# **PROGETTO S11 L5**

## **Assembly**

- 1. Quale salto effettua il malware.
- 2. Disegno del diagramma di flusso
- 3. Funzionalità implementate all'interno del malware
- 4. Istruzione call, 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

## 1. Quale salto condizionale effettua il malware.

Il salto condizionale che effettua il Malware è il seguente

0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Viene effettuato il salto condizionale alla **loc 0040FFA0** in quanto, il valore inziale di **EBX** è **10** e successivamente viene incrementato di **1**, divenendo **11.** Successivamente viene comparato con "**cmp EBX**, **11**". Poiché i valori sono uguali, si procede all'esecuzione del salto condizionale alla **loc** 

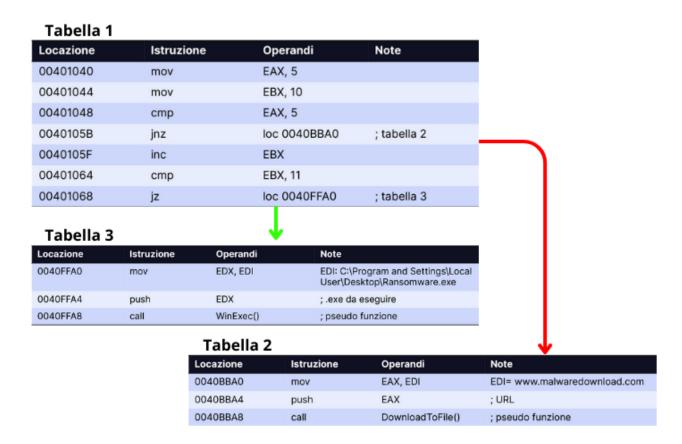
**0040FFA0**, poiché *jz* (Jump to Zero) viene eseguito solamente se la comparazione precedente restituisce 0.

Non viene eseguito il salto condizionale precedente, ossia:

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2

Poiché, una volta equiparati i due valori con "cmp EAX, 5", otteniamo come risultato 0, poiché uguali, avendo un salto condizionale di tipo jnz (Jump Not to Zero) non viene quindi eseguito poiché avverrebbe solamente a condizione che il risultato della precedente comparazione restituisse un valore diverso da 0.

#### 2. Disegno del diagramma di flusso



#### 3. Funzionalità implementate all'interno del malware

All'interno del Malware troviamo principalmente due funzionalità:

- Download di un file da un URL
- Esecuzione di un file malevolo

La prima funzionalità che incontriamo è quella riportata nella Tabella 2, in cui troviamo il download di un file dal sito **www.malwaredownload.com**. Il downloader è un programma che scarica da Internet un malware oppure un componente di esso e lo esegue sul sistema target. In fase di analisi, possiamo identificare un download in quanto utilizzerà inizialmente l'API URLDownloadToFile() per scaricare bit da Internet e salvarli all'interno di un file sul disco rigido del computer infetto.

La seconda funzionalità che troviamo è nella Tabella 3 che permette l'esecuzione di

#### C:\ProgramandSettings\LocalUser\Desktop\Ransomware.exe.

Una funzione di tipo **dropper**, che permette l'installazione e l'esecuzione immediata o futura del malware, indicando il percorso in cui è memorizzato.

# 4. Istruzione call, come sono passati gli argomenti alle successive chiamate di funzione.

Nel caso della funzione **DownloadToFile** la logica di esecuzione è abbastanza semplice, viene impostato come parametro **EDI** l'Url del sito, viene poi spostato in **EAX**, con la funzione *mov*. Il parametro **EAX** viene poi inserito nello stack con il *push* e viene utilizzata la pseudofunzione **DownloadToFile()** per scaricare il malware.

Anche nel caso della chiamata di funzione di **WinEx()** la logica è molto simile a quella della funzionalità precedente, viene spostato il valore **EDI**, corrispondete al percorso del malware, in **EDX** e successivamente inserito nello stack con la funzione *push* e infine viene eseguita la pseudofunzione **WinEx** per eseguire il malware.