Progetto Epicode 01.12.2023

Christian Huamacto

Malware Analisys

- Individuare ed esporre le librerie che importa l’eseguebile “Malware_U3_W2_L5.exe”
- Individuare ed esporre le sezioni da cui è composto l’eseguibile “Malware_U3_W2_L5.exe ”
- Con riferimento al pezzo di codice Assembly X86, nella slide 5, identificare I costrutti noti e ipotizzare il comportamento della funzionalità implementata

Librerie importate

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

Utilizzando CFF Explorer, possiamo scegliere il file da analizzare (in questo caso “Malware_U3_W2_L5.exe”) e quindi individueremo le seguenti librerie:

- **KERNEL32.dll:** questa libreria contiene le funzioni principali per interagire con il sistema operativo
- **WININET.dll:** questa libreria contiene le funzioni per l’implementazione di alcuni protocolli di rete come HTTP, FTP, NTP

Sezioni del Malware

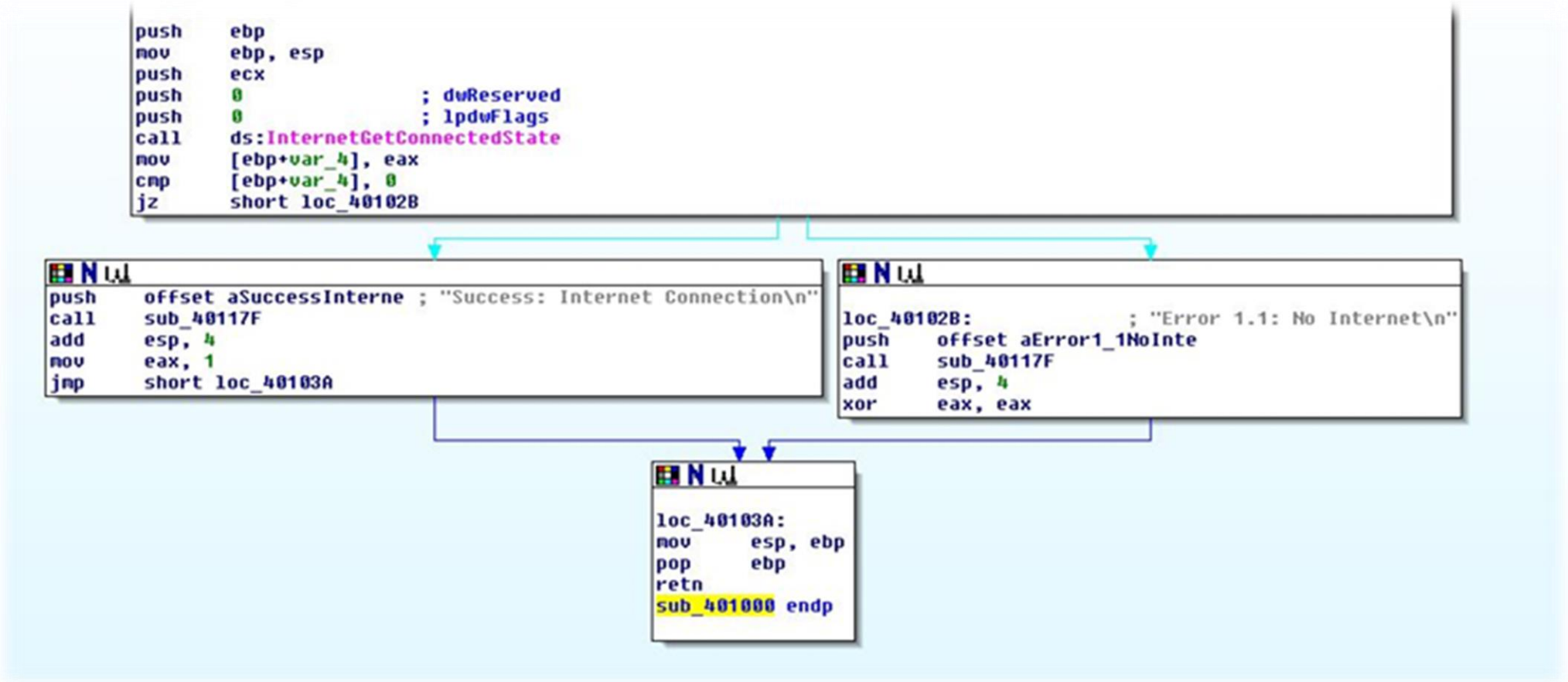
Sempre utilizzando CFF Explorer possiamo ricavare le sezioni da cui è composto il malware .

