PROGETTO SETTIMANA 11

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

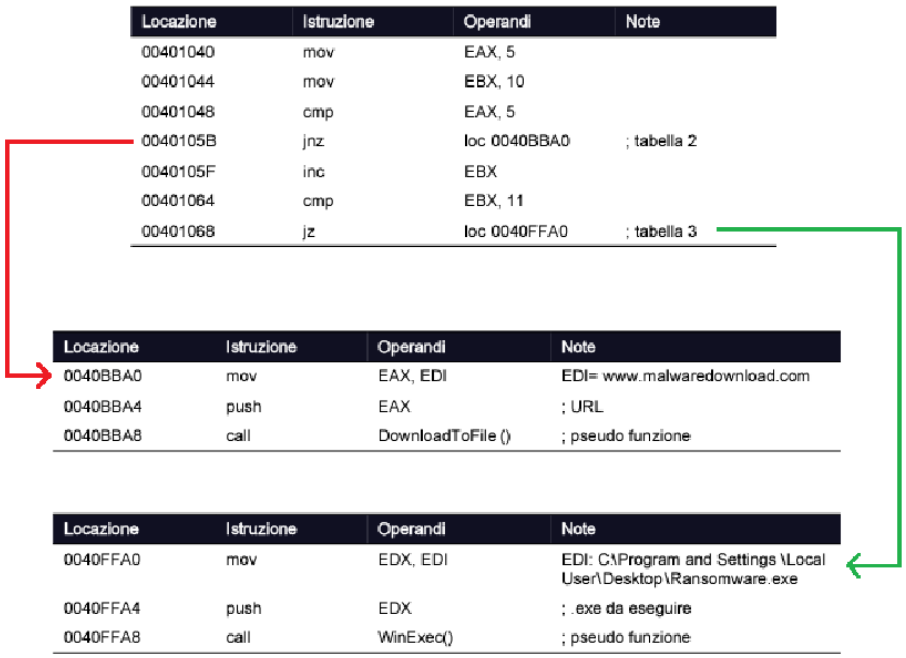
Domanda 1 – salto condizionale

Nel codice il salto condizionale che viene effettuato è il seguente:

- **jz loc0040FFA0**

Qui il salto viene effettuato dopo il confronto tra i registri EBX e 11. Se il registro EAX è uguale a 11 il programma effettua il salto alla locazione **loc0040A0**

Domanda 2 – diagramma di flusso



Domanda 3 – funzionalità implementate

Possiamo individuare due funzionalità implementate all'interno del malware:

- Download di file -> il malware riesce a connettersi all'URL www.malwaredownload.com che è presente nell'indirizzo contenuto in EDI. Questa sequenza di istruzioni termina con la chiamata alla funzione "DownloadToFile()" che è proprio quella che andrà a scaricare il file malevolo.
- Esecuzione di file -> il malware è anche in grado di eseguire un file in formato ".exe" che va a prendere in "C:\Program and Settings\Local User\Desktop\Ransomware.exe". Il file verrà eseguito grazie alla chiamata di funzione "WinWxec()". Questa funzione sarà quella che andrà ad eseguire il file potenzialmente scaricato che sembrerebbe essere un Ransomware.

Domanda 4 – passaggio argomenti alle funzioni

Nella prima chiamata di funzione "**DownloadToFile()**" l'indirizzo di www.malwaredownload.com, che è contenuto in EDI, viene caricato nel registro EAX. Viene poi eseguito un push di EAX sullo stack per passare l'URL come argomento della funzione, che verrà poi chiamata.

Nella seconda chiamata di funzione "**winExec()**" il path del file, contenuto anch'esso in EDI, viene caricato nel registro EDX. Successivamente viene eseguito un push di EDX per passare alla funzione come argomento il path del file.

In entrambi i casi gli argomenti delle funzioni vengono passati attraverso lo stack