Международное объединение детективов

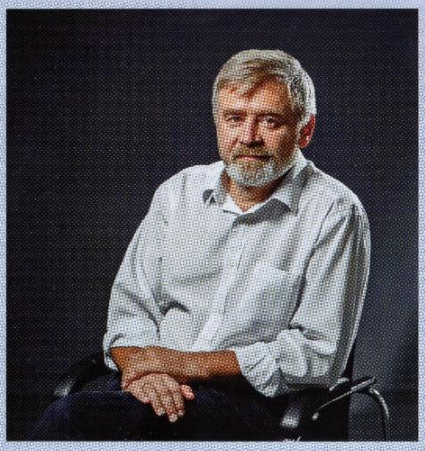
IAPD – International Association of Private Detectives

Сборник материалов 2020

Больше, чем хакер. Интернет-разведка в цифровом мире

Андрей **Масалович**

БОЛЬШЕ, ЧЕМ ХАКЕР. ИНТЕРНЕТ-РАЗВЕДКА В ЦИФРОВОМ МИРЕ



Масалович Андрей Игоревич

Партнёр МОД.
Кандидат физико-математических наук, руководитель ряда успешных проектов по аналитическому оснащению банков, ФПГ, крупных торговых сетей, государственных организаций. В прошлом – подполковник ФАПСИ, основатель интернет-разведки.

Специалист по связям с реальностью

Шесть утра. Начинается новый день, полный чудес. Первый звонок, как водится, из Юго-Восточной Азии (ну конечно, у них там время подходит к обеду). Клиент спрашивает, можно ли узнать адекватные цены на конкретные модели рабочих станций для forensics (компьютерной криминалистики). Проблема: такие компьютеры используют в основном силовые структуры разных стран, контракты секретны, поставщики этим пользуются – и новым покупателям беззастенчиво задирают цены. «Минутку, повиси на трубке. Вот, спецслужбы соседней страны только что закупили два компьютера модели Ка-301 по 11 тысяч долларов за штуку». Итак, первое чудо явлено – заказчик понимает, что ему только что (и почти даром, по его меркам) раскрыли содержание реальных секретных контрактов, о которых его коллеги могут только мечтать. В чем секрет? Никакого чуда – большинство контрактов в Азии (даже секретных) включают поставку товаров, которые проходят через порт Сингапура – и отпечатываются в специализированной базе данных, вместе с детальной спецификацией и точной ценой каждой компоненты. Надо только быть зарегистрированным в этой базе, не бояться чуждого интерфейса (к слову, на китайском), а также иметь специализированных роботов, который автоматизируют ваши запросы. Не пугает? – тогда деловой пульс Азии уже сегодня застучит в вашем сердце.

Второй звонок – уведомление поисковой системы Avalanche: в потоке данных, касающихся

заданного объекта интереса (к слову – радикальной исламистской группировки в социальных сетях) появилась оперативно-значимая информация – номер банковского счета, на который экстремисты собирают пожертвования. Упс, этот номер счета уже проходил по нашим базам – пару лет назад его использовала вполне респектабельная исламская организация, распространяющая по миру Коран и труды Пророка. Когда чем-то долго занимаешься, тебе начинает везти – поднимаем архивы этой организации, и (о, второе чудо), среди участников этой организации находим молодого волонтера, который гордится своей миссией, и – не шучу – фотографирует посылки с религиозной литературой. Причем на фото видны наклейки на посылках с обратным адресом и телефоном руководителя организации-отправителя. Итак, в наших руках координаты владельца счета, который сегодня финансирует экстремистов. Заказчик будет доволен :-).

