Immagine che contiene testo, Carattere, schermata, bianco

Descrizione generata automaticamente  
vengono dichiarate le variabili e chiamate le funzioni WH\_Mouse che registra gli input del mouse e SetWindowsHook che registra gli input da tastiera.

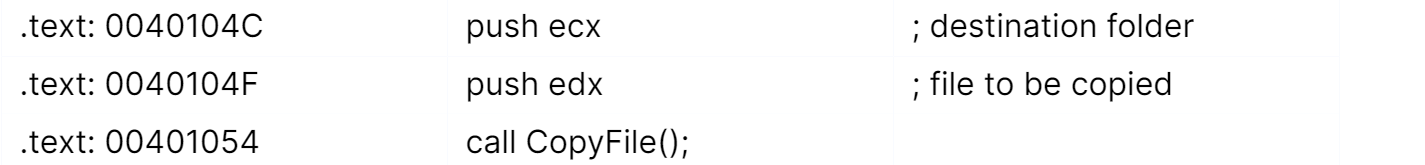
Immagine che contiene testo, Carattere, ricevuta, bianco

Descrizione generata automaticamente

Viene azzerato il valore di ECX

Viene poi spostato [EDI] in ECX e [ESI] in EDX

Qui viene creata la persistenza all’avvio



E qui viene richiamata la funzione principale

Il malware analizzato è un Keylogger