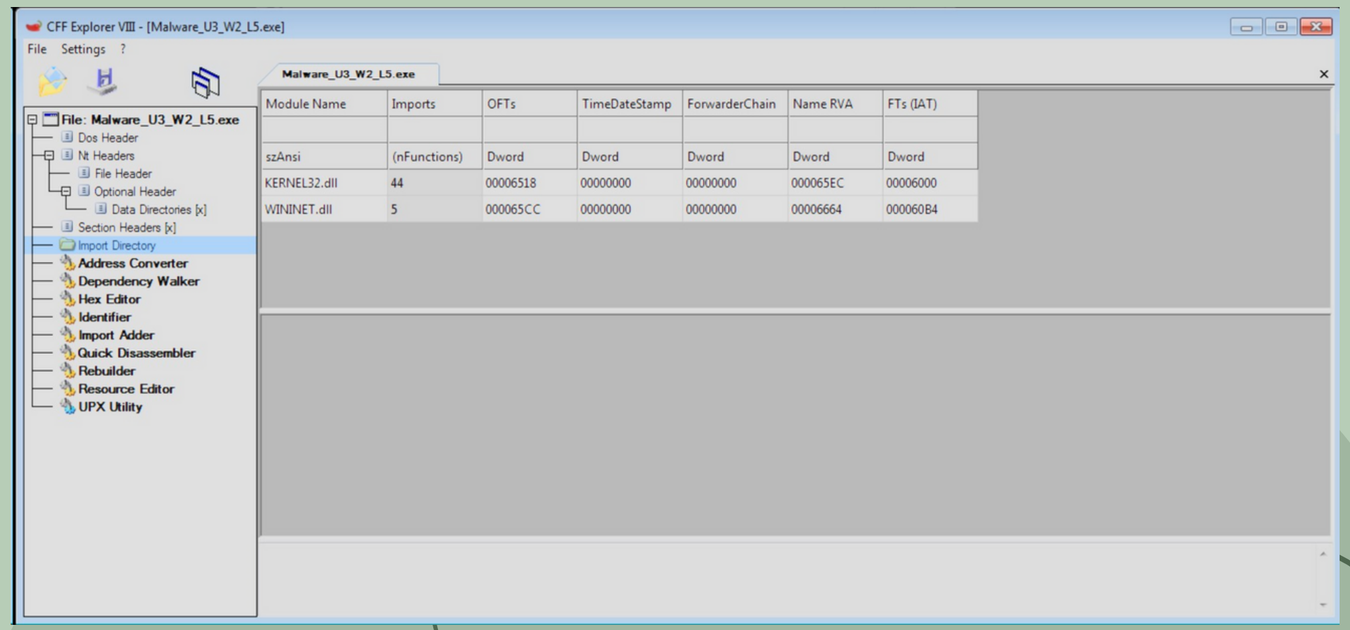
Analisi statica e dinamica

Indice

Argomenti trattati

Llbrerie importate



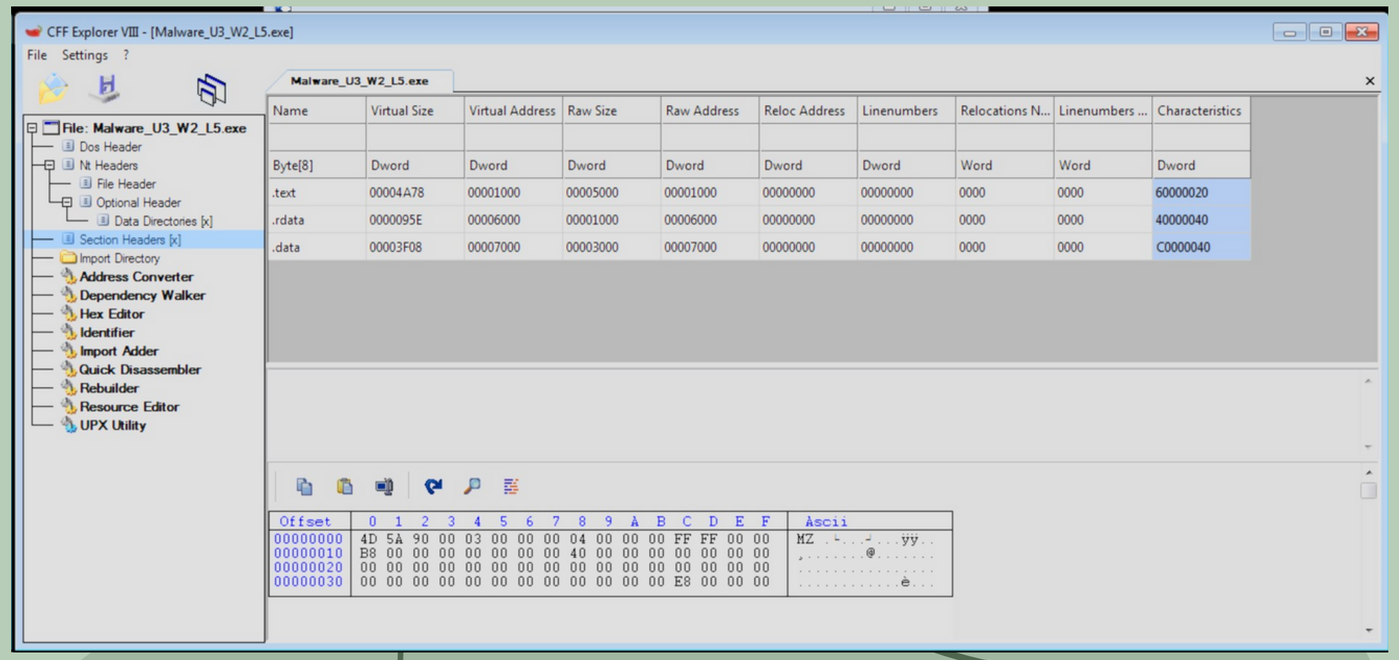
Libreria KERNEL32.dll

il Kernel32.dll è un componente Microsoft Windows è un file DLL(Dynamic Link Library) responsabile di servizi essenziali, come la gestione della memoria, la creazione di processi e thread, e la gestione delle eccezioni.

Libreria WINNET.dll

wininet.dll è una libreria di collegamento dinamico in windows, fornisce servizi di rete