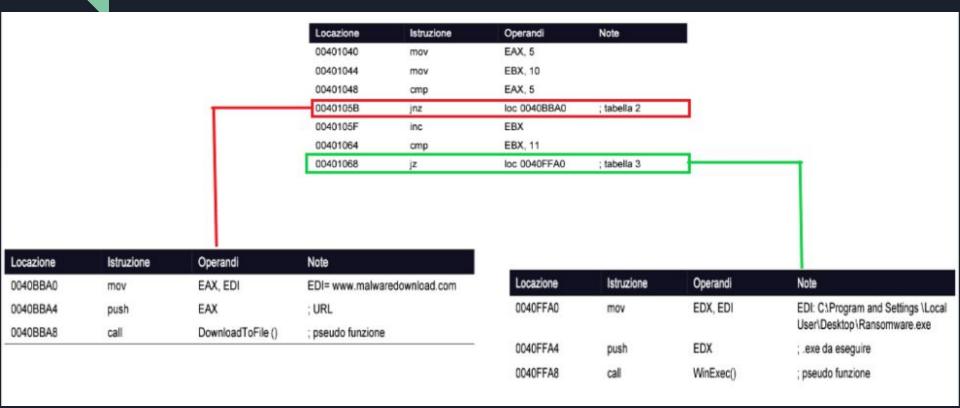
# UNITÀ 3 SETTIMANA 3 COMPITO 5

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.

#### TRACCIA 1°

Il malware effettua un salto condizionale alla locazione 0040BBA0 se il confronto tra il registro EAX e il valore 5 non dà esito positivo (non zero). Successivamente, se il registro EBX è incrementato e il risultato del confronto tra EBX e 11 è positivo (zero), viene effettuato un altro salto condizionale alla locazione 0040FFA0.



Le diverse funzionalità implementate all'interno del malware includono:

Download di un file da un URL specifico (www.malwaredownload.com) e salvataggio su disco.

Esecuzione di un file . exe dal percorso specificato (C:\Program and Settings\Local User\Desktop\Ransomware.exe).

Per quanto riguarda le istruzioni call presenti nelle tabelle 2 e 3, i dettagli tecnici dipendono dal contesto e dalle convenzioni di chiamata della specifica architettura e del sistema operativo di destinazione. Tuttavia, generalmente, nell'esempio fornito, gli argomenti delle chiamate di funzione vengono passati attraverso i registri. Ad esempio, prima della chiamata a DownloadToFile(), l'URL viene caricato nel registro EAX e poi spinto nello stack per essere utilizzato dalla funzione. Similarmente, prima della chiamata successiva, il percorso del file .exe viene caricato nel registro EDX e spinto nello stack.