S11/L5

- Nel codice fornito, il malware effettua un salto condizionale nel punto **0040BBA0 in tabella 2**. Questo salto condizionale avviene sulla base del risultato della comparazione tra i registri EAX e 5, eseguita dall'istruzione cmp EAX, 5 seguita dall'istruzione jnz loc_0040BBA0.

  Il comando **cmp** (compare) confronta il valore nel registro EAX con il valore 5, ma il risultato del confronto non modifica direttamente il flusso del programma. È l'istruzione successiva, **jnz** (jump if not zero), che determina il salto condizionale. Questo comando esegue il salto alla locazione 0040BBA0 solo se il risultato della comparazione non è zero, ovvero se EAX non è uguale a 5.

- **Controllo dei registri EAX ed EBX**
  Il malware inizia impostando il registro EAX a 5 e il registro EBX a 10. Successivamente, controlla se il valore di EAX è uguale a 5 utilizzando l'istruzione cmp EAX, 5. Se EAX non è uguale a 5, salta alla locazione 0040BBA0. Altrimenti, incrementa il valore di EBX di 1 e controlla se EBX è uguale a 11.
  Se il valore di EBX è uguale a 11, il malware salta a 0040FFA0.

  Download di file da un URL
  Alla locazione 0040BBA0, il malware esegue un'operazione di download di file da un URL specifico, che nel codice è rappresentato dalla stringa "www.malwaredownload.com"

- Nel codice assembly fornito, le istruzioni call vengono utilizzate per chiamare la funzione DownloadToFile().
  Nel codice fornito, la chiamata alla funzione DownloadToFile() sembra utilizzare la convenzione di passaggio degli argomenti tramite lo stack, dato che viene utilizzata l'istruzione push per caricare gli argomenti prima della chiamata della funzione.