# Funzionalità dei Malware

Tipo di malware in base alle funzioni interessate

Evidenziazione delle chiamate di funzione principali aggiungendo una descrizione

Metodo utilizzato dal malware per ottenere la persistenza sul sistema operativo

Orlando Tangari

```
.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 = «pat to
                                                        startup_folder_system»
.text: 00401048        mov edx, [ESI]                   ESI = pat_to_Malware
.text: 0040104C        push ecx                         ; destination folder
.text: 0040104F        push edx                         ; file to be copied
.text: 00401054        call CopyFile();
```

Il malware risulta essere un keylogger per via della modalità usata alla riga cinque, ovvero: *SetWindowsHook()*.

```
.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 = «pat to
                                                        startup_folder_system»
.text: 00401048        mov edx, [ESI]                   ESI = pat_to_Malware
.text: 0040104C        push ecx                         ; destination folder
.text: 0040104F        push edx                         ; file to be copied
.text: 00401054        call CopyFile();
```

La funzione *hook* è dedicata al monitoraggio degli eventi di una data periferica, in questo caso: il mouse.

La funzione copia un file esistente in uno nuovo.

Chiamate di funzione principali

```
.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 = «pat to
                                                        startup_folder_system»
.text: 00401048        mov edx, [ESI]                   ESI = pat_to_Malware
.text: 0040104C        push ecx                         ; destination folder
.text: 0040104F        push edx                         ; file to be copied
.text: 00401054        call CopyFile();
```

Inizializzazione del registro tramite XOR.

Il malware copia il suo eseguibile nella startup folder, controllata all'avvio del sistema operativo, per essere eseguito automaticamente.

Funzione che permette la copia del file.

Metodo utilizzato dal malware per ottenere la persistenza sul sistema operativo