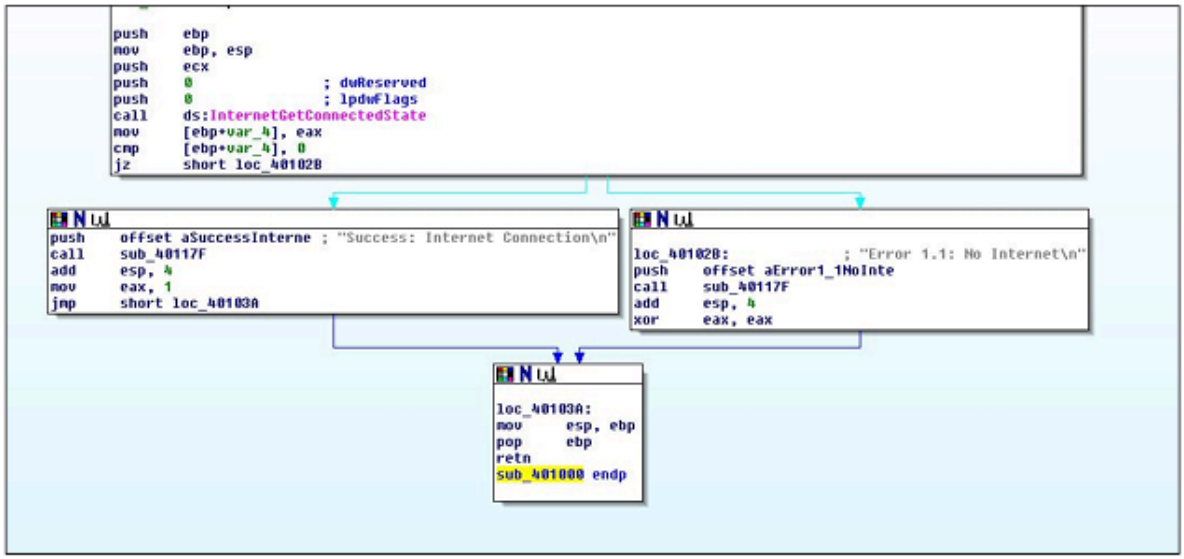
Cyber Security & Ethical Hacking

Progetto S10/L5

Analisi statica e dinamica: approccio pratico

Figura 1



Traccia

Con riferimento ai file presenti all'interno della macchina virtuale dedicata per l'analisi dei malware, rispondere ai seguenti quesiti:

- Quali librerie vengono importate dal file eseguibile?
- Quali sono le sezioni di cui si compone il file eseguibile del malware?

Con riferimento alla figura, risponde ai seguenti quesiti:

- Identificare i costrutti noti (creazione dello stack, eventuali cicli, costrutti)
- Ipotizzare il comportamento della funzionalità implementata

Svolgimento

Parte I

In questo progetto ci chiedeva di rispondere dei quesiti, facendo riferimento al file "Malware_U3_W2_L5", presente nella macchina virtuale dedicata apposta.

Primo quesito:

- Quali librerie vengono importate dal file eseguibile?

Utilizzando il tool CFF Explorer, andiamo a vedere le librerie che vengono importate dal file, che sono: **KERNEL32.dll and WININET.dll**

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

KERNEL32.dll contiene le funzioni principali per interagire con il sistema, mentre **WININET.dll** contiene la funzione di implementare alcuni protocolli di rete.

Secondo quesito:

- Quali sono le sezioni di cui si compone il file eseguibile del malware?

Utilizzando sempre il tool CFF explorer, ci spostiamo nel pannello "Section Headers" per andare a controllare i file eseguibili del malware.

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

Le sezioni che troviamo sono: **.text, .rdata and .data**

.text contiene le istruzioni per la CPU dove eseguirà il software quando sarà avviato.

.rdata contiene le informazioni delle librerie e le funzioni importate/esportate dall'eseguibile.

.data contiene i dati globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Parte II

Nella seconda parte del progetto chiede sempre di rispondere ai quesiti, facendo riferimento alla figura 1.

Primo quesito:

- Identificare i costrutti noti (creazione dello stack, eventuali cicli, costrutti)

Creazione dello stack

Ciclo IF

Secondo quesito:

- Ipotizzare il comportamento della funzionalità implementata

Tramite questo codice si può capire se la macchina sia connessa o no a Internet, nel ciclo if si possono vedere i due messaggi se c'è o no la connessione.


push offset aSuccessInterne ; "Success: Internet Connection\n"
call sub_40117F
add esp, 4
mov eax, 1
jmp short loc_40103A
loc_40102B: ; "Error 1.1: No Internet\n"
push offset aError1_1NoInte
call sub_40117F
add esp, 4
xor eax, eax