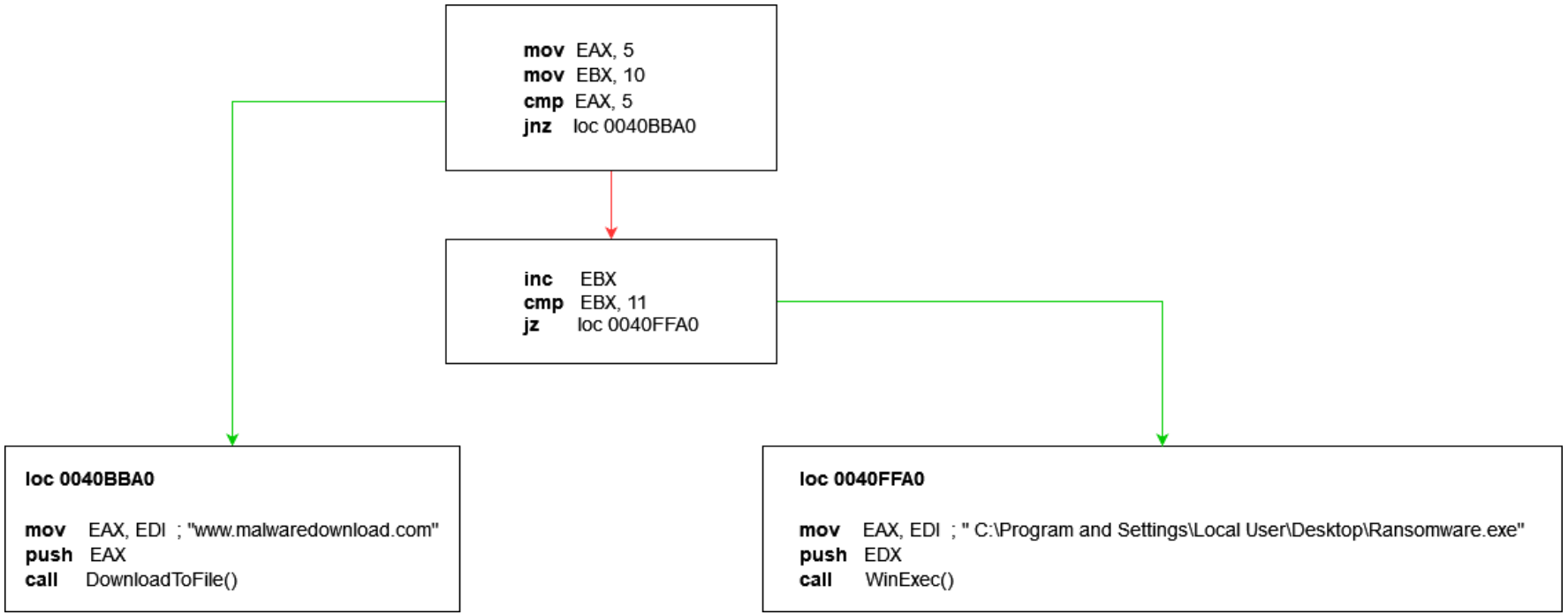
In questo esercizio andremo ad investigare il codice di un malware in assembly x86, visibile nel diagramma di flusso qui sotto.
Iniziamo subito dall'individuare i due salti condizionali che vengono effettuati (freccie verdi):

- **jnz** sarebbe un "Jump not zero", ovvero viene effettuato il jump se la "zero flag" non è settata, ovvero se in "cmp EAX, 5" EAX non corrisponde a 5. In questo caso il jump viene effettuato verso l'URL "www.malwaredownload.com" (Possibile malware downloader). In caso contrario il jump non viene effettuato (freccia rossa) e prosegue fino al **jz**.

