REPORT ESERCIZIO SETTIMANALE PRATICO

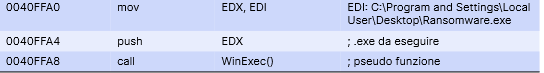
ANALISI MALWARE

Nel seguente report verrano illustrate le seguenti tracce richieste dall’esercizio

1.



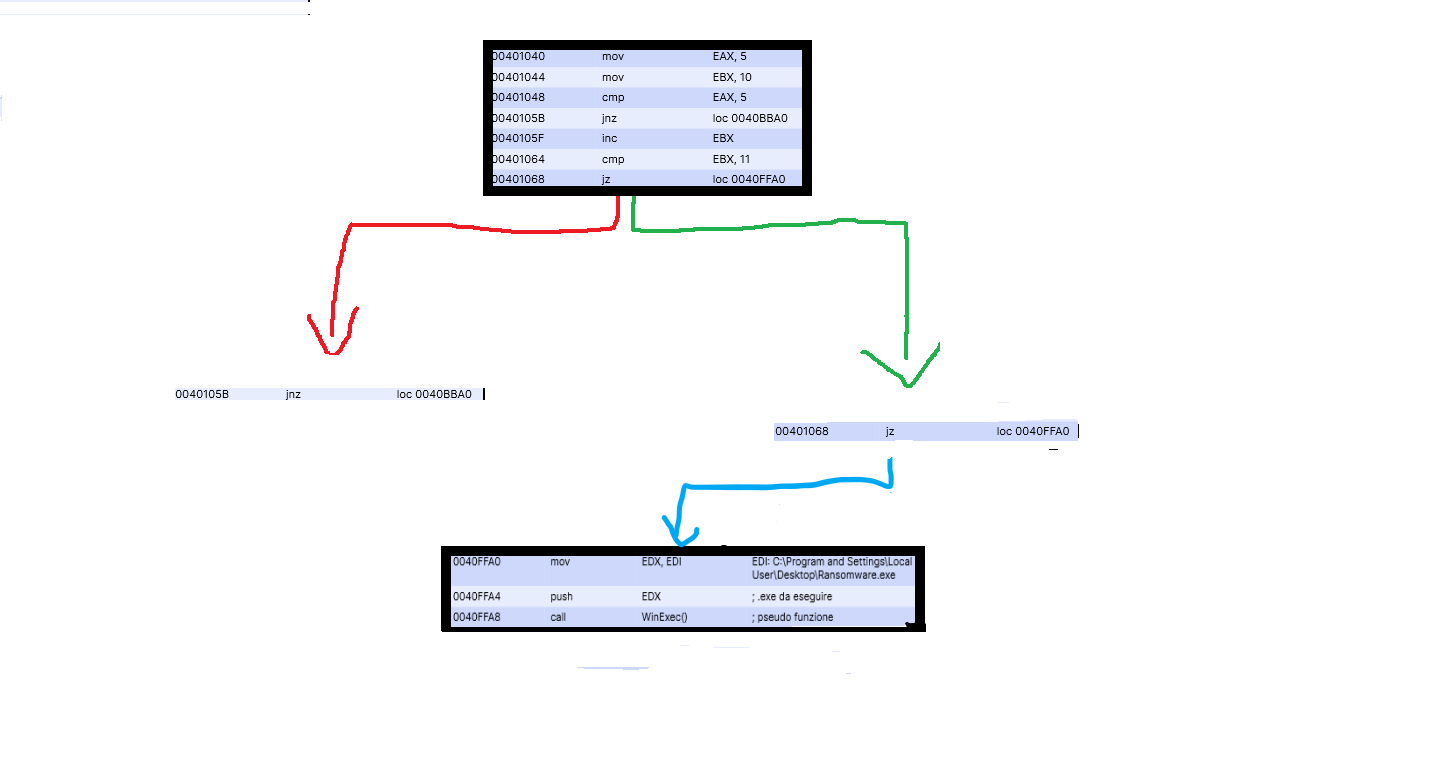
I salti condizionali effettuati sono i seguenti: La funzione jnz loc ha effettuato il jump alla memoria di locazione specifica perché la condizione di zf è su 0 ovvero false, mentre la funzione jz loc ha effettuato il jump perché la condizione di zf è true ovvero zf=1



3&4.

Le funzionalità del malware sono le seguenti illustrate nello screenshot, il malware eseguito effettua una prima chiamata per eseguire il codice (call WinExec(), API di windows che serve per avviare il processo una volta scaricato dalla rete ovvero il ransomware inserito nel registro EDX spostato poi sullo stack), per poi richiamare l’url del sito e di conseguenza effettuare una seconda chiamata (call) in modo da effettuare l’operazione di download (DownloadToFile() ) del file malevolo.

Il passaggio di argomenti viene effettuato dal registro EDI che contiene l’url dove si trova il malware, che viene successivamente inserito nel registro EAX, spostato conseguentemente sullo stack.

2. in questo screenshot sono graficamente illustrati i salti effettuati e non effettuati, comprese le seguenti elaborazioni degli argomenti passati alle successive chiamate delle relative funzioni. Il salto non viene effettuato alla locazione dello stack 00401058 perché il risultato della comparazione zf equivale a 1 ovvero true. Quindi il jump viene fatto da jz.