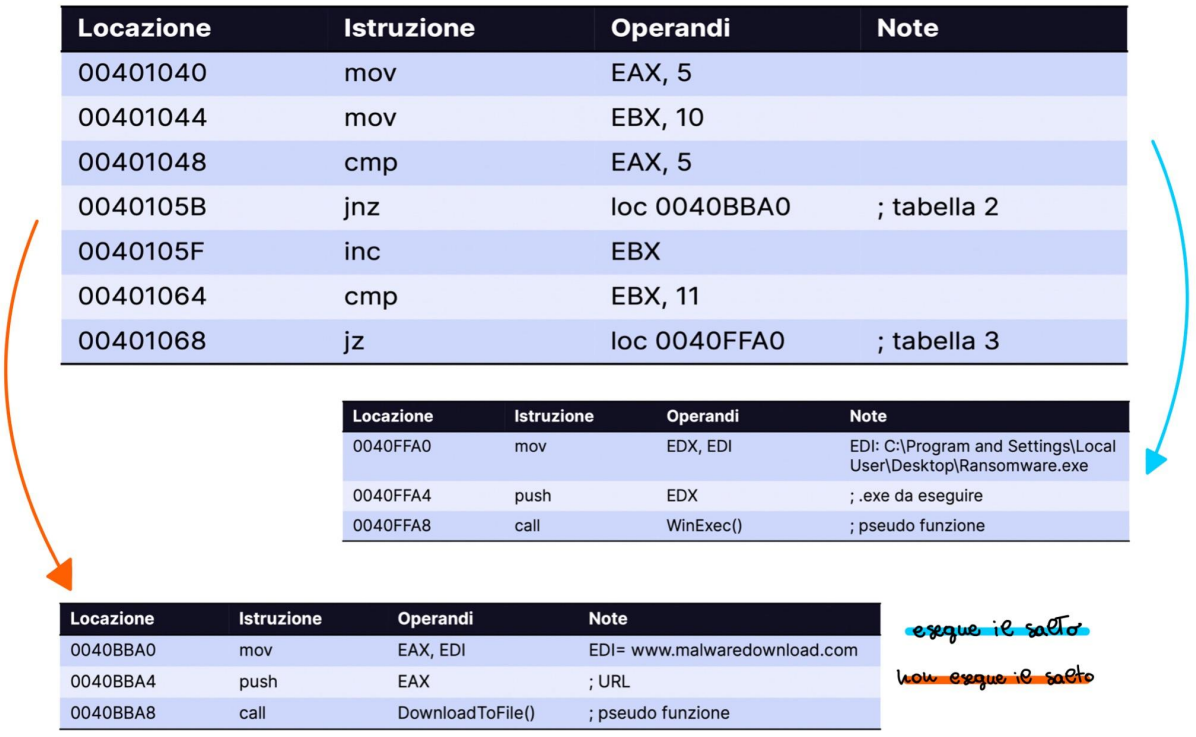
Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

- 1 -

Come si può notare all'inizio delle istruzioni vengono inseriti 5, 10 nei registri **EAX** è **EBX,** dopo di che troviamo un **jnz** che però non verrà eseguito perché **la** cmp precedente confronta **EAX** con 5 il quale è uguale a 0, di conseguenza il salto non verrà eseguito proprio perché non rispetta la condizione.

D'altro canto il salto **jz,** invece verrà eseguito dato che, una volta eseguito un incremento di EBX, abbiamo una **cmp** tra **EBX è 11** risulta appunto uguale a 0, in questo caso la condizione del salto è soddisfatta, si può dunque concludere che il salto effettuato è **jz**

- 2 -



- 3 -

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

- ☐ la Funzione **call WinExec()**
- ☐ la Funzione **call DownloadToFile()**

- 4 -

I parametri della funzione **call WinExec()** vengono passati copiando dentro il registro **EDX** il contenuto del registro **EDI**, è poi inserendo tramite il comando **push** il registro **EAX** nella stack che andrà ad utilizzare la funzione call.

Mentre i parametri della funzione **call DownloadToFile()** vengono passati copiando al interno di **EAX** il contenuto di **EDI**, ed infine si inserisce tramite il comando **push** il registro **EAX** nella stack che andrà ad utilizzare la funzione call.