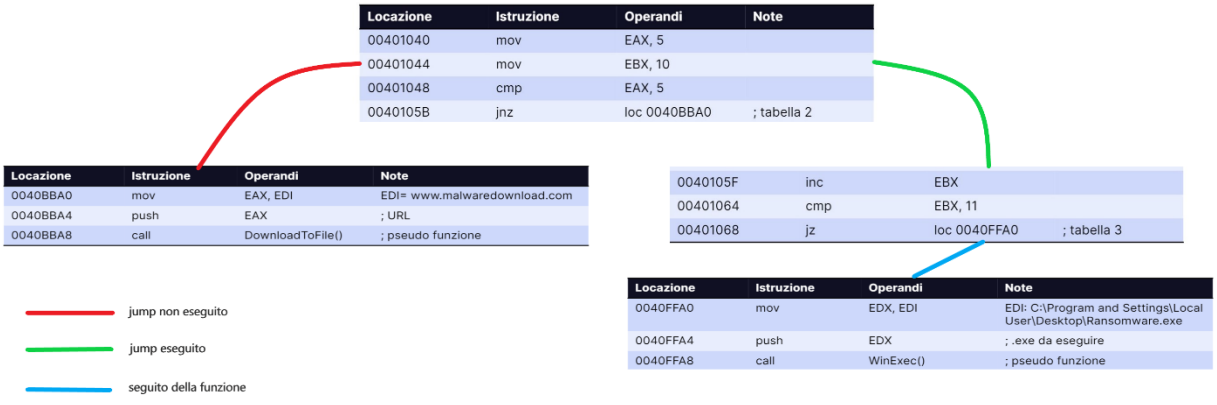
Analisi e grafico del malware

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. Il primo salto, ovvero jnz, non viene effettuato poiché il risultato di cmp è 0, dal momento che EAX ha valore 5 (di conseguenza lo ZF vale 1). Mentre il secondo, quindi jz, viene effettuato poiché EBX – dopo che viene incrementato di uno – ha valore 11 e quindi il cmp risulta 0 (perciò lo ZF ha valore 1); questo avviene perché il jz esegue il salto se il risultato di cmp è 0 e al contrario jnz lo effettua solo se il risultato di cmp è diverso da 0.

2. Diagramma di flusso:



3. La prima funzionalità implementata è tramite “DownloadToFile()” che si occupa di scaricare un file dalla risorsa fornita dal parametro. La seconda funzionalità è data da “WinExec()” che invece crea un processo.

4. *Tabella 2:*

   Innanzitutto viene copiato il contenuto di EDI, ovvero il sito che tiene il download di un altro malware, nel registro EAX. Successivamente viene pushato il registro EAX a cui si rifarà la chiamata alla funzione "DownloadToFile()" che utilizzerà il parametro con al suo interno l'URL per sapere da dove scaricare.

   Tabella 3:

   Prima di tutto viene copiato il contenuto di EDI, quindi il percorso dove è salvato l'esecutivo del ransomware, nel registro EDX. In seguito viene pushato il registro EDX che contiene il .exe da eseguire, così che la funzione "WinExec()" si occuperà di creare il processo con il parametro dato.