per le applicazioni. Gestisce i download e caricamenti http/https, gestisce i cookie, le autenticazioni e supporta i proxy. E' fondamentale per l'accesso a internet da app, contiene funzioni di networking, inclusi sockets e url.

Sezioni



.txt

contiene le istruzioni e le righe di codice che la cpu dovrà eseguire una volta che il malware verrà avviato

.rdata

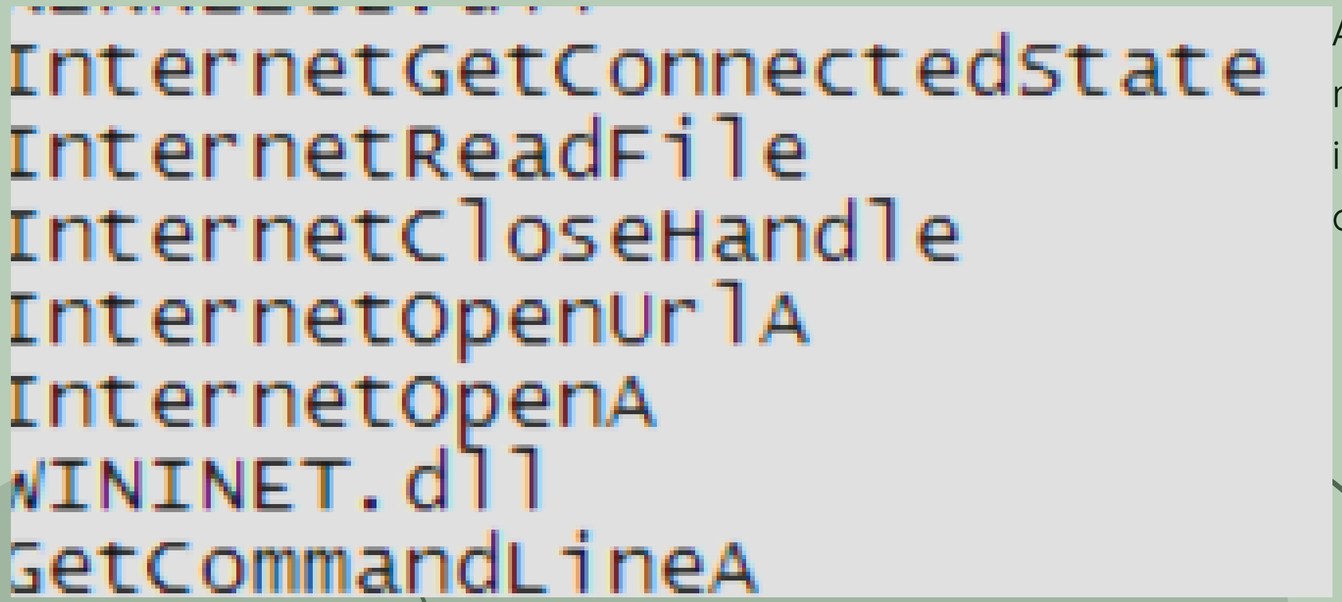
contiene le informazioni che riguardano le librerie e le funzioni importati ed esportati dal programma

