Progetto S11L5

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.

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

2)

```
mov EAX, 5
mov EBX, 10
cmp EAX, 5
jnz loc 0040BBA0 ;     tabella 2
```

Il jnz (jump if not zero) non salta alla locazione di memoria specificata perchè la ZF non è settato a 1, ovvero il valore è a 0

ZF (Zero flag) = 1
cmp = 5 - 5 = 0

```
inc EBX
cmp EBX, 11
jz loc 0040FFA0 ; tabella 3
```

1) Il jz (jump if zero) salta alla locazione di memoria specificata perchè la ZF è settato a 1, ovvero il valore è a 0

ZF = 1
cmp = 11 - 11 = 0

Tabella 2

loc 0040BBA0:

```
mov EAX, EDI            EDI= www.malwaredownload.com
push EAX ;              URL
call DownloadToFile() ; pseudo funzione
```

Tabella 3

loc 0040FFA0:

```
mov EDX, EDI            EDI: C:\Program and Settings\Local User
                        \Desktop\Ransomware.exe
push EDX ;              .exe da eseguire
call WinExec() ;        pseudo funzione
```

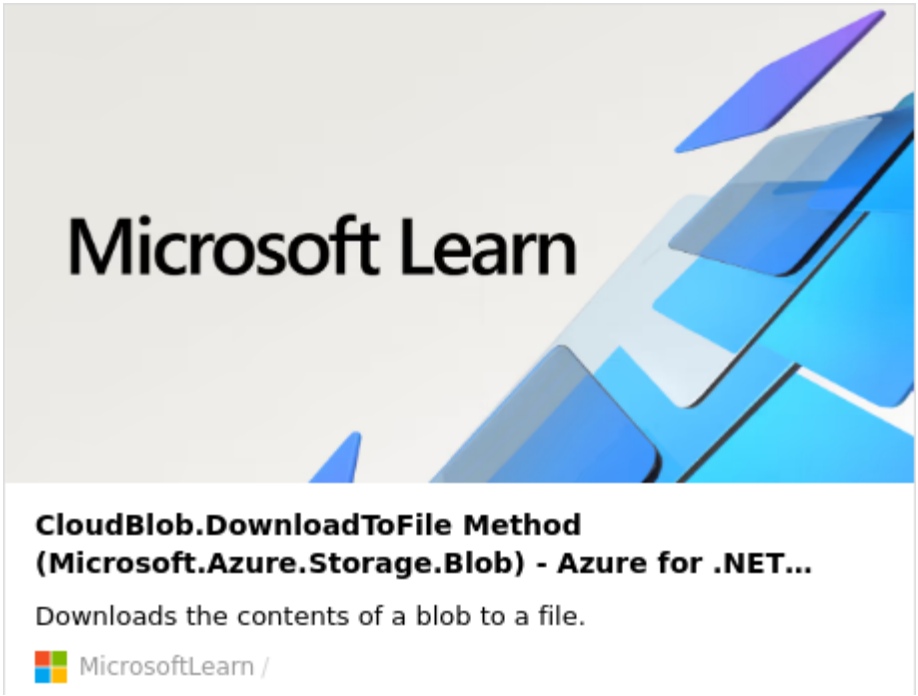
3-4) Un downloader è un programma che scarica da internet un malware oppure un componente di esso e lo esegue sul sistema target.

Possiamo identificare un download in quanto utilizzerà inizialmente l'API **DownloadToFile()** per scaricare bit da internet e salvarli all'interno di un file sul disco rigido del computer infetto.

Tra i parametri richiesti dalla funzione vi sono «szFileName» che sarà il nome del file salvato sul disco rigido a valle del download e «szURL» che invece è l'URL al quale il malware si collegherà per scaricare il contenuto malevolo. La funzione restituisce un valore «S_OK» se il download è andato a buon fine, diversamente restituirà un codice di errore.

WinExec() è il tipo di API che il downloader utilizza per avviare il malware scaricato da internet

DownloadToFile



WinExec