S11L4

Consegna:

La figura nella riportata successivamente mostra un estratto del codice di un malware. Bisogna identificare:

1) Il tipo di Malware in base alle chiamate di funzione utilizzate.

2) Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa

3) Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

```
.text: 00401010    push eax
.text: 00401014    push ebx
.text: 00401018    push ecx
.text: 0040101C    push WH_Mouse          ; hook to Mouse
.text: 0040101F    call SetWindowsHook()
.text: 00401040    XOR ECX,ECX
.text: 00401044    mov ecx, [EDI]         EDI = «path to
                                          startup_folder_system»
.text: 00401048    mov edx, [ESI]         ESI = path_to_Malware
.text: 0040104C    push ecx               ; destination folder
.text: 0040104F    push edx               ; file to be copied
.text: 00401054    call CopyFile();
```

Risoluzione:

1) Sulla base delle funzioni chiamate dal malware, è possibile identificarlo come un keylogger; infatti, questo tipo di malware generalmente utilizza due tipi di funzione:

-**SetWindowsHook()** è una funzione che installa un Hook che permette di monitorare degli eventi legati ad una eventuale periferica (come mouse, tastiera, monitor, …) e ne salva i dati catturati su un file di log.

-**GetAsyncKey()** è una funzione che permettere di conoscere lo stato di ogni pulsante sulla tastiera di un dispositivo su cui è girato il malware, potendo quindi controllare gli input dell'utente.

2)In questo caso si può notare la chiamata di funzione **SetWindowsHook()** e più nello specifico ci si può rendere conto del fatto che l'Hook di questo malware vuole monitorare

gli input del mouse della vittima per via del parametro **WH_Mouse**. In più dopo è presente la funzione **CopyFile()** che serve per creare un duplicato dell'eseguibile nella cartella di startup del dispositivo, in questo modo ogni qualora il PC in questione viene avviato, verrà eseguito il malware in modo tale che l'attaccante possa sapere gli input del mouse della vittima

3) Il codice ottiene la persistenza copiando il suo eseguibile nella cartella **"startup_folder_system"**. Il codice presente nella tabella a partire dall'istruzione che si trova all'indirizzo di memoria 00401040, setta il registro ECX a 0, successivamente inserisce il path della cartella "startup_folder_system" e l'eseguibile del Malware nei registri ECX ed EDX. In seguito, chiama la funzione **CopyFile()** con le istruzioni push ECX e push EDX. La funzione CopyFile() quindi copierà il contenuto di EDX (ovvero l'eseguibile del malware) nella cartella di startup del sistema operativo.