.data

contiene tutti i dati e le variabili globali del programma, accessibili da tutte le parti del programma

Ipotesi

Analisi del programma con strings



Attraverso l’analisi delle stringhe presenti sul malware, possiamo individuare vari comandi relativi a internet, specialmente per aprire url ed eseguire comandi

Ipotesi

Analisi del programma con strings

```
Error 1.1: No Internet
Success: Internet Connection
Error 2.3: Fail to get command
Error 2.2: Fail to ReadFile
Error 2.1: Fail to OpenUrl
http://www.practicalmalwareanalysis.com/cc.htm
Internet Explorer 7.5/pma
Success: Parsed command is %c
```

Possiamo individuare una serie di errori, tra cui l'assenza di internet, di ricevere il comando, leggere il file o aprire il collegamento, mentre nelle frasi di esecuzione corretta troviamo la connessione ad internet e l'analisi del comando

Ipotesi

Analisi del programma con strings

Da questa prima analisi possiamo dedurre l'utilizzo di una connessione ad internet, le possibili applicazioni sono molteplici e sono necessarie analisi più approfondite per poter dedurre il tipo esatto di virus, ma le principali possibilità sono:

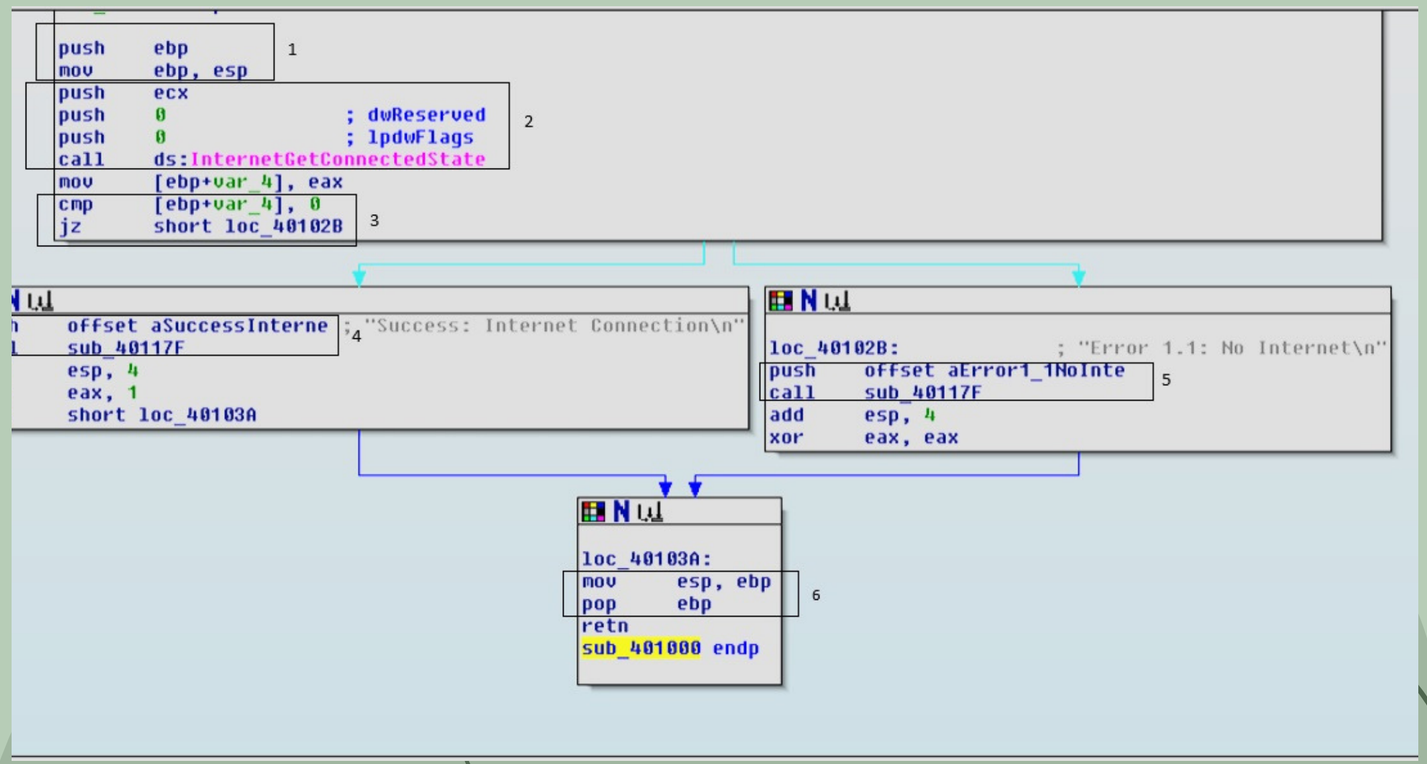
trojan

backdoor

keylogger

Individuazione dei costrutti

1)creazione dello stack di memoria



2)chiamata della funzione ”internetGetConnectedstate”

3)Costrutto if/else

4)Chiamata subroutine 40117F

5)chiamata della subroutine 40117F

6)Rimozione dello stack di memoria

Ipotesi

nella subroutine appena analizzata possiamo individuare 4 blocchi principali di esecuzione.
All’interno del primo blocco vediamo la chiamata alla funzione per controllare lo stato della connessione ad internet.
