# Звіт про розроблене шкідливе програмне забезпечення KeyLogger

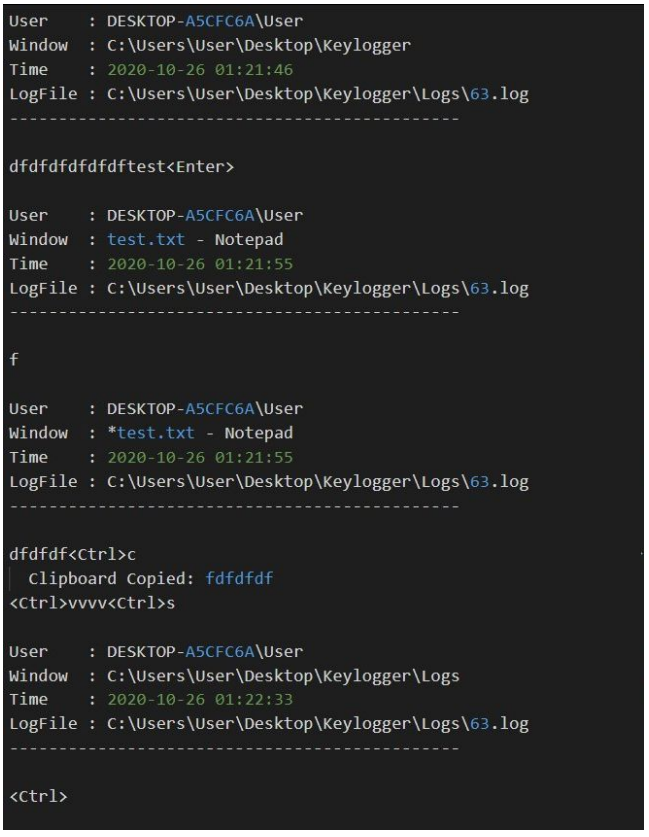
Виконали студенти КН-3
Бородайкевич Євген та Волошко Максим

## Активація

Шкідливе програмне забезпечення є виконуваною програмою, яка запускає фоновий процес. Є можливість вдосконалення, реалізувавши автозапуск цього вірусу при скачуванні на комп’ютер.

## Поведінка

Суть цього вірусу полягає у відслідковуванні натискання клавіш користувачем, вікон та програм, у яких були натискання, та час. Програма виводить у файл інформацію так, як показано на малюнку. Також, при копіюванні якогось тексту, у файлі це буде відмічено “Clipboard Copied”. Застосунок виводить лише ті, клавіші, які несуть важливу інформацію, але список таких клавіш може бути легко розширеним.




## Наслідки

Наслідки цього шкідливого програмного забезпечення можуть бути дуже серйозними. Внаслідок відслідковування натискання клавіш, зловмисник може отримати інформацію про вашу персональну

інформацію, таку як паролі, логіни тощо. Завдяки визначенню вікна, у якому були здійснені натискання, а також часу, злодій матиме змогу ідентифікувати, які застосунки найбільш використовувані та наскільки важливою буде інформація у них.

## Убезпечення

Найбільш дієвим способом убезпечення від цього шкідливого програмного забезпечення буде обережне користування інтернетом. Оскільки цей вірус є виконуваним файлом, до вашого комп’ютеру він потрапляє лише, коли ви завантажили його (у явному або прихованому вигляду). Також слід мати на своєму комп’ютері антивірус, який би перевіряв скачані файли з інтернету та регулярно робив би сканування файлів на виявлення загроз або несанкціонованого використання ресурсів комп’ютера фоновим процесом.

## Знешкодження

Для знешкодження спочатку потрібно ідентифікувати сам процес, який використовує ресурси комп’ютера. Потім знайти розташування файлу, який запускає цей процес, видалити файл та завершити процес. Після цього краще за все змінити всі паролі, які були використані останнім часом та які є важливими для вас, а також переглянути свою активність у найбільш використовуваних додатках, щоб пересвідчитися, які дії зловмисник виконував з вашого облікового запису.