REPORT

30/09/2022

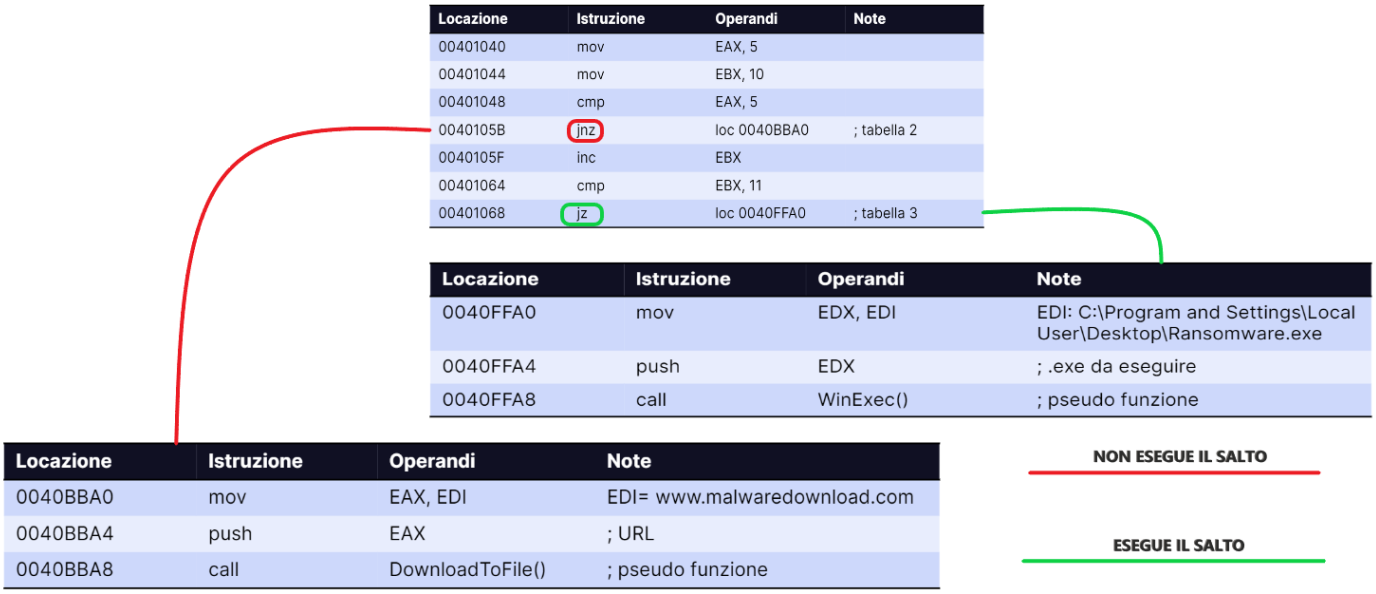
1. In riferimento alla tabella 1:

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

possiamo notare che all'inizio delle istruzioni vengono inseriti i valori 5 e 10 rispettivamente nei registri **EAX** e **EBX**. Successivamente troviamo una **jnz** (jump if not zero) che non viene eseguita poiché la **cmp** (compare) precedente compara **EAX** con 5 che è uguale a 0, quindi il salto non rispetta la condizione e non viene eseguito.

Il salto successivo **jz** (jump if zero), invece, viene eseguito dato che, dopo aver effettuato un incremento di **EBX** (quindi 10+1), abbiamo una **cmp** (compare) tra **EBX** e 11 che è uguale a 0. La condizione del salto è verificata e di conseguenza possiamo concludere che il salto effettuato è **jz** (jump if zero).

2. Diagramma di **flusso**:



3. Le funzionalità implementate dal Malware sono la funzione **call WinExec()** che crea un nuovo processo e la funzione **call DownloadToFile()** che scarica dei file malevoli da Internet.

4. I parametri della funzione **call WinExcec()** vengono passati prima copiando all'interno del registro **EDX** il contenuto del registro **EDI** (il path del file eseguibile **Ransomware.exe**), e poi inserendo con il comando **push** il registro **EDX** nello **stack** che viene utilizzato dalla funzione **call**.

   I parametri della funzione **call DownloadToFile()** vengono passati prima copiando in **EAX** il contenuto di **EDI** (che è il nome del sito da utilizzare **per scaricare i file malevoli**), e poi, come nel caso della funzione precedente, si inserisce con il comando **push** il registro **EAX** nella **stack** che verrà utilizzato dalla funzione **call**.