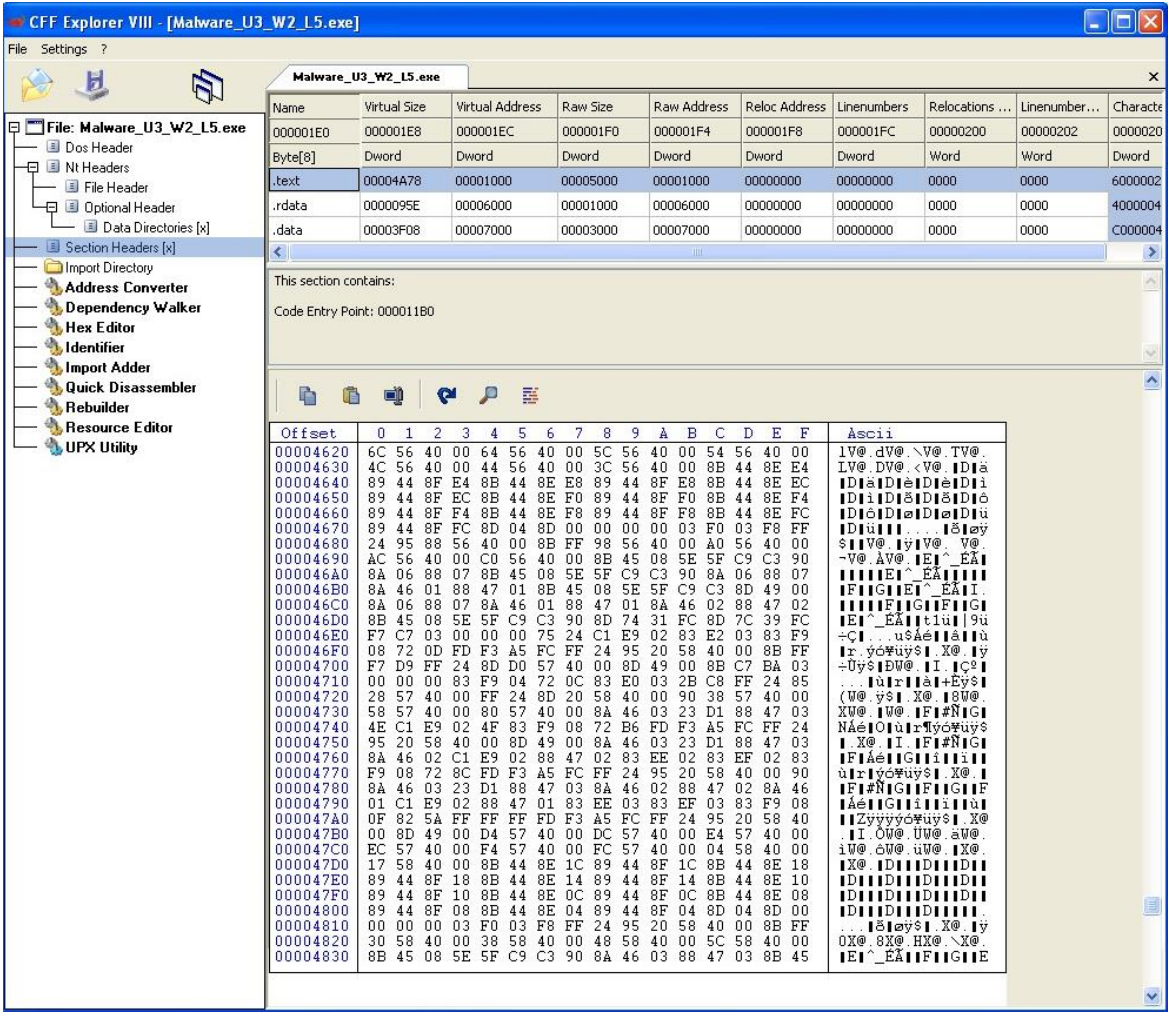
Libreria KERNEL32.DLL

Libreria contenente le funzioni principali per interagire con il sistema operativo.



