PROGETTO S11L5 – LUCA DANELLI

1) Spiegate, motivando, quale salto condizionale effettua il malware

Dall'analisi del codice vediamo che sono presenti due istruzioni di tipo jump, agli indirizzi 0040105B e 00401068. Il primo è di tipo jnz, jump not zero, che viene effettuato se lo zero flag non è settato (quindi vale 0). Il secondo invece è di tipo jz, jump zero, che viene effettuato se lo zero flag è settato (quindi vale 1). Per capire se i salti vengono effettuati occorre esaminare le istruzioni precedenti alle istruzioni jz e jnz:

Salto 1:

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2

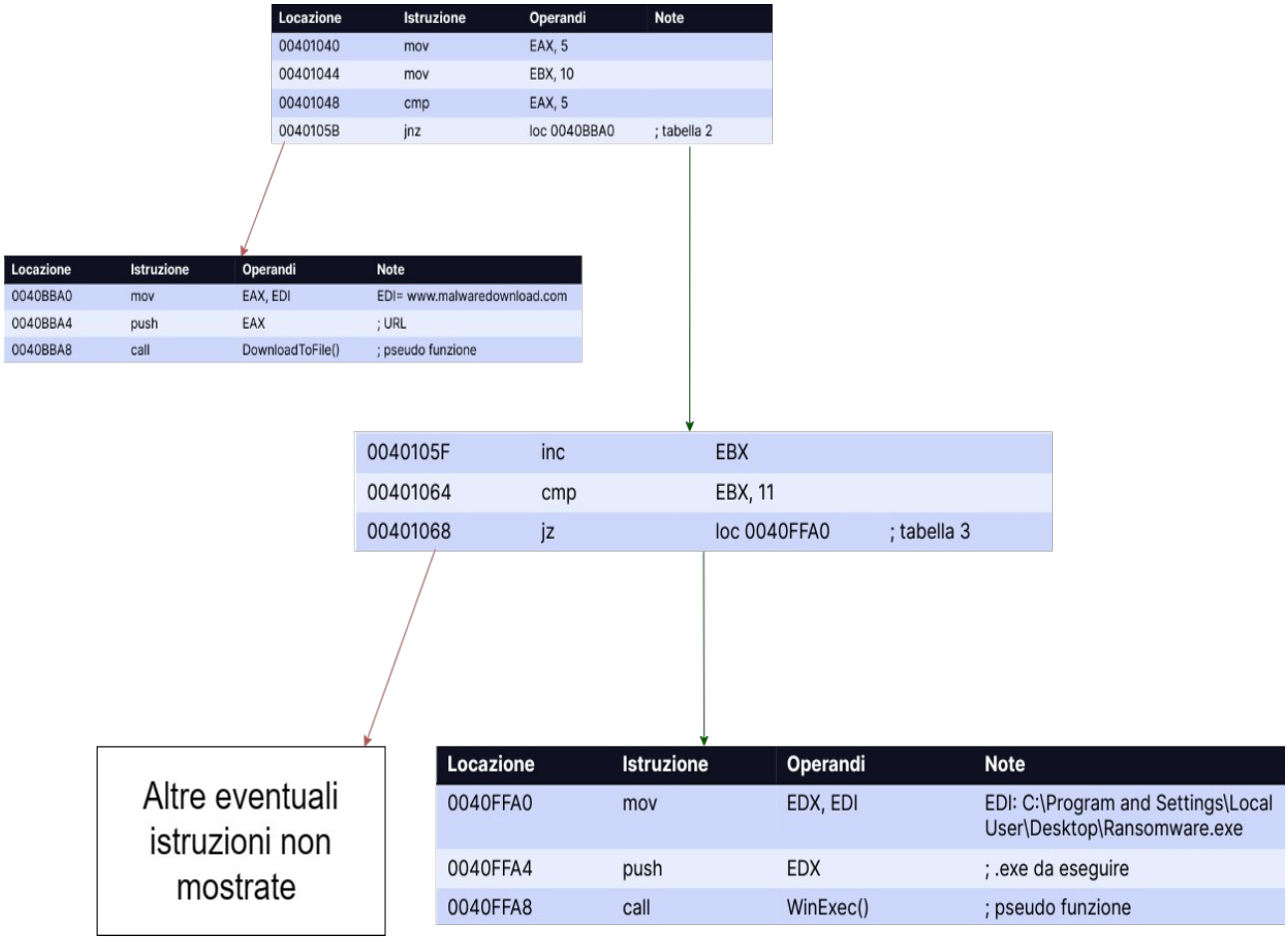
La prima istruzione ci dice che EAX vale 5. Nella terza istruzione viene confrontato il valore di EAX con 5. Essendo i due operandi uguali, l'istruzione compare setterà lo zero flag a 1 e quindi il primo salto **non** verrà effettuato. Il programma quindi eseguirà l'istruzione successiva al jump senza spostarci sull'indirizzo di memoria specificato 0040BBA0

Salto 2:

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

Nella prima istruzione il registro EBX viene incrementato di 1. Dall'istruzione all'indirizzo 00401044 del primo screenshoot sappiamo che il suo valore era 10, quindi ora vale 11. Successivamente il suo valore viene comparato proprio con 11, e quindi lo zero flag verrà settato a 1.In questo caso quindi l'esecuzione del programma **salterà** all'indirizzo specificato 0040FFA0

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?

Il codice del malware supporta le funzionalità di download e di esecuzione processi. La funzione DownloadToFile() è usata per scaricare file da internet sulla macchina attaccata, una volta passato l'url per il download, mentre la funzione WinExec() viene utilizzata per creare un processo una volta specificato il path del file da eseguire sulla macchina infetta.

4) Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

Funzione DownloadToFile():
Viene copiato il contenuto di EDI in EAX, successivamente viene passato EAX alla funzione come argomento tramite l'istruzione push, che salva il dato in cima allo stack. Dalle note del codice capiamo che probabilmente in un'istruzione precedente è stato salvato l'url di download nel registro EDI.

Funzione WinExec():
Viene copiato il contenuto di EDI in EDX, successivamente viene passato EDX alla funzione come argomento tramite l'istruzione push, che salva il dato in cima allo stack. Dalle note del codice capiamo che probabilmente in un'istruzione precedente è stato salvato il percorso del file da eseguire nel registro EDI.