**FUNZIONALITÀ DEI MALWARE**

**TRACCIA**

La figura nella slide successiva mostra un estratto del codice di un malware. Identificate:   
1) Il tipo di Malware in base alle chiamate di funzione utilizzate. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa. 2) 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();

**ESERCIZIO**

1) Il Malware chiama le seguenti funzioni:  
- **call SetWindowsHook()** (riquadro rosso): dapprima viene pushato nello stack l'input del mouse tramite **push WH\_Mouse** e successivamente viene chimata la funzione **call SetWindowsHook()** per impostare un hook al mouse, che potrebbe essere parte di un keylogger per monitorare le attività della vittima e salverà le informazioni su un file di log.  
- **call CopyFile()** (riquadro blu): è utilizzata per copiare un file da una posizione all'altra. In questo caso, il path del malware ed il path della Startup Folder (riquadro verde).   
Questo è utilizzato per copiare il malware stesso o altri file per la sua esecuzione nella Startup Folder.  
  
  
2) Il malware ottiene la persistenza proprio andandosi a copiare nella Startup Folder (riquadri blu e verde). In questo modo il malware riesce a copiare il suo eseguibile all’interno della SF che verrà eseguito automaticamente all’avvio del sistema.