Владимир Безмалый

Цифровая гигиена

Том 3

Владимир Безмалый

Цифровая гигиена. Том 3

«Издательские решения»

Безмалый В.

Цифровая гигиена. Том 3 / В. Безмалый — «Издательские решения»,

ISBN 978-5-44-939107-0

Вы держите в руках третий том сказок и рассказов в области информационной безопасности. Надеюсь это поможет вам стать немного защищеннее.

ISBN 978-5-44-939107-0

Содержание

Цифровая гигиена
Том 3

Владимир Безмалый

ISBN 978-5-4493-9107-0 (т. 3)
ISBN 978-5-4493-9108-7
Создано в интеллектуальной издательской системе Ridero

Сказки о безопасности: Слабое звено

Солнечное утро манило гулять, а не идти на работу. Так и хотелось просто пройтись по парку, не думая ни о чем, просто шуршать листьями под ногами, стучать орехами, маня местных белок, выйти к пруду, расположенному в центре парка, покормить лебедей, которые еще не улетели на юг… Много чего хотелось. Главное, чего не хотелось – это идти на работу. Но ведь сегодня пятница, а значит впереди выходные. Так что на работу идти нужно!

– Софи, что у нас интересного с утра, кроме изумительного кофе с миндальными пирожными?

– Ой, шеф! Тут такое… Даже не знаю, как сказать. Я понимаю, что люди бывают глупые и беспечные. Но я даже представить не могла, что они могут работать в управлении ИТ нашего департамента безопасности. Ну вроде бы туда дураков не принимают. Как выяснилось, я ошибалась!

– Так, Софи, приглашай ко мне Марка, Риту, Курта и сама заходи. Будем слушать твой рассказ.

Прошло минут пятнадцать.

– Шеф, вот что произошло. Злоумышленник взломал защиту сети департамента юстиции и украл более 200 Гб данных, в том числе имена, фамилии, номера телефонов, адреса электронной почты 20 тыс. сотрудников департамента полиции и 10 тыс. сотрудников департамента внутренней безопасности.

– Ого!

– Мало того. Данные были им опубликованы в открытом доступе на веб-сайте.

– И как это произошло?

– Злоумышленнику удалось взломать аккаунт сотрудника департамента полиции, после чего он связался с оператором департамента внутренней безопасности и, выдавая себя за легитимного пользователя, получил доступ к инфраструктуре департамента полиции.

– Погодите, но как он получил доступ?

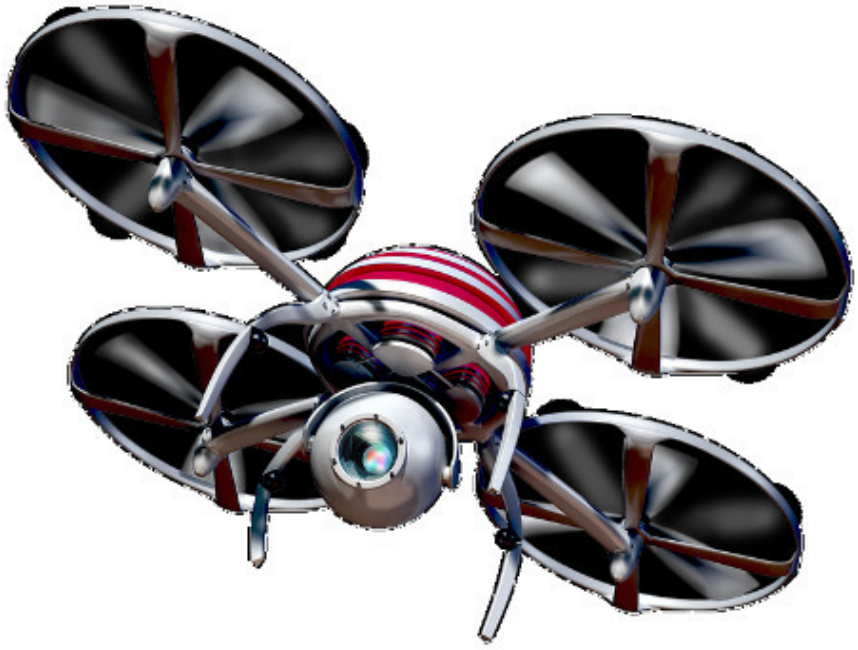
– А вот это самое интересное. Тут нам помогло то, что все внешние телефонные звонки записываются. Злоумышленник сказал, что не так давно устроился на работу. Оператор задал вопрос, а есть ли у него код доступа к данным. Злоумышленник ответил, что нет, тогда оператор посоветовал ему воспользоваться их кодом!

– Интересно, чем думал оператор?

– Ну не знаю, чем он думал, но теперь у него есть время подумать. Его явно уволят с работы. По крайней мере я посоветую сделать именно так.

> *Как ни странно, но именно такая история с утечкой данных министерства юстиции США произошла в феврале 2016 г. Только код доступа передал оператор ФБР. И снова мы сталкиваемся с тем, что самое слабое звено – человек, а не техника.*

Сказки о безопасности: Перехват дрона



Утро выдалось серым и туманным. После вчерашнего легкого мороза термометр показывал плюс два. Сыро, холодно, противно. Но на работу идти нужно. Гулять в такую погоду по парку удовольствие небольшое. Поэтому Иоганн решил вызвать дежурную машину.

Но только он собрался это сделать, как раздался резкий телефонный звонок.

– Иоганн, я выслал за вами машину. И за вашими ведущими специалистами тоже.

– Что случилось?

– Не по телефону. Приезжайте!

Голос начальника дворцовой охраны, господина Кранца, звенел от возбуждения.

Ну вот и все. Утро началось!

Прошло 20 минут.

– Что случилось? Кого вы вызвали?

– Как обычно. Вас, Риту, Мари и Курта. Естественно, операция, как и все что относится к безопасности императора, совершенно секретно.

– Как обычно. Мы были, но нас не было.

– Совершенно верно. Прошу за мной. Расскажу в кабинете. Да, коллеги, прошу сдать ваши смартфоны дежурному, он положит их в сейф. Никаких записей. Все записи, сделанные в ходе расследования, сдать мне лично под роспись.

– Понятно. А все же, что случилось?