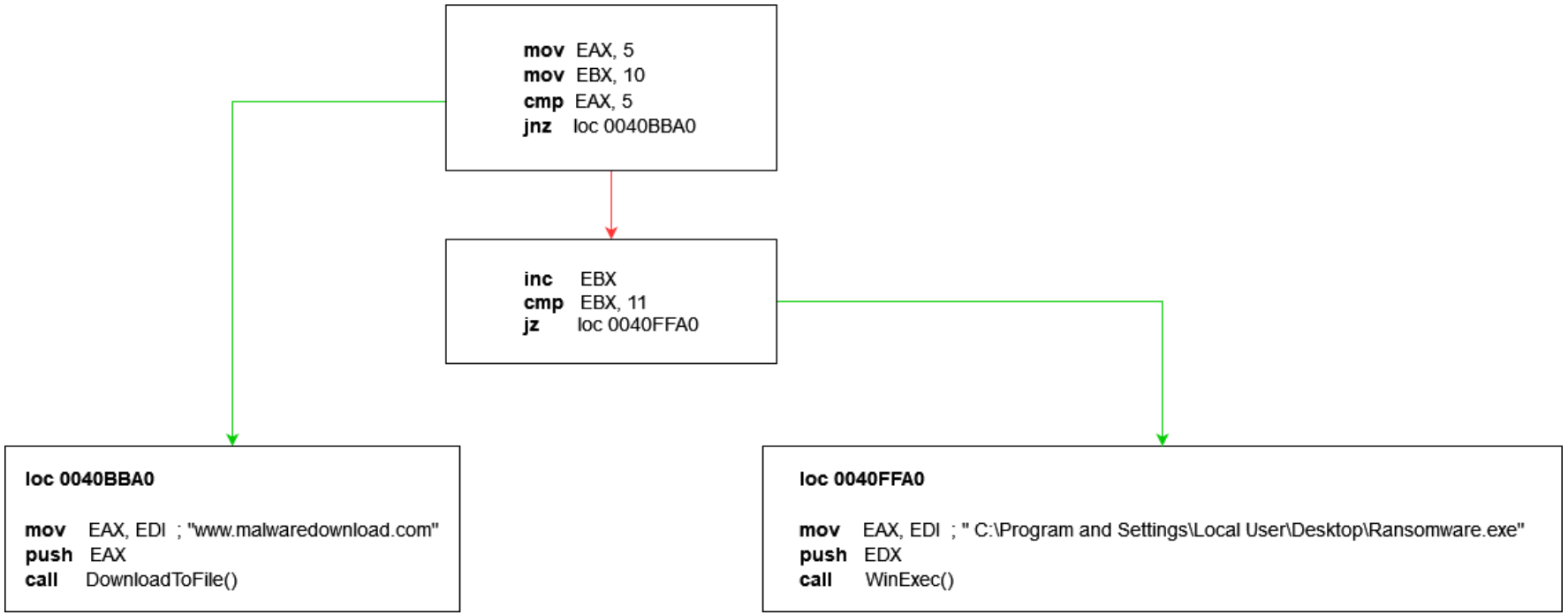
- **jz** sarebbe l'esatto contrario, "jump zero", il jump viene effettuato se la "zero flag" è settata, ovvero se in "cmp EBX, 11" EBX è uguale ad 11. In caso contrario potrebbe esserci del codice in più che non viene mostrato, ma in questo caso il jump viene effettuato verso una directory contenente un file chiamato "Ransomware.exe", un eseguibile (possibile ransomware).



Passiamo adesso ad evidenziare alcune funzionalità del malware. Oltre ai salti condizionali implementati all'interno del codice, ci sono altre due "azioni" che può effettuare:

- **Download di file**, tramite il primo salto condizionale **jnz**, il programma viene indirizzato sull'URL "www.malwaredownload.com" e tramite la chiamata di funzione "DownloadToFile()" potrebbe dare la possibilità al malware di scaricare nel sistema ulteriori file malevoli, come un downloader.

- **Esecuzione di file malevoli**, tramite il secondo salto condizionale jz, il programma invece viene indirizzato verso una directory con all'interno un file eseguibile, sicuramente malevolo. Nel caso fosse un ransomware, crittograferebbe tutti i file nel sistema, per poi chiedere un riscatto per decrittografarli.



Le due funzioni che ritroviamo in questo malware sono:

- **DownloadToFile,** dove il primo argomento, EAX, sarebbe l'indirizzo/URL del file da scaricare, mentre il secondo argomento è EBX, ovvero dove dovrà esser salvato il file una volta scaricato.

- **WinExec** invece viene eseguita con un solo argomento, EAX sarebbe la directory nel quale c'è il file da eseguire.

Possiamo dedurre quindi che potrebbe trattarsi di un Downloader/Ransomware, il programma fa il primo salto condizionale **jnz** viene reindirizzato sull'URL, scarica e salva il ransomware alla directory selezionata. Ricomincia, effettua il secondo salto condizionale **jz** ed esegue il ransomware.