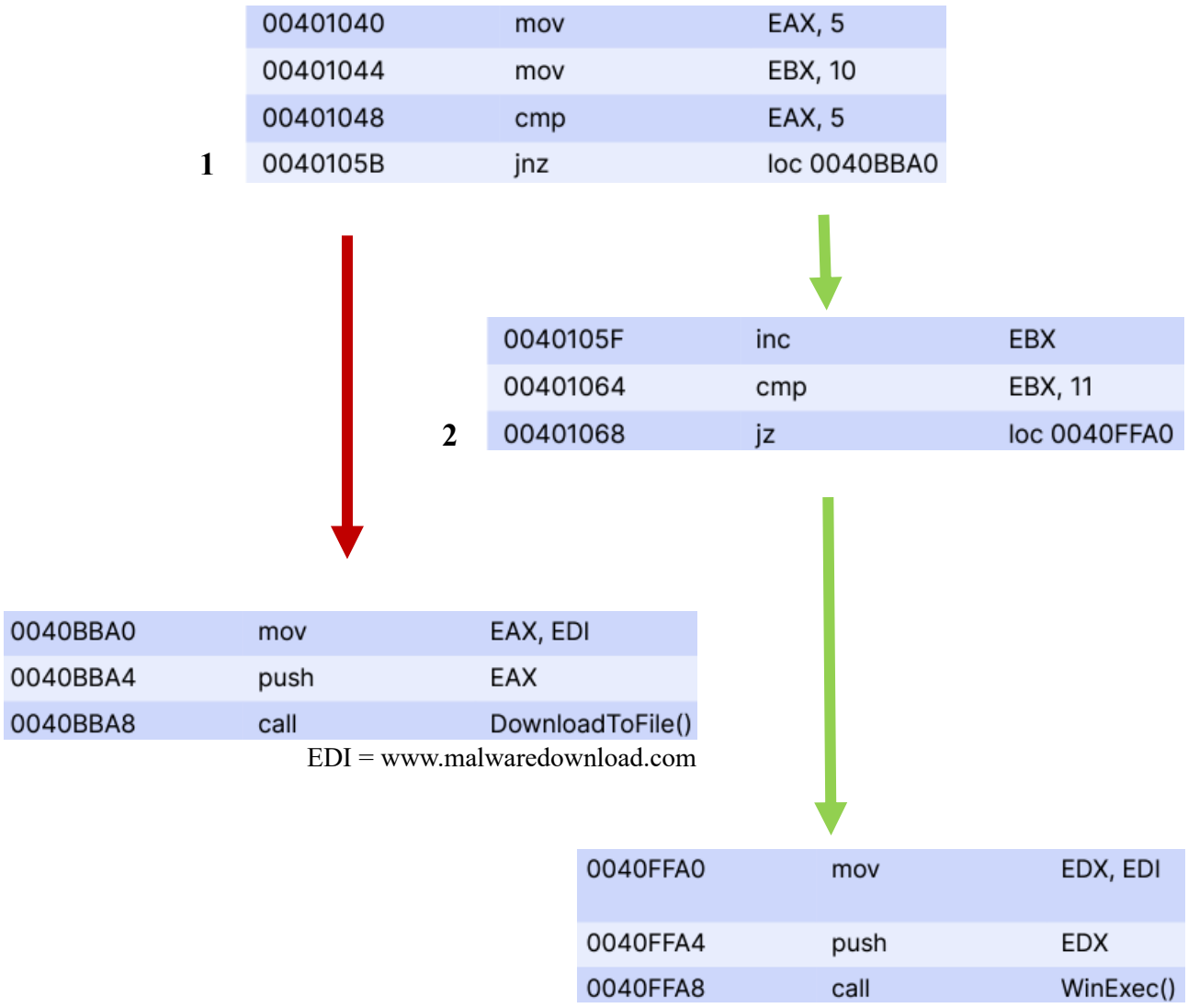
Analisi Comportamento Malware Tramite Codice Assembly

Nel seguente report esamineremo un frammento di un **malware** rappresentato in codice **Assembly**, evidenziandone i relativi **salti condizionali** (mostrando un diagramma di flusso esemplificativo) e le diverse **funzionalità** presenti.

Il codice esaminato è il seguente: è già stato suddiviso ed organizzato in un diagramma di flusso, il quale sarà spiegato di seguito.



Spiegazione salti condizionali

Nel diagramma sopra, le frecce verdi rappresentano lo svolgimento del codice al netto dei salti condizionali. Nel dettaglio:

1. Nel primo blocco di codice, nel registro **EAX** viene copiato il valore 5. Successivamente viene fatto un **paragone** (**cmp)** tra EAX e 5: essendo uguali, ci viene **restituito 0** e quindi la **ZF** viene **settata** a **1**. Il salto condizionale qui presente, **jnz**, avviene se la ZF **NON** è **settata** (quindi **ZF=0**); il salto non viene quindi effettuato e il codice prosegue normalmente (freccia verde a destra). La freccia rossa a

sinistra mostra invece l'eventuale salto che sarebbe stato effettuato sa la condizione di jnz fosse stata veritiera.

2. Nel secondo blocco di codice, **EBX**, a cui era stato assegnato il valore 10, viene **incrementato** (**inc**) divenendo 11. Viene successivamente effettuato un paragone con **cmp** tra EBX e 11 che, avendo lo stesso valore, danno come **risultato 0**; la **ZF** viene quindi **settata** a **1**. Il salto condizionale qui presente, **jz**, avviene se **ZF=1**: la condizione è veritiera e quindi **il salto avviene** verso l'indirizzo indicato, ossia 0040FFA0. Il salto è rappresentato nel diagramma dalla seconda freccia verde.

Funzionalità del malware

Per quanto riguarda il funzionamento del malware, basandoci sul codice qui presente, possiamo immaginare che si tratti di un **downloader** con lo scopo di scaricare ed eseguire un **ransomware**. In particolare, nel primo blocco di codice, il programma esegue un check per decidere se scaricare o direttamente eseguire il codice malevolo:

- Se il ransomware vero e proprio deve essere ancora scaricato, l'eseguibile, attraverso il primo salto condizionale, esegue le istruzioni necessarie per il **download**. In particolare, nel registro **EAX** viene copiato l'indirizzo (con **mov**) dove si trova la stringa dell'**URL**, precedentemente salvata in **EDI**. EAX, e quindi l'URL, è quindi **introdotto nello stack** tramite **push** e successivamente preso come **argomento** dalla funzione chiamata dal **call** alla riga successiva, la quale andrà ad effettuare il download.
- Se il ransomware è già stato scaricato, si passa all'ultimo blocco di codice. Il registro **EDI**, contenente l'indirizzo in cui è salvato il percorso per l'eseguibile **Ransomware.exe**, viene copiato in **EDX** che è poi **introdotto nello stack** da **push**. EDX diviene quindi l'**argomento** della funzione chiamata dal **call** alla riga successiva, ossia un'API di Windows usata per far partire un eseguibile.

Giuseppe Pariota