– Неделю назад над дворцовым комплексом мы засекли квадрокоптер. Охрана отреагировала мгновенно, и он был сбит. Квадрокоптер стандартный, гражданского образца. Мало ли. Заблудился. Но два дня назад атака повторилась. И снова объект был сбит. Нас интересует, кто за этим стоит. Идеально не только перехватить следующий объект, а и вычислить оператора, а лучше бы того, кто за ним стоит.

– Н-да… Веселая задача. Но как?

– Шеф, я тут читала, наши приборостроители презентовали на последней выставке вооружений комплекс, способный перехватывать управление беспилотниками и определять местонахождение его оператора.

– Мари, я понимаю, что знания твои разносторонни, но что тебя занесло на выставку вооружений?

– Да брат пригласил. Он же помешан на авиации, вы ж помните.

– Господин Кранц, нам срочно нужен такой комплекс. И инженеры по его настройке и обслуживанию. А лучше полностью подготовленный расчет обслуживания такого комплекса.

– Хорошо. Я вызову их.

– Им нужно подготовить комнату во дворце. И нам тоже. Кроме того, здесь рядом должна дежурить группа захвата. Круглосуточно!

– Безусловно!

– Мари, а что вы можете рассказать об этом комплексе?

– Система предназначена не только для борьбы с беспилотными летательными аппаратами – с ее помощью можно подавлять вещательные станции, командные пункты связи, сигналы сотовых сетей, сети Wi-Fi, WiMax и DECT. От обнаружения беспилотника до подавления сигнала управления уходит порядка 25 с, а если частоты известны заранее, то порядка 700 мкс.

– Допустим, мы подавим управление, но как вычислить оператора?

– Шеф, вы меня поражаете. Дроны автоматически возвращаются в точку запуска при глушении сигнала управления. Но мы также можем посадить его в любом месте.

– Каким образом?

– Система создает ложное навигационное поле, меняя динамические координаты, в результате чего беспилотник уводится в сторону и в конечном счете приземлится там, где необходимо нам, а не оператору.

– Спасибо, Мари! Думаю, нам всем пора снова организовывать наши внутренние семинары по пятницам. Чтобы все могли делиться знаниями. Увы, информации столько, что физически не успеваешь прочесть. Согласны, коллеги?

– Безусловно!

Оператора дрона задержали через несколько дней. Он признался, что наблюдение проводилось по заказу террористической организации. Дальше уже следствие проводилось силами департамента внутренней безопасности.

Такое решение не фантастика и уже создано в России для нужд Вооруженных Сил

Сказки о безопасности: Атака детей

– Шеф! У нас проблема! Вернее, не у нас, но пришли к нам.

– Софи, будьте добры, подробнее и без паники. Давайте с начала.

– К нам обратился директор одной известной компании. Он пожаловался на утечку данных. Его специалисты обнаружить утечку не смогли.

– И что тут трагического?

– Да только пришла на работу, даже не успела пальто снять, а тут звонок… Крик, шум! Короче, как обычно. Вот я и разволновалась, извините, пожалуйста.

– Все нормально! Постарайтесь сохранять спокойствие. Для дела полезнее.

– Хорошо! Я постараюсь.

– Попросите их перезвонить мне.

Прошло полчаса.

– Иоганн, если вы не против, мы с моим руководителем службы безопасности приедем к вам в гости?

– Я не против, но, наверное, куда полезнее, если мы приедем к вам сами. Как думаете?

– Приезжайте, мы вас ждем.

– Карл, Рита, на выезд. Нас ждут. Думаю, в ближайшую неделю вы будете работать в этой компании.

Прошла неделя.

– Шеф, все куда интереснее. Данные были похищены с помощью учетных записей директора компании и их коммерческого директора.

– Ого! Это интересно, но как?

– Оказывается, все просто. Атака была осуществлена с помощью их любимых детей.

– Погодите. С этого момента подробнее.

– Учетную запись директора исследовала Рита, а я занимался коммерческим директором.

– Вы выяснили, что у них общего?

– Да. У обоих дети 12—13 лет. Сыновья. Оба очень любят играть на ПК. И обоим это запрещают родители.

– То есть?

– Разрешают играть лишь с 18 до 20 в присутствии родителей.

– У них уже были проблемы?

– Да. Оба запустили учебу, чересчур увлекались играми.

– Как это произошло?

– Проблема оказалась простой как дрова. Для ребенка не создавалась отдельная учетная запись. Он играл под учетной записью родителя. Соответственно, ему кто-то (сейчас разбираются кто), дал флэшку с кодами для игр. Он запустил программу с флэшки и… все! Троян на ноутбуке директора.

– А что с коммерческим? Так же?

– Там похоже. Только там заразили смартфон. Загрузили по совету друга игру, а в игре троян. Учетной записи для ребенка тоже нет.

– Понятно. Таким образом, оба нарушили одно и то же правило. Для детей нужно создавать отдельные ограниченные учетные записи. А на смартфоне, кроме того, нужно запретить загрузку программ из посторонних источников! Это сделано не было. Вот и поплатились.

А вы разрешаете детям играть на вашем компьютере под своей учетной записью? Она имеет административные права?

Сказки о безопасности: Игроки за рулем

Вчера лежал снег, а сегодня на улице снова грязь, ветер, дождь. Осень и зима никак не могли договориться. Мокрые ветки царапали стекла и снова шел дождь. Выходить на улицу в такую погоду никак не хотелось. Но служба есть служба, и идти все равно нужно. Тем более на этой неделе предстоял визит в канцелярию императора. И хотя совещание вроде бы никак не касалось департамента интеллектуальных преступлений, все же что-то не давало покоя.

Выглянув в окно, Иоганн понял, что идти пешком ну никак не хочется и вызвал дежурную машину.

– Шеф, у вас через два дня совещание в канцелярии императора. Вы не забыли?

– Помню. Софи, напомните мне тему совещания.

– Оно будет посвящено дорожному движению в столице. Резко выросло количество аварий на дорогах. Дорожная полиция пока не может понять причины. Водители вдруг стали совершенно не внимательны.

– Стоп. А позовите ко мне нашего аналитика. Роберт на работе?

– Да, безусловно. Сейчас приглашу.