possiamo individuare un if con il jump zero che controlla il risultante della funzione e
se è stata individuata la connessione viene effettuata una subroutine che non conosciamo e viene impostato il valore del registro eax come 1 (presumibilmente vero)
In caso non ci fosse connessione viene eseguita la stessa subroutine e viene impostato eax a 0 (usando il confronto con se stessa in xor)

CODICE	SIGNIFICATO
PUSH EBP	INSERISCE EBP IN CIMA ALLO STACK
MOV EBP, ESP	IMMETTE IL VALORE DI ESP ALL'INTERNO DI EBP
PUSH ECX	METTE ECX IN CIMA ALLO STACK
PUSH 0 ; DWRESERVED	METTE IL VALORE 0 IN DWRESERVED IN CIMA ALLO STACK
PUSH 0 ; LPDWFLAGS	METTE IL VALORE 0 IN LPDWFLAGS IN CIMA ALLO STACK
CALL DS:INTERNETGETCONNECEDSTATE	CHIAMA LA FUNZIONE
MOV [EBP+VAR_4],EAX	IMMETTE IL VALORE CONTENUTO IN EAX IN [EBP+VAR_4]
CMP [EBP+VAR_4], 0	FA LA COMPARAZIONE TRA IL VALORE CONTENUTO IN [EBP+VAR_4] E 0

JZ	SALTA SE LA FLAG ZERO DELLA PRECEDENTE COMPARAZIONE È VERA
PUSH OFFSET ASUCCESSINTERNE	METTE IN CIMA ALLO STACK L'OFFSET SELEZIONATO
CALL SUB_40117F	CHIAMA LA SUBROUTINE
ADD ESP,4	AGGIUNGE 4 AD ESP
MOV EAX, 1	INSERISCE IL VALORE 1 IN EAX

JUMP	ESEGUE UN JUMP NON CONDIZIONALE
LOC_40102B	"SEGNALIBRO" DI INDIRIZZO DI MEMORIA
PUSH OFFSET AERROR1_NOINTE	METTE IN CIMA ALLO STACK L'OFFSET SELEZIONATO
CALL SUB_40117F	CHIAMA LA SUBROUTINE
ADD ESP,4	AGGIUNGE 4 AD ESP

XOR EAX,EAX	CONFRONTA EAX CON SE STESSA RESETTANDOLA
LOC_40103A	“SEGNALIBRO” DI INDIRIZZO DI MEMORIA
MOV ESP, EBP	IMMETTE IL VALORE DI EBP IN ESP
POP EBP	TOGLIE EBP DALLO STACK DI MEMORIA
RETN	RITORNA AL PROGRAMMA CHIAMANTE
SUB_401000 ENDP	ENDPOINT DELLA SUBROUTINE

Grazie!