Analisi avanzate

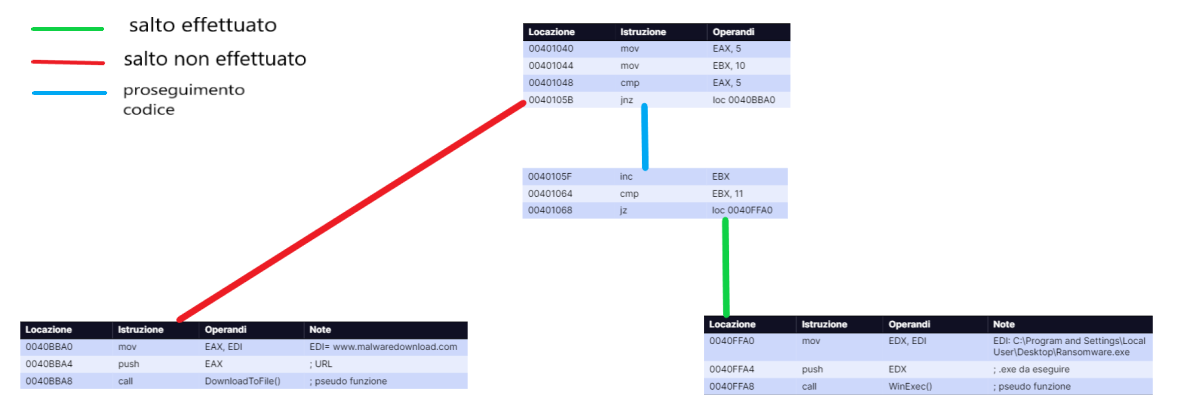
Nell’esercizio di oggi bisognava analizzare il codice di un malware e rispondere a dei quesiti.

1)



In questa tabella possiamo notare due salti, il primo non viene effettuato perché viene passato 5 dentro il registro **EAX** il quale viene comparato (**cmp**) con 5 e quindi il risultato sarà 0. Dato che il risultato è 0 lo **ZF** sarà 1 e quindi non effettuerà il **jnz** (jump if not zero) perché lo **ZF** non è 0. Mentre nel secondo salto viene passato 10 su **EBX**, incrementato di 1 e poi confrontato con 11 il cui risultato sarà 0 e lo **ZF** 1. Dato che abbiamo un **jz** (jump if zero) ovvero salterà in caso lo **ZF** sia 1, allora il salto viene effettuato.

2)



In questa immagine si può notare come un salto verrà effettuato e l’altro no.

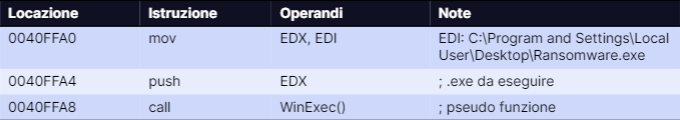
3)

Le funzionalità implementate nel malware sono **WinExec()** che viene usata per creare un processo e **DownloadToFile()** usata per scaricare file da un determinato **URL**.

4)



In questa tabella possiamo notare come viene copiato l’**URL** del malware (**EDI**) dentro il registro **EAX**, il quale viene passato come parametro della funzione **DownloadToFile()**.



Mentre qui viene copiato il percorso dell’eseguibile del malware (**EDI**) dentro il registro **EDX**, il quale viene passato come parametro della funzione **WinExec()**.