Прикладное применение реверс-инжиниринга в расследованиях и атрибуции

В последние годы мы наблюдаем рост интереса к сфере ИБ. В России и за рубежом увеличивается объем инвестиций и расходов в ИБ, увеличивается количество материала в СМИ и медиа, постоянно открываются секьюрити стартапы. Очень популярны у молодых специалистов направления в услугах аудита и «пентеста» (тестирование на проникновение). Классический реверс-инжиниринг считается сложным и спрос на специалистов в этой области явно превышает предложение. Несмотря на это, будущие специалисты предпочитают не заниматься такой сложной темой, считая ее излишне специализированной и сложной. Наталья Касперская предложила даже искусственно затруднить выезд за рубеж таким специалистам (<https://www.gazeta.ru/army/2017/08/26/10859996.shtml>).

Самые известные прикладные назначения реверс-инжинирнга – «взлом» программ, плагиат, патчинг, поиск уязвимостей. Не все перечисленное является законным, и это еще одна причина, почему специалисты по реверс-инжинирингу не могут быстро и легко найти работу, т.к. сфера применения применения данных знаний и навыков ограничена. В данной презентации я хочу рассказать, как реверс-инжиниринг помогает в расследованиях и решении задач threat intelligence (киберразведке) в Group-IB на реальных рабочих кейсах. Наша работа не только законна, но и помогает сделать мир лучше.

Презентация условно разбита на 3 части:

1. Преступная группа Silence
   1. Обвинения ЦБ Украины в адрес спец служб РФ об атаке на банковский сектор и наше опровержение данных обвинений с помощью реверс-инжиниринга. 2 слайда
   2. Определение рода деятельности и состава группы, а также языковая принадлежность преступников. 2-3 слайда
2. Cobalt
   1. Выявление самой первой атаки, совершенной хакерами, которых называют самой большой угрозой банковскому сектору по всему миру. 2 слайда
3. Qryptor
   1. Определение автора, его имени, места проживания и страницы в соц сетях по следам, оставленным во вредоносной программе. 2 слайда

**Суммарное время выступления** – 35-45 минут. 30 минут на презентацию + 10 минут на вопросы.