– И сами заходите. Как мне помнится, вы были одним из лучших аналитиков во время учебы в Академии.

– Спасибо!

– Это ко не мне. Это ректору Академии. Он вас так охарактеризовал.

– Роберт, Софи! Вам предстоит помочь мне понять, что же случилось с водителями? Что у нас такого произошло за последние три месяца, что они стали невнимательны?

– За последние три месяца? Думаю, что невнимательными стали не только водители, а и пешеходы. Вспомните появление массового сумасшествия – игры «Поймай дракона».

– Ах да, толпы бродящих зомби по улицам со смартфонами в руках, пытающиеся поймать виртуальных дракончиков… Ажиотаж прошел довольно быстро, и данная игра уже не фигу-

рирует на первых полосах в СМИ. Вместе с тем она показала, как легко и сильно можно влиять на поведение и привычки людей.

– Да. Эта игра показала, насколько быстро у людей отключается мозг в погоне за целью. Даже если цель виртуальна.

– А никто не пытался оценить ущерб от этой игры?

– Ну почему же. Наши преподаватели провели весьма любопытный анализ по столице. Ущерб составил порядка нескольких миллионов империалов.

– А вы могли бы найти мне результаты этого анализа?

– Легко. Ведь там одним из ведущих аналитиков была Софи. Да-да, шеф, вы недооцениваете вашего прекрасного секретаря. Эта милая девушка хоть сегодня могла бы стать руководителем нашего аналитического бюро, которое давно пора создать.

– Спасибо за подсказку. Софи! Вам поручение. Поищите мне на выпускном курсе студентку, которая могла бы заменить вас на должности секретаря и готовьтесь к новой работе. Думаю, указ императора о создании аналитического отдела не заставит себя долго ждать. Роберт! Жду отчет.

Через два часа отчет Академии был на столе Иоганна. Там были приведены конкретные цифры, касающиеся аварий, которые произошли как по вине водителей, игравших за рулем, так и по вине пешеходов-игроков. Когда эти цифры сравнили с общим числом аварий, оказалось, что более 25% всех аварий можно объяснить именно игрой.

Выступление Иоганна на совещании поразило присутствующих. Никто и подумать не мог, что даже такая обыденная тема, как количество аварий в столице, может быть настолько связана с информационными технологиями.

По окончании совещания император издал два указа, одним из которых создавался аналитический отдел в департаменте Иоганна, а вторым – вносились изменения в правила дорожного движения. Отныне под угрозой огромного штрафа запрещалось использование смартфонов за рулем.

> *Исследователи Университета Пердью попытались оценить ущерб, нанесённый игрой Pokemon GO. Согласно их исследованию, за первые 148 дней после появления игры в США только лишь автомобилистами было нанесено ущерба на сумму 2,0—7,3 млрд. долларов. Сюда включили все аварии, которые, согласно официальным отчётам, произошли по вине играющих в Pokemon GO за рулём. Более того, по этой же причине два человека расстались с жизнью.*

Сказки о безопасности: Защита от дронов

– Доброе утро, Иоганн! Впрочем, мы вряд ли можем назвать его очень добрым. Вас уже минут 10 дожидается представитель имперской службы безопасности, он очень взволнован, однако молчит и ждет вас.

– Жанетт, вы предложили ему кофе?

– Безусловно, шеф! Однако он вежливо отказался, сказав, что с удовольствием выпьет его вместе с вами.

– Хорошо! Тогда зовите его и принесите нам, пожалуйста, кофе со сливками.

– Одну минуту!

В кабинет Иоганна вошел молодой человек, которого с успехом можно было принять за банковского клерка. Он ничем не отличался от десятков и сотен тысяч других молодых людей. Более того, увидев его на улице, вы бы никогда не запомнили его лицо. Оно чем-то было похоже на лица всех остальных людей и казалось, что вы уже его где-то видели.

– Доброе утро, господин директор!

– Доброе утро! Называйте меня просто по имени, Иоганн. Что произошло?

– У нас чрезвычайное происшествие. Вчера над нашей новой атомной электростанцией мы засекли квадрокоптер. Он оборудован мощной видеокамерой весом около 5 кг. Мы сумели его посадить, однако кому он принадлежит, понять так и не смогли.

– А что было в отснятых материалах?

– Сама станция, пути подъезда к ней. Мы подозреваем подготовку к террористическому акту. Боюсь даже представить, если бы этот беспилотный аппарат был оборудован взрывчаткой. Это привело бы к огромной аварии.

– Безусловно. И что вы предлагаете? И причем тут наш департамент?

– Мы считаем, что необходимо в состав постов противовоздушной обороны вокруг станций вводить специальные станции по борьбе с беспилотными средствами.

– Давно пора, я уже говорил об этом. А в Академии вводить специальность по борьбе с беспилотными средствами. Но пока денег нам не выделили, я как раз собрался на доклад к императору, где настоятельно буду требовать этого.

– Наше руководство готово вас поддержать. Но пока таких специалистов очень мало, мы хотели бы попросить вас поучаствовать в обучении военных.

– Мы согласны, но здесь гораздо большую помощь могут оказать специалисты компании, производящей средства перехвата беспилотников.

– Естественно. Мы уже говорили с ними. Но нам нужны будут не только специалисты по перехвату. Нам нужны те, кто сможет расшифровать информацию, собранную такими устройствами, а тут без вас не обойтись.

– Согласен. Готовьте приказ. Его нужно будет согласовать с департаментом обороны, департаментом контрразведки и нами, естественно, а затем утвердить у императора.

Так в империи появились войска радиоэлектронного противодействия. Угроза атак с воздуха, да и не только с воздуха была признана абсолютно реальной.

> *Увы, угроза атаки дронов, начиненных взрывчаткой, актуальна уже сегодня. В октябре 2014 г. полиция Нью-Йорка заявила, что дроны, несущие взрывчатку, стали террористической угрозой номер один для властей города. В октябре и ноябре того же года было зарегистрировано порядка двух десятков случаев нарушения дронами воздушного пространства над 15 из 19 АЭС, находящихся в разных уголках Франции.*

Сказки о безопасности: Самоуничтожение дрона

– Доброе утро, Иоганн! Впрочем, мы вряд ли можем назвать его очень добрым.

