PROVA PRATICA

MALWARE ANALYSIS

04-07-2023

```
00401040    mov     EAX, 5
00401044    mov     EBX, 10
00401048    cmp     EAX, 5
0040105B    jnz     loc 0040BBA0
0040105F    inc     EBX
00401064    cmp     EBX, 11
00401068    jz      loc 0040FFA0
```

SPIEGAZIONE SALTO

In questo caso il salto non avviene dato che nell'istruzione precedente viene eseguita una comparazione valida che conseguentemente imposta la "Zero Flag" , questo cambiamento fa si che il salto "jnz", che avviene solo se la flag rimane intoccata, non avvenga.

```
0040BBA0    mov     EAX, EDI
0040BBA4    push    EAX
0040BBA8    call    DownloadToFile()
```

SPIEGAZIONE BLOCCO ISTRUZIONI

Il malware in questo punto del codice inizialmente sposta il contenuto di EDI (link web malevolo) in EAX, poi pusha il registro nello stack per passarlo come argomento alla funzione che segue, l'URL viene passato come un puntatore ad una stringa nel parametro di funzione "szURL". Questo è un classico comportamento dei malware di tipo Downloader che si insinuano nel sistema operativo vittima per poi connettersi alla rete e far si che il vero malware venga scaricato da un server remoto gestito dall'attaccante, se avvenuto con successo, il malware potrebbe successivamente implementare funzioni atte ad avviare il nuovo file scaricato come CreateProcess, ShellExecute o in questo caso WinExec.

SPIEGAZIONE SALTO

Il malware effettua questo salto condizionale dato che il codice mnemonico "jz" sposta il flusso di esecuzione del programma nel caso in cui la "Zero Flag" è stata settata ad 1, in questo caso l'istruzione precedente esegue una comparazione che a livello macchina viene vista come una sottrazione che non modifica gli operandi ma solo le flag corrispondenti, appunto se il risultato dell'operazione è zero la flag citata prima viene impostata ad 1.

```
0040FFA0    mov     EDX, EDI
0040FFA4    push    EDX
0040FFA8    call    WinExec()
```

SPIEGAZIONE BLOCCO ISTRUZIONI

In questo blocco il malware effettua lo spostamento di EDI (path malware secondario) nel registro EDX, così facendo ha la possibilità di pushare questo valore nello stack passandolo come argomento per la funzione successiva andando a riempire il parametro "lpCmdLine" come puntatore di una stringa. La funzione chiamata alla fine ha il compito di eseguire il file indicato come se l'utente ci avesse cliccato sopra aprendo un nuovo processo quasi sicuramente malevolo, nella maggior parte dei casi il file che viene eseguito è stato scaricato dallo stesso malware con un blocco di codice simile a quello a sinistra.