Analizzare il comportamento del malware

Con riferimento al codice che si trova nelle slides e che metterò di sotto possiamo analizzare quanto segue

Table

Description automatically generated

1. **Salto condizionale**

Il malware esegue il salto condizionale dalla locazione 00401068 alla locazione 0040FFA0

**Esegue il salto** perchè quando facciamo la comparazione tra EBX e 11 il risultato è diverso da 0, quindi 1. Quando il risultato di **jz** equivale a 1, avviene il salto

Il **salto non viene effettuato** alla locazione 00401058 con il comando **jnz** perchè il risultato della comparazione equivale a 1.Dalla tabella vediamo come 5 viene inserito nel registro EAX, che viene comparato con 5.

1. **Diagramma**

**Timeline

Description automatically generated**

1. **Funzionalità Malware**

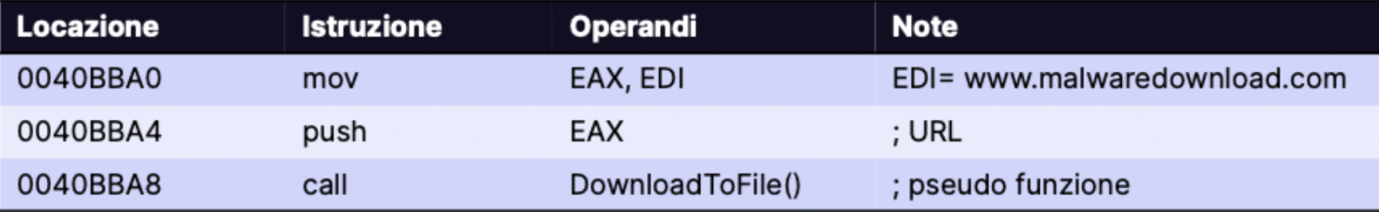
Le funzionalità implementate nel malware sono **DownloadToFile()** e **WinExec()**

* **DownloadToFile():** E un API di windows che serve per scaricare il file malware da internet salvandolo all’interno di un file sul disco rigido del computer infetto
* **WinExec():** E un API di windows che serve per avviare un processo una volta scaricato dalla rete

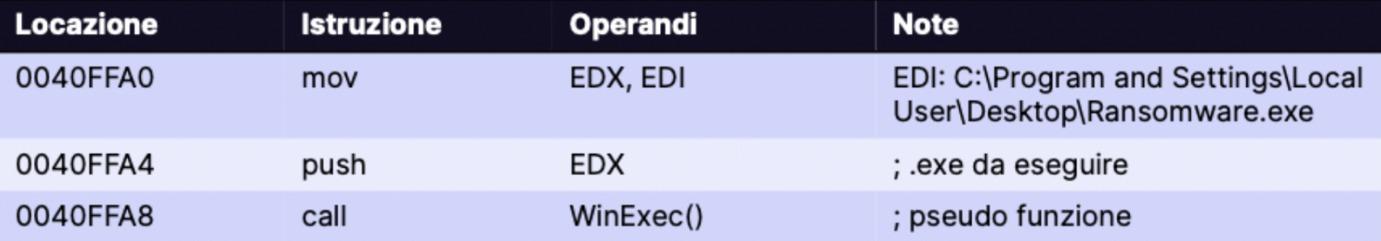
1. **Passaggio di argomenti**

Con riferimento alle istruzioni call presenti nell tabella 2 e 3 possiamo dedurre che:

* Il parametro EDI viene prima inserito nel registro EAX e poi viene pushato l’url ed per finire viene eseguito con la call



* Nella seconda parte viene passato al registro EDX dopodiche viene pushato l’exe ed infine eseguito con il comando WinExec()

****