– Вилли! Что произошло?

– Наши люди попытались перехватить управление дроном, которого засекли при попытке пересечь границу. Однако произошло странное. Вроде бы вначале он стал подчиняться нашим командам, однако потом резко пошел вниз и вдруг начал распадаться на части. Эти части разлетелись на довольно большой территории. Но главное – пропал груз. Он был сброшен над озером, и мы его не нашли.

– Ну что ж, бывает. Не всегда вашим людям должно везти.

– Иоганн, так бы оно так. Но не совсем! Это уже третий похожий случай. При первой попытке перехватить дрон он взорвался в воздухе. Во второй раз – резко спикировал и сбросил груз над озером, а потом сам распался на части. Снова-таки, над водоемом. Это уже не просто случайности. Кто-то научился делать дроны, которые при попытке перехватить управление просто распадаются на части и сбрасывают груз над водоемом. Мы хотим понять, как это делается и кто научился это делать.

– Интересный вопрос. Мы попробуем вам помочь.

Прошел месяц.

– Вилли, мы сможем помочь вам в деле с дроном.

– Как? Вы нашли причину?

– Да. Самораспадающийся дрон придумала фирма А. В случае аварии он начинает разваливаться. Но при этом он анализирует, над какой поверхностью пролетает, и старается самоуничтожиться над безлюдной поверхностью. В первую очередь – над водной, чтобы причинить минимальный ущерб. В свою очередь контрабандисты усовершенствовали этот метод. Вот и все.

– Такого я просто не ожидал.

Amazon запатентовала дрон, который в случае поломки, например при взрыве аккумулятора или повреждении пропеллера, будет самостоятельно распадаться по частям прямо в воздухе под управлением контроллера. Последний будет быстро анализировать траекторию полета, состояние погоды и окружающую местность перед тем, как начать процесс распада.

Сказки о безопасности: Перепрошитый эйрбэг

– Доброе утро, сэр! Впрочем, мы вряд ли можем назвать его очень добрым.

– А что случилось?

– На трассе 45 авария, сэр! Погиб владелец автомобиля, мистер Морган. Но вот что удивляет. Приехали наши эксперты и говорят, что вся механика в полном порядке, а автомобиль выскочил за пределы трассы на повороте и врезался в дерево. При этом водитель даже не пытался тормозить.

– На какой скорости он ехал?

– Порядка 130—140 км/ч.

– А может у него стало плохо с сердцем или он перебрал лишнего?

– Наркотиков и алкоголя в крови не обнаружено. Механика, повторю еще раз, в полном порядке.

– Обратитесь за помощью к изготовителям автомобиля. Пусть пришлют эксперта. У нас же с ними соглашение.

Прошла неделя.

– Ну что там с экспертизой.

– Эксперт заявил, что механика в полном порядке, а вот подушки безопасности выстрелили до аварии. Водителя оглушило, и он вылетел с трассы.

– Погодите, это как?

– По словам эксперта, кто-то изменил прошивку бортового компьютера и как только скорость превысила 130 км/ч, подушка автоматически выстрелила.

– Но как удалось сменить прошивку?

– Автомобиль за два дня до этого был на плановом техническом обслуживании. Судя по всему, именно там и был перепрошит бортовой компьютер. Нужно бы съездить на эту станцию и поговорить с тем, кто занимался компьютером.

– Ну так съездите и привезите сюда этого умника.

Прошел день.

– Шеф, нам не повезло. Человек, который перепрошивал компьютер – мертв. По словам владельца станции, это был очень умный сотрудник и компьютеры автомобилей он смотрел

только сам. А позавчера он попал под грузовик, водитель которого скрылся с места происшествия. Сам грузовик был в угоне. Его нашли за несколько кварталов от места аварии.

– Да… Нам не удалось выйти на преступника.

– Да, но нас есть и хорошие новости. При полном осмотре попавшего в аварию автомобиля в запасном колесе были обнаружены наркотики. Теперь мы понимаем, кто и почему убил водителя. Судя по всему им нужен был не сам водитель, а эта запаска. Но снять ее они не смогли. Помешали свидетели. Так что теперь будем искать, кому это было выгодно.

Отдавая в будущем ремонт свой «компьютерный» автомобиль, вам придется смотреть за контрольными суммами прошивки на сайте производителя и в своем авто.

Сказки о безопасности: От слежки не спрятаться

Когда же наконец-то на улице будет светить солнце? Снова тучи, снова темно. Вот уже скоро 9 утра, а в кабинете снова приходится включать свет. Черные тучи заволокли небо. Пошел снег.

Иоганн не любил такую погоду. Когда на улице рано темнело, у него портилось настроение. В такое время хорошо сидеть в кресле у камина, укрывшись пледом и читать книгу, изредка попивая чай со смородиновым бальзамом. Но служба есть служба, и тут не выбирают.

– Доброе утро, шеф! Вам звонят из департамента внутренней безопасности.

– С утра? Интересно что у них произошло. Соединяйте.

– Доброе утро, Иоганн! Сейчас к вам приедет наш курьер, посмотрите, сможете ли вы помочь.

Прошло полчаса. Каково же было удивление Иоганна, когда вместо простого курьера он увидел перед собой заместителя директора департамента внутренней безопасности.

– Здравствуйте, Иоганн! Не удивляйтесь, проблема настолько серьезная, что я просто не смог ее доверить обычному курьеру. Да и кофе у вас замечательный. Придется к вам мою секретаршу отправить на стажировку. А теперь о серьезном.

У нас проблема. Прибывает курьер наркоторговцев. Увы, мы знаем только его номер мобильного телефона. Нам нужно понять с кем он будет встречаться в нашей стране. Проблема в том, что мы не знаем ни кто это, ни через какую границу он прибудет.

– Думаю, что мы сможем вам помочь. Марк, подойди, пожалуйста. У нас есть интересная задача.

– Шеф, на самом деле задача с одной стороны интересная, а с другой – тривиальная. Нам нужно отследить, какие телефоны будут рядом с искомым и при этом будут переходить с ним из соты в соту. Задача не сложная, но требует больших вычислений. Сделаем! Мы как раз работали над такой задачей.

Прошла неделя.

– Ну что, Марк? Порадуешь наших «смежников».