- **.text:** contiene le righe di codice che la CPU eseguirà una volta che il software sarà avviato.
- **.rdata:** include le informazioni delle librerie e delle funzioni importate ed esportate dall'eseguibile.
- **data:** di solito contiene i dati o le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma

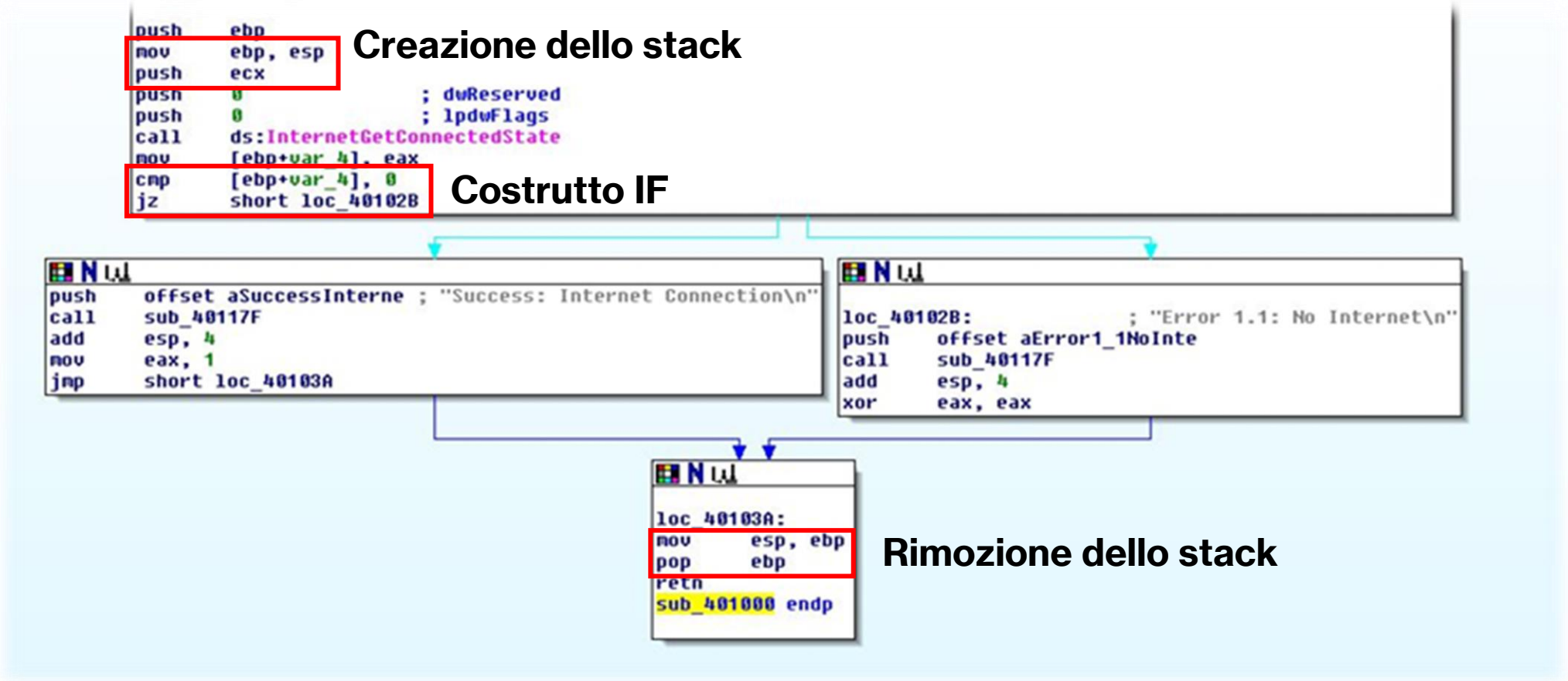
Malware_U3_W2_L5.exe

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

Codice in Assembly x86



Identificazione costrutti noti



Ipotesi sul comportamento della funzionalità utilizzata

Il seguente frammento di codice in Assembly ci indica che attraverso la funzione **InternetGetConnectedState**, si determina se su una macchina è presente una connessione internet.
Tramite il **costrutto IF**, avviene un controllo sulla funzione, che a seconda del parametro restituito (uguale a 0/diverso da zero) ci indica a schermo la presenza o meno di una connessione internet sulla macchina target. Nel caso della presenza di una connessione internet, ci restituirà il messaggio '**Success: Internet Connection**', viceversa avremo '**Error 1.1: No Internet**'.

Grazie