##### ***Команда: „Продам гараж за флаги“***

##### ***Задание: Расследование инцидента.1***

##### 1. Злоумышленник попал на машину при помощи загрузки вируса под видом популярной компьютерной игры “Minecraft”, загруженной владельцем машины. Во время исполнения файла “minecraft.jar” выполнился вредоносный код, проанализировав который, мы поняли, что злоумышленник пробросил reverse shell на свою машину, которая находилась в одной сети вместе с пострадавшим.

##### 2.

##### 3. Для получения пароля злоумышленник воспользовался кейлоггером logkeys, который пишет лог в var/log/logkeys.log. Посмотрев файл logkeys.log, увидели комбинацию цифр и букв, похожую на пароль и повторили все действия. Попробовав этот пароль мы убедились, что он подходит.

##### 4. Посмотрев bash\_history пользователя root, предположили, что логи logkeys сохраняются в файл logkeys.log и попробовали найти такой файл командой “find . -name logkeys.log”, где . - директория раздела смонтированного образа. Команда выдала путь до файла logkeys.log - var/log/logkeys.log.

##### 5. Открыв файл passwords.kdbx мы увидели пароль, названный windows\_rdp. Прогуглив мы поняли, что это пароль от приложения для удалённого доступа к рабочему столу Windows.