– Конечно. Вот два номера, которые сопровождали нашего курьера. Более того, я могу сказать, где конкретно они встречались. Мало того, кто еще был на встрече и куда потом они отправились.

– Умница! Твои ребята сумеют отслеживать их дальнейшее передвижение?

– Безусловно. Причем в любой стране и с любыми сим-картами и даже без таковых. Ведь у нас широко распространены бесплатные точки Wi-Fi. А кто мешает отслеживать их?

– Молодцы! Думаю, что нам пора отслеживать таким образом телефоны. Естественно, это необходимо делать в тайне.

– Но как же приватность?

– А разве она существует? Ты еще в это веришь?

– Я? Нет давно.

> *Такой способ отслеживания телефонов существует достаточно давно. Издание The Washington Post раскрыло информацию о программе слежения за абонентами сотовых операторов по всему миру. Как следует из оказавшихся в распоряжении редакции документов Эдварда Сноудена, АНБ США создало программу CO-TRAVELER, анализирующую информацию о совместных перемещениях мобильных устройств.*

Сказки о безопасности: Как госслужащие подставились

Наконец-то на улице выглянуло солнышко. Небо очистилось от вчерашних туч и ничего не напоминало о том, что две недели подряд лил дождь. Выйдя на улицу, хотелось улыбаться всем встречным, ведь на улице наконец-то солнце!

Иоганн отправился на службу пораньше, чтобы немного прогуляться по утреннему парку. Сегодня пятница, а значит впереди выходные. Можно будет выспаться, погулять с собакой, поиграть с ребенком и просто отдохнуть!

Однако его мечты были самым грубым образом прерваны. Звонили с работы.

– Шеф, когда вас ждать? За вами выслать машину?

– Не стоит, я буду через 10 минут. У нас снова ЧП?

– Конечно. Из-за того, чтобы пожелать вам доброго утра, я бы не звонил.

Прошло 10 минут.

– Доброе утро, шеф!

– Доброе утро! Что у нас в этот раз произошло?

– Утечка персональных данных почти 200 тыс. пользователей подпольного сайта «для взрослых».

– Причина?

– Некорректная конфигурация базы данных. На сайте публиковались так называемые «подсмотренные» фото женщин, которые не подозревали, что их фотографируют. Примечательно, что среди утекших данных были обнаружены адреса электронной почты и IP, относящиеся к военным ведомствам и государственным органам как нашей империи, так и некоторых наших союзников.

– Что еще утекло?

– Логины, пароли, даты рождения и некоторые логи сайта, такие как «дата регистрации», «дата последней публикации», «репутация». Финансовой информации среди этих данных обнаружено не было.

– Ого! Но, вероятно, это не все?

– Увы, нет. Наиболее печально то, что среди похищенных данных находились адреса электронной почты, зарегистрированные в зонах. gov и. mil, что может привести к шантажу чиновников и военных.

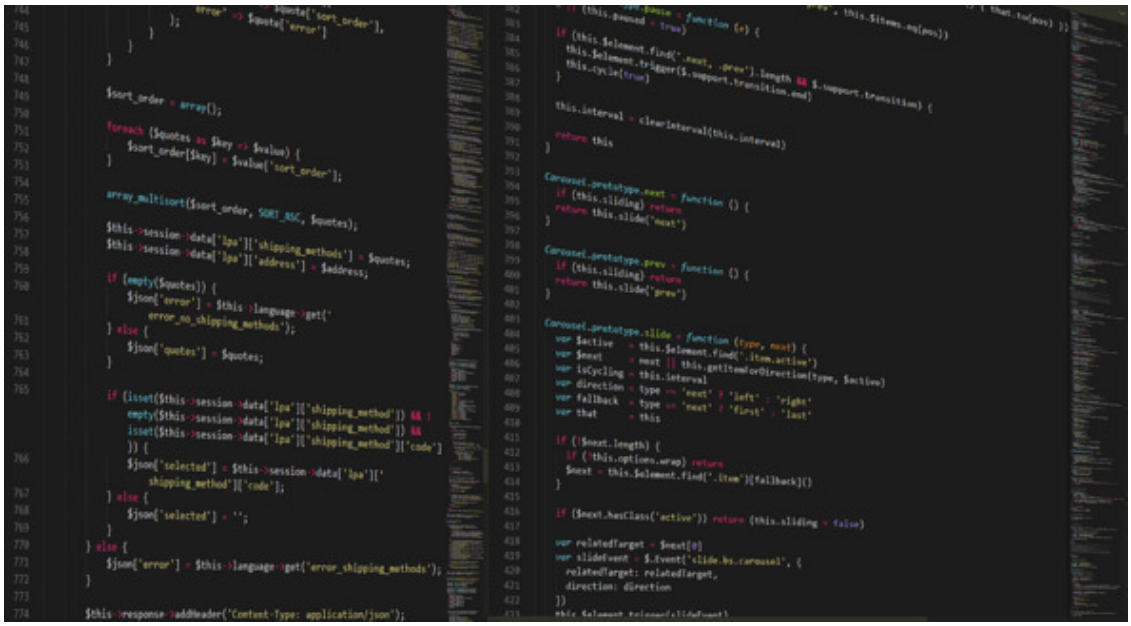
– Согласен, это чрезвычайно важно. Вы уже сообщили руководителям этих пользователей о необходимости срочно сменить почтовые адреса? А скомпрометированные поставить на контроль?

– Безусловно.

– Придется еще раз напомнить пользователям о запрете использования корпоративных почтовых ящиков в личных целях!

> *Увы, эта история состоялась на самом деле. Персональные данные почти 180 тыс. пользователей подпольного сайта «для взрослых» The Candid Board попали в сеть из-за некорректно сконфигурированной базы данных. Примечательно, что среди утекших данных были обнаружены адреса электронной почты и IP, относящиеся к военным ведомствам и госорганам США, Великобритании и Австралии.*

Сказки о безопасности: Как агентов раскрыли



– Иоганн! Приезжайте скорее! Машина за вами уже вышла! Ваши ведущие специалисты тоже оповещены! Все отозваны из отпусков! У нас ЧП! Вернее, даже не так. У нас беда! В силовых структурах объявлена высшая степень готовности! На моей памяти такого еще не было! Всем рекомендовано прервать отпуска и прибыть к месту службы. Охране объектов выдано автоматическое оружие, а всем агентам обязательно носить с собой личное оружие. Вернее даже не только агентам, а всем сотрудникам, включая вспомогательный персонал.

