

S11-L5

MALWARE ANALYSIS

TRACCIA

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

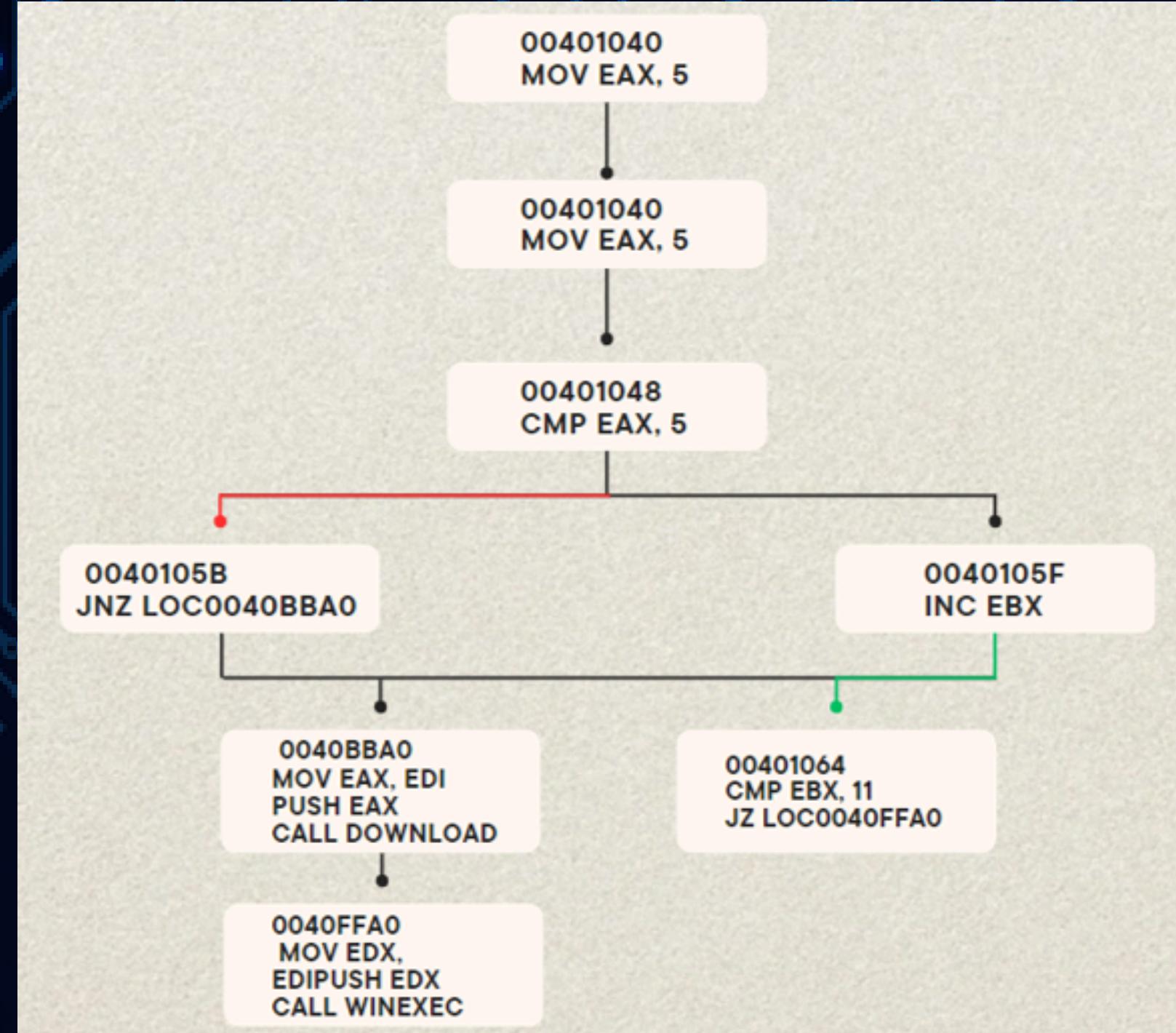
1. Spiegate, motivando, quale salto condizionale effettua il Malware.
2. Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.
3. Quali sono le diverse funzionalità implementate all'interno del Malware?
4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione . Aggiungere eventuali dettagli tecnici/teorici.

SALTO CONDIZIONALE

Un salto condizionale è un'istruzione in linguaggio assembly che fa sì che l'esecuzione del programma passi a un altro indirizzo di memoria solo se una certa condizione è soddisfatta. Nel caso del malware, l'istruzione `jnz loc0040BBA0` situata all'indirizzo `00401048` fa parte della Tabella 1. Questo salto condizionale viene eseguito se il valore contenuto nel registro EAX è diverso da 5. Se EAX è uguale a 5, il salto non avviene e l'esecuzione continua con l'istruzione successiva.

| | | | |
|----------|-----|--------------|-------------|
| 00401048 | cmp | EAX, 5 | |
| 0040105B | jnz | loc 0040BBA0 | ; tabella 2 |

DIAGRAMMA DI FLUSSO



Funzionalità implementare

Le varie funzionalità incorporate all'interno del malware includono il download di un file dal sito www.malwaredownload.com tramite l'uso della funzione downloadtofile.

In altre parole, il malware è programmato per recuperare un file da un indirizzo web specifico, utilizzando una funzione che si occupa di scaricare il file e salvarlo localmente sul sistema infettato. Questa capacità permette al malware di ottenere ulteriori componenti o aggiornamenti direttamente da internet.

| Locazione | Istruzione | Operandi | Note |
|-----------|------------|----------|---|
| 0040BBA0 | mov | EAX, EDI | EDI= www.malwaredownload.com |

esecuzione di un file .exe dalla directory C:/Program and Settings/Local User/desktop/ utilizzando la funzione winexec.

| Locazione | Istruzione | Operandi | Note |
|-----------|------------|----------|---|
| 0040FFA0 | mov | EDX, EDI | EDI: C:\Program and Settings \Local User\Desktop\Ransomware.exe |

PASSAGGIO DEGLI ARGOMENTI

Facendo riferimento alle istruzioni "call" riportate nelle tabelle 2 e 3:

Chiamata a DownloadToFile(): Prima di eseguire questa funzione, il registro EAX viene impostato al valore di EDI, che contiene l'URL www.mlawaredownload.com. Successivamente, EAX viene pushato nello stack come parametro per la funzione DownloadToFile().

Chiamata a WinExec(): Prima di eseguire questa funzione, il registro EDX viene impostato al valore di EDI, che contiene il percorso del file .exe da eseguire. Dopodiché, EDX viene pushato nello stack come parametro per la funzione WinExec()



GRAZE