Settimana 11 Lezione 4 Daniele D'Esposito

Traccia:

```
.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                  ; destinationfolder
.text: 0040104F   push   edx                  ; file to be copied
.text: 00401054   call    CopyFile();
```

La figura mostra un estratto del codice di un malware. Identificate:

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

il malware e' un **key logger** perche' utilizza la funzione **SetWindowsHook** della libreria **winuser.h** che controlla l'utilizzo del mouse

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

SetWindowsHook e' la prima chiamata di funzione e ha bisogno di 4 parametri e si occupa di monitorare il sistema per determinati tipi di eventi; il primo parametro e' **idhook** e decide il tipo di evento, in questo caso viene scelto di monitorare il mouse selezionando il valore 7 che corrisponde a **WH_Mouse.**
La seconda funzione e' **CopyFile** che copia un file esistente in un nuovo file; il primo parametro corrisponde al file da copiare e la seconda alla destinazione della copia

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

Per ottenere la persistenza il malware utilizza la tecnica dello start up folder, copiare il file all'interno della cartella start up in modo tale che parta all'avvio