– Да что случилось, Мари!

– Не знаю, шеф! Машина уже должна подъезжать к дому. Да! Учтите, вы поедете не в департамент, а на объект «Озеро»!

– Понял, выезжаю.

Прошло полчаса.

– Итак, господа, у нас чрезвычайное происшествие. В Интернете обнаружена база данных, содержащая более 250 тыс. имен, фотографий, домашних и электронных адресов агентов департамента имперской безопасности. Кроме того, там же находятся данные о членах их семей, о состоянии их карточных и банковских счетов, номера автомобилей и номера их рабочих, домашних и мобильных телефонов. Кроме того, на этом сервере обнаружены копии 160 тыс. файлов из внутренней системы ведения дел и расследований.

Это самая грандиозная утечка данных! Император в бешенстве. От нас ждут ответа, получил ли кто-либо кроме исследователей безопасности из фирмы А доступ к этим данным.

– Шеф, как давно они обнаружили утечку?

– Позавчера.

– А при каких обстоятельствах?

– Абсолютно случайно, в том-то и дело. База данных обнаружена на домашнем сервере в облаке. Сервер принадлежит одному из разработчиков департамента имперской безопасности. Это его домашний сервер!

– Погодите, правильно ли я понимаю, что он вынес все эти данные домой???

– Абсолютно верно! Официальная причина – он хотел усовершенствовать некоторые свои программы и работал с ними дома.

– Вызовите ко мне руководителя отдела разработки, начальника службы ИБ этого департамента и начальника службы ИТ. И пригласите присутствовать на беседе директора департамента! Безобразие какое! Они что, не контролируют внешние устройства? Не контролируют копирование совершенно секретной информации? Они что, не понимают, что они делают?

– Судя по всему, именно так!

– Марк, вы возглавите расследование. Полномочия у нас с вами самые широкие. Император уже подписал приказ.

Прошло две недели.

– Иоганн, вы будете удивлены, но лица, скопировавшие всю эту информацию, реально хотели сделать как лучше и не планировали ее продавать или предоставлять к ней доступ кому-то другому. Они просто стремились усовершенствовать свое же программное обеспечение!

– Ужасно. Вот уж действительно, дорога в ад вымощена благими намерениями. Нам с вами придется самим заняться построением системы информационной безопасности этого департамента.

– Но у нас нет столько людей.

– Придется привлекать студентов старших курсов Академии, а куда деваться?

> *Увы, похожая история произошла в Department of Homeland Security, США. Согласно документам, полученным в мае USA TODAY, на домашнем (!) сервере сотрудника DHS была обнаружена конфиденциальная персональная информация 246 тыс. сотрудников этого ведомства.*
>
> *Кроме того, на этом же сервере обнаружены копии 159 тыс. файлов из внутренней системы ведения дел и расследований генеральной прокуратуры.*

Сказки о безопасности: Говорящий мусор

Это утро в полицейском участке началось с того, что капитан собрал детективов и задал им вопрос.

– Коллеги, доброе утро! У нас проблема. Нам нужно как можно быстрее собрать максимально полную информацию о жителях дома 17 на 5-й улице. Это частный одноэтажный коттедж. Мы не знаем, сколько в нем проживает людей. Мы не знаем, мужчины это или женщины. Фактически мы ничего не знаем. Ваши предложения?

– Попробовать поискать что-то в социальных сетях?

– Поговорить с соседями?

– Оба предложения не подходят. В социальных сетях люди не пишут свой почтовый адрес. Говорить с соседями – нельзя, мы вспугнем их. Думайте, коллеги, думайте!

– Поговорить с провайдером, который предоставляет Интернет в этот дом? И заодно с представителями энергетической компании. Так мы сможем приблизительно понять, сколько людей там проживает (по среднему потреблению электроэнергии).

– Запросить у мобильного провайдера данные о мобильных телефонах по этому адресу?

– Отлично! Итак, что еще?

– Шеф, а почему мы не думаем о самом полном источнике информации? О мусоре! Под видом мусорщиков пришлем туда наших ребят и проанализируем их мусор!

– Гениально, стажер! Вот этим и займитесь вместе с Карлом и Дином. Вывоз мусора у них сегодня вечером. Жду результаты.

Наступил вечер. Анализ мусора занял половину ночи.

Утром пришло время очередного доклада.

– Шеф, в доме живут трое. Судя по найденным в мусоре чекам из магазина и пиццерии, едоков там на троих. Кроме того, мобильный провайдер указывает на минимум три мобильных телефона. Кстати, самое интересное. В дом заказали товары бытовой химии, которые применяются для изготовления взрывчатых веществ, а также три недорогих мобильных телефона. Значит они собираются создать минимум три бомбы с мобильными взрывателями.

– Погоди, может они уже собрали эти бомбы?

– Нет. Один из компонентов заказан только на завтра. А без него эти штуки не взорвутся.

– Вызывайте спецназ. Будем штурмовать здание. Они внутри?

– По сведениям мобильной компании – да. Но сейчас проверим.

– Как?

– Сын соседки регулярно запускает квадрокоптер. А сегодня вместо него коптер запустит наш специалист. А мы посмотрим картинку. В том числе в тепловом диапазоне. И точно будем знать, что происходит.

– Стажер, вы получите от нас наилучшие рекомендации! Все же хорошо вас учат в Академии!

А вы всегда смотрите, что выбрасываете в мусор?

Сказки о безопасности: Записанный маршрут

Утро сегодня, как и много дней подряд, началось с того, что за окном шел дождь. Вернее, даже не просто дождь, а что-то непонятное, не то дождь, не то туман. Погода кажется шептала всем, чтобы они оставались дома и спали дальше. Но нужно идти на службу.

– Капитан, у нас происшествие.

– А когда было иначе? Что случилось?

– Утром патруль попытался остановить черный автомобиль с номерами соседнего округа. Но вместо того, чтобы остановиться, пассажир начал отстреливаться, а машина попыталась скрыться.