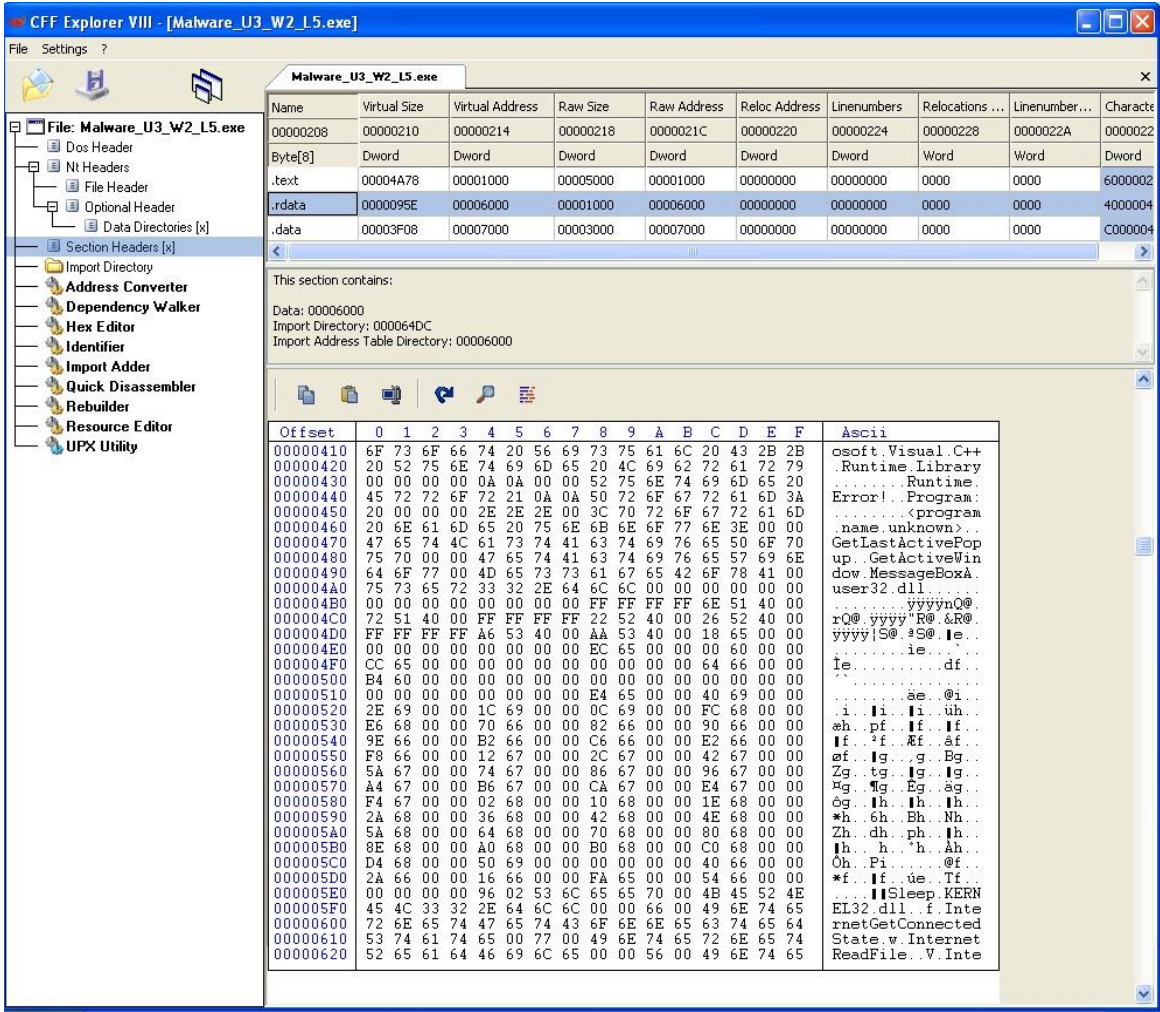
### Libreria WININET.dll

Libreria contenente le funzioni per implementare alcuni protocolli di rete come:  
HTTP, FTP, NTP.



### Sezione .text

Sezione che contiene le righe di codice che la CPU eseguirà una volta che il software sarà avviato. Unica sezione di un file eseguibile che viene eseguita dalla CPU.



### Sezione .rdata

Sezione che include le informazioni delle librerie e le funzioni importate ed esportate dall'eseguibile.



