```
.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();
```

Identificate:

- ***Il tipo di Malware in base alle chiamate di funzione utilizzate.***
- ***Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa.***
- ***Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo.***

Questo malware sembra essere un keylogger che cerca di ottenere l'accesso remoto al sistema e/o rubare informazioni sensibili, utilizzando hook di sistema per monitorare l'attività dell'utente e copiandosi in una posizione di avvio per garantire la **persistenza**.

- ***SetWindowsHook():***

E' un tipo di keylogger. Un keylogger è un particolare tipo di malware programmato per intercettare tutto ciò che l'utente della macchina infetta digita sulla tastiera.

Questa funzione non fa altro che installare un metodo (una funzione) chiamato «hook» dedicato al monitoraggio degli eventi di una data periferica, come ad esempio la tastiera o il mouse. Il metodo «hook» verrà allertato ogni qualvolta l'utente digiterà un tasto sulla tastiera e salverà le informazioni su un file di log.

- ***CopyFile():***

Una volta che il malware ha identificato il dispositivo esterno, copia se stesso (il suo file eseguibile) all'interno del dispositivo stesso utilizzando la chiamata alla funzione CopyFile() A questo punto, non dovrà fare altro che rinominare il file come «Autorun» per fare in modo che all'avvio della periferica, il malware sia eseguito automaticamente o mediante doppio click da parte dell'utente.

Iniezione di un hook per eventi del mouse: La chiamata a SetWindowsHook con il parametro WH_Mouse suggerisce che il malware voglia intercettare gli eventi del mouse nel sistema operativo. Questo potrebbe consentire al malware di monitorare e interagire con le azioni dell'utente legate al mouse.

Copia del file in una cartella di avvio del sistema: Dopo aver impostato l'hook per gli eventi del mouse, il malware sembra copiare se stesso in una cartella di avvio del sistema. Questo viene fatto utilizzando la funzione CopyFile, che copia un file da una posizione all'altra nel filesystem. Presumibilmente, il malware si copia nella cartella di avvio del sistema, il che significa che verrà eseguito ogni volta che il sistema viene avviato, garantendo così la sua persistenza nel sistema.

- ***BONUS: Analisi più dettagliata delle singole istruzioni a un livello più basso:***

push eax: Questa istruzione mette il valore attuale del registro eax nello stack della memoria. Lo stack è una struttura dati utilizzata per l'organizzazione della memoria temporanea durante l'esecuzione di un programma.

push ebx: Questa istruzione mette il valore attuale del registro ebx nello stack della memoria.

push ecx: Questa istruzione mette il valore attuale del registro ecx nello stack della memoria.

push WH_Mouse: Questa istruzione mette il valore WH_Mouse nello stack della memoria. WH_Mouse è un parametro che verrà utilizzato successivamente.

call SetWindowsHook(): Questa istruzione chiama una funzione chiamata SetWindowsHook(). Il valore di WH_Mouse passato come parametro è utilizzato per specificare il tipo di hook da impostare.

XOR ECX, ECX: Questa istruzione esegue un'operazione di XOR tra il registro ECX e se stesso, impostando il registro ECX a 0.

mov ecx, [EDI]: Questa istruzione sposta il valore memorizzato all'indirizzo di memoria contenuto nel registro EDI nel registro ECX. Il valore di EDI è il percorso alla cartella di avvio di sistema.

mov edx, [*ESI]:* Questa istruzione sposta il valore memorizzato all'indirizzo di memoria contenuto nel registro ESI nel registro EDX. Il valore di ESI è il percorso al malware.

push ecx: Questa istruzione mette il valore del registro ECX (che contiene il percorso alla cartella di avvio di sistema) nello stack della memoria.

push edx: Questa istruzione mette il valore del registro EDX (che contiene il percorso al malware) nello stack della memoria.

call CopyFile(): Questa istruzione chiama una funzione chiamata CopyFile() che copia un file da una posizione all'altra, utilizzando i valori nello stack come parametri (il percorso di destinazione e il percorso del file da copiare).