Progetto week 2 unit 3

Analisi statica contenuti “Malware_U3_W2_L5”

Malware_U3_W2_L5.exe

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

Come si puo vedere dall’immagine sopra usando CFF explorer ricaviamo che le librerie importate sono:

- KERNEL32.dll che è una libreria che contiene le funzioni principali per interagire col sistema
- WININET.dll che è una libreria con funzioni per l’implementazione di alcuni protocolli di rete come HTTP, NTP, FTP.

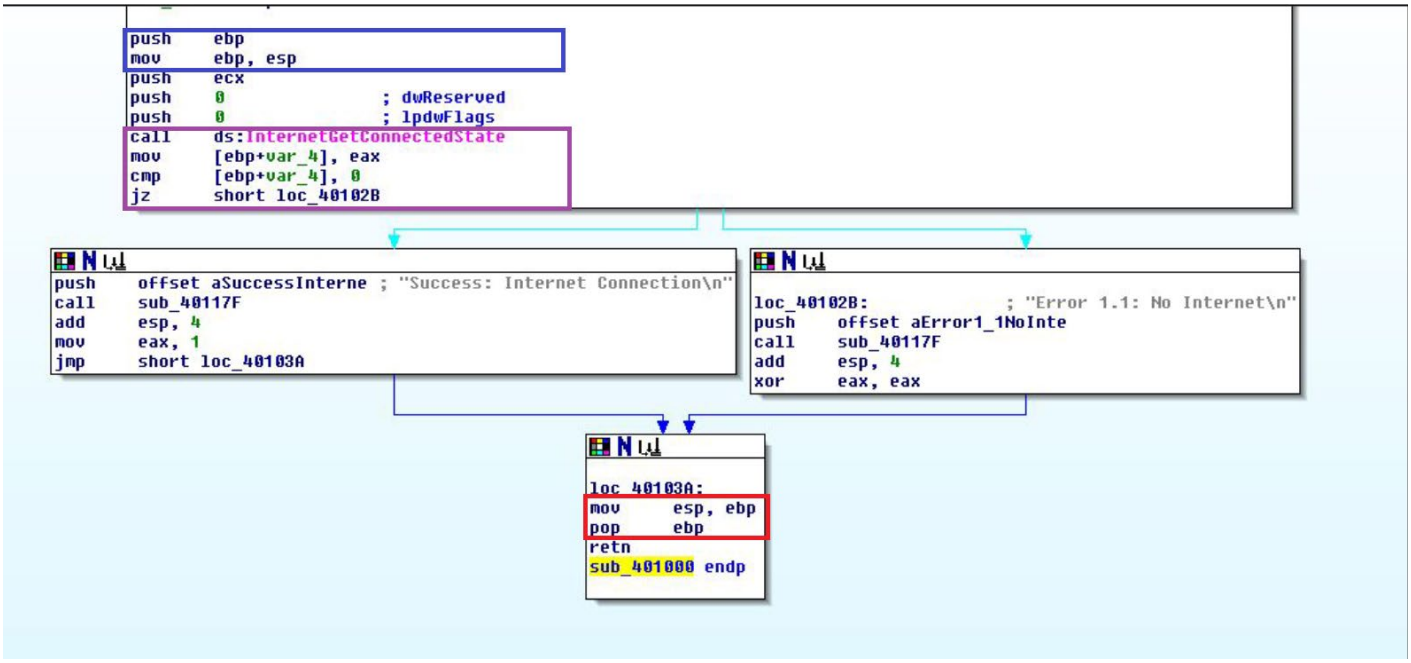
Malware_U3_W2_L5.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	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

Seguendo qui è possibile vedere le sezioni che compongono il file eseguibile del malware, tra cui possiamo vedere:

- “**.text**” che contiene righe di codice che la CPU eseguirà all’avvio del software.
- “.**rdata**” include in modo generale le informazioni riguardanti le librerie e le funzioni importate/esportate dal software
- “**.data**” contiene dati/variabili globali del programma eseguito.

Analisi codice Assembly slide 3



Possiamo vedere:

- BLU: La creazione della stack
- VIOLA: Comparazione con IF (cmp) delle variabili e se nella riga “jz” sotto il risultato corrisponde a 1 (ZF=1) salta al locazione che fa il printf del messaggio di errore, se diverso la connessione risulta riuscita
- ROSSO: La Rimozione della stack

Da questo codice possiamo dedurre che il malware fa un check della connessione internet e se risulta assente stampa un errore di mancata connessione, invece nel caso contrario stampa un messaggio di connessione riuscita e chiude la stack.