13 июля 2022 г.

Репортеры без границ запускают “Лабораторию цифровой безопасности RSF” (RSF Digital Security Lab)

18 июля 2022 года, ровно через год после разоблачения массового использования шпионского ПО Pegasus, направленного, в частности, против журналистов, организация "Репортеры без границ" (RSF) представит свою Digital Security Lab: лабораторию цифровой криминалистики, созданную для противодействия угрозам онлайн-слежки.

Целью базирующейся в Берлине Digital Security Lab является проведение углубленного анализа цифровых устройств журналистов, подозревающих, что за ними ведется слежка. Это может быть и заражение этих устройств, и взлом их аккаунтов в социальных сетях: журналисты сталкиваются с множеством угроз, борьба со всеми из которых требует надежных и тщательных решений.

> "Использование цифровых атак одновременно и отвратительно, и коварно, - заявил генеральный секретарь RSF Кристоф Делуар, - журналисты становятся излюбленной целью этих невидимых глазом атак: RSF не оставит их один на один с цифровыми наемниками и хищниками свободы прессы".
>
> “Скандал с Pegasus продемонстрировал, что угрозы для журналистики, к сожалению, вполне реальны, - добавил директор организации "Репортеры без границ" в Германии Кристиан Мир, - создавая Лабораторию цифровой безопасности, RSF отвечает на многочисленные просьбы о помощи, поступающих к нам от журналистов по всему миру, которые опасаются, что за ними шпионят или, что они стали объектом других форм кибер-атак".

За помощью в Digital Security Lab могут обратиться любые журналисты, которые подозревают, что за их устройствами шпионят в связи с их журналистской работой. Существует несколько признаков, которые должны предупреждать об опасности. Например, сложные попытки фишинга (получения подозрительных сообщений, содержащих вредоносные ссылки), необъяснимые утечки информации или

репрессивные меры авторитарных государств. Всё это должно побудить журналистов задуматься о защите своих устройств и их проверке.

Созданная Digital Security Lab состоит из команды трех экспертов, которым поручено обследовать устройства журналистов на тему наличия в них следов шпионских программ. Хакеры часто используют методы фишинга, чтобы обманом заставить журналистов перейти по вредоносной ссылке или открыть зараженное вложение. Поэтому поиск улик и цифровых следов начинается с анализа подозрительных сообщений на предмет наличия в них шпионских программ. После этого команда изучает уже установленные программы и проверяет иные следы данных, которые могут дать подсказки о ранее запускавшихся программах или производившихся с устройствами манипуляциях.

Расследование международной сети СМИ выявило 18 июля 2021 года, что телефоны десятков тысяч политиков, правозащитников и журналистов потенциально были взломаны с помощью шпионской программы Pegasus, разработанной израильской компанией NSO Group. В списке телефонных номеров зараженных устройств фигурировали номера более 200 журналистов. Чтобы добиться расследования этого дела, 20 июля 2021 года RSF совместно с двумя франко-марокканскими журналистами подали иск к неустановленному лицу в прокуратуру города Парижа.