

Analisi avanzata Malware

Quesiti.

- 1) Spiega e motiva quale salto condizionale effettua il malware.
- 2) Diagramma di flusso identificando i salti indicando con la linea **verde** i salti effettuati e con la linea **rossa** i salti non effettuati.
- 3) Descrivi le diverse funzionalità implementate nel malware.
- 4) Dettagliare come sono passati gli argomenti della tabella 2 e 3 alle successive chiamate di funzione.

Quesito 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 |

Il salto condizionale che effettua il malware è il “00401068 JZ”.

EBX è 10 fino a prima dell’ incremento quando viene comparata diventa 11 quindi il flag sarà 1. JZ effettua il salto esclusivamente quando il flag è 1.

I quadrati in blu seguono il registro **EBX** (mov,inc,cmp,jz).

Quesito 2

-  Esegue il salto
-  Non esegue il salto
-  Continua la funzione

| 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 |

Come ho spiegato nel punto 1 la funzione salta direttamente a “loc 0040FFA0”.

Quesito 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 |

Le funzionalità implementate dal malware sono: Downloadtofile e winExec.

La prima per scaricare file dal sito www.malwaredownload.com.

La seconda per eseguire il file Ransomware.exe.

Quesito 4

- Esegue il salto
- Non esegue il salto
- Continua la funzione

| 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 |

Vedendo la figura prendiamo in considerazione solo i due Jump in basso, sinistra e destra.

PARTE SINISTRA: si inserisce **EDI** nel registro **EAX**, si pusha sulla stack il registro **EAX** e si chiama la funzione Downloadtofile(). **EDI** in questo caso è un URL nello specifico www.malwaredownload.com. (downloader)

PARTE DESTRA: si inserisce **EDI** nel registro **EDX**, si pusha EDX sullo stack e si chiama la funzione WinExec(). In questo caso **EDI** è un path che ci porta ad un file eseguibile in questo caso Ransomware.exe. Il malware probabilmente cripterà i nostri file.