

# MALWARE ANALYSIS

## ANALISI COMPORTAMENTALE DI CATEGORIE DI MALWARE NOTE

### 1. Identificazione del tipo di malware in base alle chiamate di funzione utilizzate

.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();	

Ipotizzo che sia un **keylogger** per l'istruzione push WM\_Mouse e delle chiamate di funzione immediata SetWindowsHook()

**SetWindowsHook()**: questa funzione installa un metodo hook dedicato al monitoraggio degli eventi di una data periferica.

In questo malware hook analizza il mouse

### 2. Funzioni 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 = «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();	

funzione chiamata per monitoraggio mouse

funzione chiamata per la copia di un file

**Le principali chiamate di funzione sono:**

**call SetWindowsHook():** questa funzione installa un metodo hook dedicato al monitoraggio degli eventi di una data periferica. Questo metodo verrà allertato ogni volta che l'utente farà un click con il mouse

**call CopyFile() :** funzione che si occupa di copiare un file esistente in un nuovo file.

### **3. 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();	

Il malware ottiene la persistenza attraverso la copia del suo eseguibile nella **Startup Folder** che contiene i processi che il sistema operativo inizializzerà al suo avvio.

### **4. Analisi delle singole istruzioni**

**Push EAX:** Inserisce in cima allo stack di memoria il registro EAX

**Push EBX:** Inserisce in cima allo stack di memoria il registro EBX

**Push ECX:** Inserisce in cima allo stack di memoria il registro EBX

**Push WH\_Mouse:** Inserisce in cima allo stack di memoria l'hook WH\_Mouse per il monitoraggio della periferica mouse

**Call SetWindowsHook():** Chiama la funzione SetWindowsHook, che monitora le periferiche indicate dall'istruzione precedente

**XOR ECX, ECX:** Azzera il contenuto del registro ECX tramite operatore logico XOR

**Mov ECX, [EDI]:** Copia il contenuto dell'indirizzo di memoria sorgente [EDI] nel registro ECX

**Mov EDX, [ESI]:** Copia il contenuto dell'indirizzo di memoria sorgente [ESI] nel registro EDX

**Push ECX:** Inserisce in cima allo stack di memoria il registro ECX

**Push EDX:** Inserisce in cima allo stack di memoria il registro EDX

**Call CopyFile():** Chiama la Funzione CopyFile()