– Вы объявили «Перехват»?

– Конечно. Через полчаса водитель не справился с управлением, машина сорвалась с обрыва в пропасть. Водитель и пассажир мертвы. Автомобиль находится на нашей стоянке.

– Вы обследовали машину?

– Криминалисты сейчас заканчивают, а вот и они.

– Шеф, неудивительно, что они пытались скрыться. В машине около двух килограммов наркотиков.

– Личности водителя и пассажира установлены?

– Водителя пока нет, а пассажир – Лео Норт. Известный наркоторговец.

– Он продает в розницу?

– Нет, опт. Второй, судя по всему, его водитель. Машина принадлежит Лео. Он всегда плохо водил машину.

– Н-да… Что еще мы сможем узнать? Если бы знать маршруты этого автомобиля…

– Шеф, стажер Мартин Рид к вам просится. Говорит, что это очень срочно.

– Что ты хотел, малыш?

– Шеф, я хотел сказать, что мы сможем узнать маршруты этого автомобиля с привязкой по времени и всеми остановками.

– Да? И как?

– Шеф, я как раз в Академии писал курсовую работу по этим автомобилям. Машины фирмы К используют встроенные GPS-навигаторы с запоминанием маршрутов. Чтобы не прокладывать их заново.

– Ты сможешь извлечь из этого хлама маршруты?

– Да. За последние пару месяцев. Больше – нет.

– Что тебе нужно для этого?

– Да ничего особенного. Ноутбук и стол. Ну и сам навигатор. Я уже его снял.

– Молодец. Жду результаты.

Прошло два часа.

– Шеф, вот его маршруты. Обратите внимание. Раз в три дня, в одно и то же время, он приезжал в старый парк в центре города. Потом уезжал к себе.

– А точнее сможешь указать?

– Ну, я могу найти точку приблизительно. Потом нужно будет обыскать в радиусе приблизительно 100—200 м вокруг. Думаю, там тайник.

– Молодец, стажер. Что еще?

– Еще могу сказать, кому и как он переводил деньги. Я отследил его платежи.

– Ну что ж. Вас толково учат. Я напишу об этом в отзыве о стажировке.

> *Сегодня автомобиль марки Chrysler оборудуется навигатором с запоминанием маршрутов движения для более быстрого построения маршрута. Так что это совсем не сказка.*

Сказки о безопасности: Для определения местоположения можно обойтись без геолокации

Вчера была вьюга, а сегодня как в насмешку над понедельником утро выдалось солнечным. Так не хотелось идти на работу. Однако несмотря на солнечное утро, день выдался хмурым. Впрочем, таким же было и настроение. Непонятно, что делать с последней просьбой комиссара полиции. Нужно было разобраться, как отследить местоположение преступника. Он не использовал GPS, да и в принципе не пользовался GSM. Когда ему нужно было позвонить, он использовал ближайшую бесплатную Wi-Fi точку и звонил через Интернет. Что делать и как?

– Марк, Рита, может вы подскажете, что делать?

– Шеф, в принципе задача сводится к тому, как на его смартфон заслать нужный троян, который установит нужное нам приложение.

– Погоди, Рита, а разве существует приложение, которое позволит нам отследить его точное местоположение, если на устройстве отключен GPS?

– Конечно существует. Современные смартфоны и планшеты оборудованы огромным количеством датчиков, которые фиксируют множество различных данных, которые мы можем сравнивать с различными внешними источниками, например, топографическими картами, картами погоды, картами Wi-Fi покрытия и т. д. В принципе таких данных достаточно для того, чтобы отслеживать перемещения пользователя.

– Рита, вы гений! Нам нужно в срочном порядке в тестовой лаборатории апробировать такой подход. А что еще можно собирать?

– Давайте попробуем собрать данные об IP-сетях и Wi-Fi подключениях и сверим их с общедоступными базами данных сетей Wi-Fi, а затем нанесем их на карту.

– А если также использовать данные гироскопов, акселерометров и датчиков высоты для определения скорости, направления движения, остановки объекта и текущей высоты? А после

этого объединить все и с помощью специального алгоритма определить способ передвижения владельца, например, шел ли он пешком, ехал на поезде, автомобиле или же летел на самолете?

– А причем тут сведения о погоде?

– Можно использовать показания датчиков температуры, влажности и атмосферного давления, сравнивая полученную информацию с отчетами службы прогноза погоды для проверки и подтверждения полученных ранее результатов.

Прошло две недели.

– Что показал эксперимент?

– Точность обнаружения удовлетворительная. Главное, чтобы сторонние сервисы давали правильные данные. А то у нас выйдет как с датчиком погоды. Вспомни, Марк!

– Ага. Карта погоды соврала. А мы два дня думали, что с программой.

– Хорошо. А как заразить, придумали?

– Это самая простая задача. Придумали.

> *А вы думали, что, отключив GPS, вы станете незаметны? Не обольщайтесь! Исследователи безопасности из Принстонского университета разработали PoC-приложение PinMe, позволяющее отслеживать точное местоположение пользователя, даже если на устройстве отключен GPS. Оно было установлено на трех тестовых телефонах – Samsung Galaxy S4 i9500, Apple iPhone 6 и Apple iPhone 6S. Программе удалось отследить перемещения испытуемых без доступа к данным о геолокации устройств.*

Сказки о безопасности: Автомобильный медиа-центр

Погода этой зимой была какой-то странной. На улице снег сменялся дождем, постоянно за окном висели тучи и свет в комнате приходилось включать практически на весь день. Это очень раздражало Иоганна, ведь он любил яркое солнце, а тут день напоминал сумерки. Вот и сегодня с утра было непонятно, утро это или вечер. Любимую прогулку по парку пришлось отложить. В такую погоду не сильно хотелось идти пешком.

Заехав во двор департамента, Иоганн заметил на служебной стоянке арендованный автомобиль. Это было крайне необычно, и потому он подозвал к себе начальника караула.

– Доброе утро, Вилли! Что случилось? Кто это приехал на арендованном автомобиле и почему он стоит на площадке для служебных?

– Это Карл. Он сказал, что автомобиль нужен ему для какого-то расследования и просил предупредить, когда приедете вы, Марк и Рита.