Бог любит троицу – и подтягивается третье чудо: звонок из Давоса. Руководитель крупной компании, участник Всемирного экономического форума (напомним, 20 тысяч бизнесменов, 20 президентов, 25 тысяч долларов за участие) делится проблемой. Его на завтраке подловили представители некоей неопознанной фирмы с революционной технологией нефтепереработки и предложили посвятить им обеденное время (в дни Форума в Давосе – бесценное) для обсуждения деталей супер-прибыльного сотрудничества. Надо сделать экспресс-проверку потенциального партнера. Увы, исходных данных недостаточно не только для проверки, но и для элементарной идентификации компании. Фактически, в руках только один слайд, присланный по WhatsApp – там фигурирует название компании (массовое и безликое имя), наименование технологии (та же история) и краткая формулировка революционной сути новаторской идеи (винегрет из научных и технических терминов). К счастью, на слайде также есть изображение, в котором можно угадать часть корпоративного логотипа. Поиск по изображениям в Яндексе оказывается удачным – и у нас в руках и логотип компании и ее полное точное название. Теперь мы видим, что зарегистрирована она в Британской юрисдикции, и имеет филиалы в Литве и Казахстане. Жизнь длинная, мир маленький, и для каждой страны уже сформировался список удобных бесплатных ресурсов для экспресс-проверок: так, по Великобритании легко «пробивать» фирмы по базе DueDil, по Прибалтике – по базе LurSoft, по Казахстану – по базе Бизнес-Навигатор. Итог: компания существует, даже успела освоить 2 млн фунтов инвестиций, однако в 2015 году деньги закончились, и далее идут нулевые балансы. А в карточке филиала в Литве красуется «Находится в стадии ликвидации» (кстати, по-литовски это произносится как «Ликвидец»). Проверяем учредителей, руководителей и контакты на сайте. Никакого криминала – это действительно создатели некоторой самобытной технологии, но: она уже не взлетела, и сейчас изобретатели просто ищут новых инвесторов для второй попытки. И тратить на них время не надо.

Итак, оперативно решены три практических задачи, суммарное потраченное время – менее часа.

Все приведенные примеры реальны, это ежедневная практика «охотника за информацией» - специалиста по OSINT (Open Source Intelligence – разведка по открытым источникам). Рожденная более полувека назад в интересах спецслужб США, разведка по открытым источника переживает сегодня второе рождение. Потоки данных, сопровождающие каждый наш шаг в интегрированном цифровом мере, аккумулируются в огромных распределенных базах данных (Big Data), формируя наш «цифровой след». Сегодня цифровой след человека или компании более реален, чем его владелец (да-да, например, решение о выдаче кредита будет приниматься исходя не из вашего реального положения дел, а из образа, который сформировался в базах Всемирной Паутины).

Распределенные базы данных, глобальные коммуникации, вездесущие шпионы-гаджеты, «Интернет вещей» - все эти компоненты новой цифровой реальности вызвали к жизни новый арсенал приемов и методов быстрого сбора и экспресс-обработки необходимой информации различной природы, а также методик «обогащения данных». Как следствие, один хорошо обученный аналитик способен существенно экономить время (и бюджеты) на решении всего спектра задач экономической безопасности современных организаций и банков. Кроме того, сам факт накопления значимых данных рождает новое знание – формируется схема связей и совместных активностей объектов интереса, позволяя выявлять скрытую связанность, цепочки владения, конечных бенефициариев, организаторов и заказчиков

резонансных событий и т.д.

Возникли даже новые специальности и учебные дисциплины, например, «Аналитик конкурентной разведки». К счастью, большая часть арсенала специалистов такого профиля находится, что называется, «на кончиках пальцев» - не требуются ни сложные программы, ни дорогостоящие базы данных, только знание новых приемов, гибкость мышления и желание учиться. Очень советую посмотреть в эту сторону.

А у меня на столе стоит кружка для кофе. На кружке надпись: «Я не шпион, я могу больше». Это слоган сообщества профессионалов конкурентной разведки – SCIP (Society of Competitive Intelligence Professionals). Очень мотивирует ;-).

ПОИСК СКРЫТЫХ АКТИВОВ, ПРЕДМЕТА РАЗБИРАТЕЛЬСТВ В ВЫСОКОМ ЛОНДОНСКОМ СУДЕ

Алекс Лурье (Лондон)

Вице-президент МОД,
представитель Ассоциации по Великобритании.