**PROGETTO SETTIMANALE – ANALISI AVANZATE**

**Punto 1**

Il malware esegue il seguente salto condizionale:



In quanto “**jz”** esegue il salto condizionale quando la comparazione ha risultato POSITIVO (ZF=1), ovvero gli operandi corrispondono. Questa comparazione è



EBX (11) = 11. VERO (ZF=1) —-> jz effettua il salto

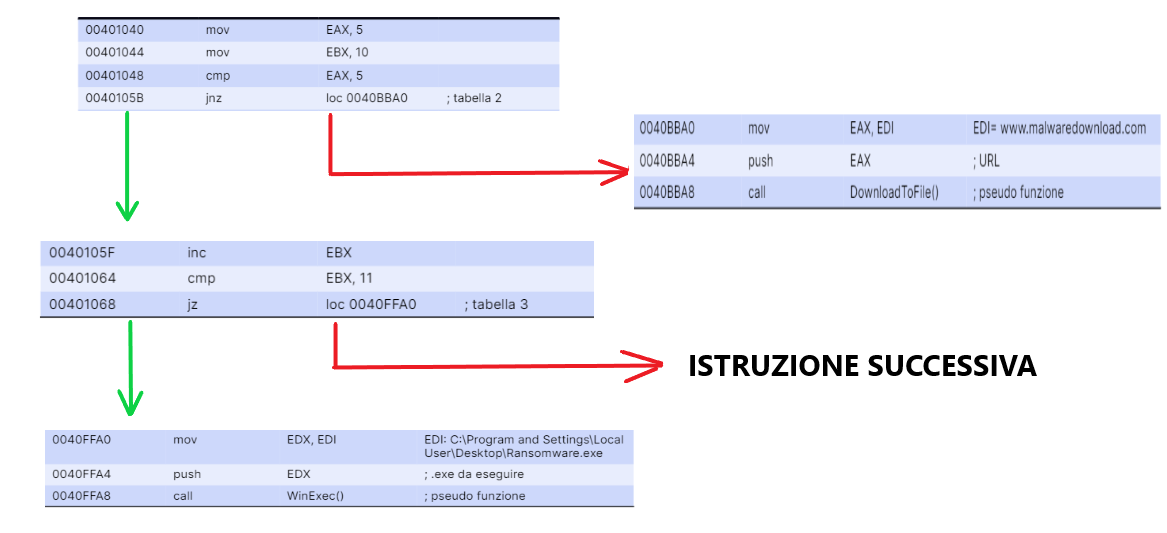
L’altro salto condizionale presente nel codice non viene effettuato poiché **“jnz”** esegue il saldo quando la comparazione ha risultato negativo cioè (ZF=0), ovvero gli operandi non corrispondono. La comparazione eseguita è la seguente:



EAX (5) = 5. VERO (ZF=1) —-> jnz NON effettua il salto.

**Punto 2**

Di seguito troviamo il diagramma di flusso stile IDA, nel quale con la freccia **ROSSA** vengono indicati i salti condizionali non effettuati, mentre con la freccia **VERDE** quelli eseguiti.



**Punto 3**

Le diverse funzionalità implementate all’interno del malware sono 2:

- La prima, riguarda la chiamata alla funzione “DownloadToFile” per gestire il download di un file, che tuttavia non viene eseguita in quanto il salto condizionale non viene effettuato. Presumibilmente questo file si tratta di un altro malware e verrebbe scaricato dall’URL: www.malwaredownload.com. Questa funzionalità è specifica dei malware della famiglia “dropper”.

- La seconda viene invece eseguita e attraverso la chiamata alla funzione “WinExec”, il cui scopo primario è creare un processo che andrà ad eseguire il file “Ransomware.exe” situato al path “C:\Program and Settings\Local User\Desktop\”.

**Punto 4**

“call” tabella numero 2



* - Il valore del registro EDI (“www.malwaredownloader.com”) viene scritto, attraverso un “mov”, nel registro EAX;
* - successivamente attraverso un “push”, viene caricato il registro EAX sullo stack;
* - viene infine utilizzata la “call” alla funzione “DownloadToFile” che si eseguirà ed effettuerà le successive istruzioni

“call” tabella numero 3



* - Il valore del registro EDI: (“C:\Program and Settings\Local User\Desktop\Ransomware.exe”) viene scritto, attraverso un “mov”, nel registro EDX;
* - successivamente attraverso un “push”, viene caricato il registro EDX sullo stack;
* - viene infine utilizzata la “call” alla funzione “WinExec” che si eseguirà, creando così un nuovo processo che avvierà l’eseguibile “Ransomware.exe”.