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 Addr
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumbers...	Characte
00000230	00000238	0000023C	00000240	00000244	00000248	0000024C	00000250	00000252	0000025
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	6000002
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	4000004
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C000004

This section contains:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	00	00	00	00	00	00	00	00	00	00	00	00	09	1C	40	00	.....!@.
00000010	64	35	40	00	00	00	00	00	00	00	00	AE	1C	40	00	00	d5@.....@!@.
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	45	72	72	6F	72	20	31	2E	31	3A	20	4E	6F	20	49	6E	Error.1.1:No.In
00000040	74	65	72	6E	65	74	0A	00	53	75	63	63	65	73	73	3A	ternet..Success:
00000050	20	49	6E	74	65	72	6E	65	74	20	43	6F	6E	6E	65	63	.Internet.Connec
00000060	74	69	6F	6E	0A	00	00	00	45	72	72	6F	72	20	32	2E	tion...Error.2.
00000070	33	3A	20	46	61	69	6C	20	74	6F	20	67	65	74	20	63	3:..Fail.to.get.c
00000080	6F	6D	6D	61	6E	64	0A	00	45	72	72	6F	72	20	32	2E	ommand..Error.2.
00000090	32	3A	20	46	61	69	6C	20	74	6F	20	52	65	61	64	46	2:..Fail.to.ReadF
000000A0	69	6C	65	0A	00	00	00	00	45	72	72	6F	72	20	32	2E	ile....Error.2.
000000B0	31	3A	20	46	61	69	6C	20	74	6F	20	4F	70	65	6E	55	1:..Fail.to.OpenU
000000C0	72	6C	0A	00	68	74	74	20	3A	2F	77	77	77	2E	70	00	rl..http://www.p
000000D0	72	61	63	74	69	63	61	6C	6D	61	6C	77	61	72	65	61	racticalmalwarea
000000E0	6E	61	6C	79	73	69	73	2E	63	6F	6D	2F	63	63	2E	68	nalysis.com/co.h
000000F0	74	6D	00	00	49	6E	74	65	72	6E	65	74	20	45	78	70	tm..Internet.Exp
00000100	6C	6F	72	65	72	20	37	2E	35	2F	70	6D	61	00	00	00	lorer.7.5/pma.
00000110	53	75	63	63	65	73	73	3A	20	50	61	72	73	65	64	20	Success:Parsed.
00000120	63	6F	6D	6D	61	6E	64	20	69	73	20	25	63	0A	00	00	command.is.%c...
00000130	00	1D	40	00	01	00	00	00	48	61	40	00	38	61	40	00	..!@...Ha@.8a@.
00000140	00	9F	40	00	00	00	00	00	00	9F	40	00	01	01	00	00	..!@.....!@..!!..
00000150	00	00	00	00	00	00	00	00	00	10	00	00	00	00	00	00	.....!..
00000160	00	00	00	00	00	00	00	00	00	00	00	00	02	00	00	00	.....!..
00000170	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	!.....!..
00000180	00	00	00	00	00	00	00	00	00	00	00	00	02	00	00	00	!.....!..
00000190	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	!.....!..
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000200	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

## Sezione .data

Sezione contenente tipicamente dati/variabili globali del programma eseguibile che devono essere eseguibili da qualsiasi parte del programma.

Sezioni in cui si compone il malware (part. 2)

Dall'analisi statica basica, si è giunti alla conclusione che, il malware Malware\_U3\_W2\_L1, crei un oggetto sulla macchina vittima per stabilire una connessione di tipo: HTTP, o FTP, o NTP.

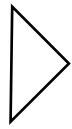
Considerazioni finali

# Progetto

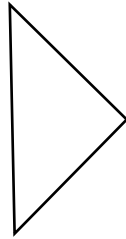
## Assembly X86

Identificazione costrutti noti  
Ipotesi di comportamento della funzione implementata

```
push    ebp
mov     ebp, esp
push    ecx
push    0          ; dwReserved
push    0          ; lpdwFlags
call    ds:InternetGetConnectedState
jz      short loc_40102B
```



Creazione stack



Chiamata di funzione  
Parametri passati  
sullo stack tramite  
istruzioni push

```
push    offset a_SuccessInternet ; "Success: Internet Internet Connection\n"
call    sub_40105F
add     esp, 4
mov     eax, 1
jmp     short loc_40103A
```

```
loc_40102B:
push    offset aError1_1NoInte
call    sub_40117F
add     esp, 4
xor     eax, eax
```

```
loc_40103A:
mov     esp, ebp
pop     ebp
retn
Sub_401000
```



Funzionalità implementata all'interno del malware facile da identificare. Il malware chiama la funzione InternetGetConnectedState.

Pseudocodice C:

```
state = internetgetconnectedstate (par1,0,0);
```

```
If (state!=0) printf ("Active connection");
```

```
Else return 0;
```

Ipotesi di comportamento della funzione implementata