S11L4

1)Il codice suggerisce la presenza di un tipo di malware noto come keylogger, in quanto vediamo l'utilizzo della funzione "SetWindowsHook" per installare un "hook" destinato al monitoraggio di un dispositivo. Tuttavia, ciò che risalta è che, a differenza del codice della lezione teorica, l'ultimo parametro passato nello stack è "WH_MOUSE". Questo suggerisce che il malware potrebbe non registrare la digitazione della tastiera dell'utente, bensì l'attività dei tasti del mouse.

2) Il Malware ottiene la persistenza copiando il suo eseguibile nella cartella di «startup del sistema operativo». Il codice presente nella tabella a partire dall'istruzione 00401040, dapprima setta a zero il registro ECX, successivamente inserisce rispettivamente il path della cartella «startup_folder_system» e l'eseguibile del Malware nei registri ECX ed EDX. In seguito, passa entrambi i registri alla funzione CopyFile() con le due istruzioni push ECX e push EDX. La funzione CopyFile() quindi copierà il contenuto di EDX (ovvero l'eseguibile del malware) nella cartella di startup del sistema operativo.