– А они уже здесь?

– Да. Ждут только вас.

– Доброе утро, коллеги! Что случилось? Попросите кто-нибудь приготовить нам кофе, а то в такую погоду очень хочется спать, а не работать!

– Кофе готов! Сейчас принесут.

– Карл, что такое? Машина сломалась? Мог бы на такси доехать.

– Шеф, вчера моя жена арендовала машину и подключила свой телефон к ее медиа-центру.

– Для чего?

– Ну хотелось ей слушать любимую музыку со смартфона и использовать свою телефонную книгу в поездке. Кроме того, так как в прокатном автомобиле установлена навигационная программа, то она использовала ее для прокладки маршрута.

– Курт и что тут криминального? Я сама так иногда делаю.

– Рита, в принципе криминального ничего. Но самое интересное начинается дальше. Вы ж знаете о моей паранойе. Перед тем, как вернуть автомобиль, я решил посмотреть, что осталось в его медиа-центре. Ведь при подключении происходит синхронизация вашего телефона с медиа-центром машины и все ваши данные сохраняются в его внутренней памяти. То же самое касается и маршрутов ваших поездок.

– И что ты увидел?

– Я увидел передвижения моей жены и шесть синхронизированных телефонных книг предыдущих водителей. Потом я дал запрос во все прокатные компании. Оказалось, политики стирать данные предыдущих клиентов нет ни у одной из них.

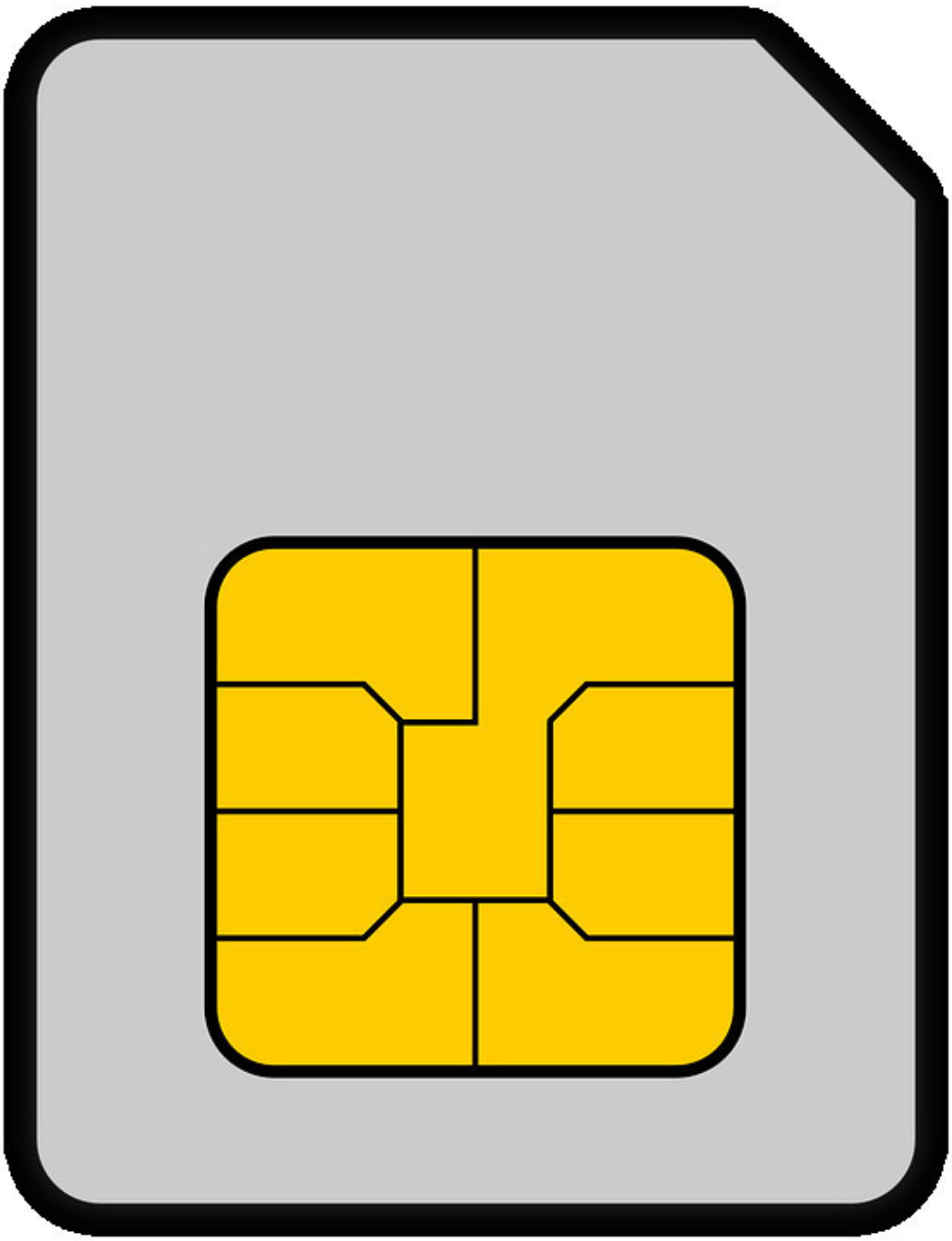
– Курт, ты поднял весьма и весьма интересную проблему. Но ты ж знаешь, у нас инициатива наказуема. Ты поднял вопрос, тебе и готовить документы. Нужно докладывать об этом императору. А кроме того, в пятницу вечером в вечерней передачи на первом канале телевидения империи тебе же придется выступать по этому поводу.

– Шеф, а давайте выступит Мари. Она куда фотогеничнее меня.

– Ну что ж, готовьтесь выступать вдвоем.

Увы, эта история совсем не фантастика, это реальность. Помните об этом, когда будете арендовать автомобиль.

Сказки о безопасности: Инсайдерское ограбление



– Потапыч, сможете помочь?

– Что случилось?

– Нам нужна ваша консультация. У нас в банке произошло хищение денег со счетов клиентов. Всего пострадали порядка 20 человек.

– А что именно вы выяснили?

– Мошенники регистрировали SIM-карту на имя жертвы, затем заходили в мобильное приложение банка и подавали заявление на замену банковской карты, используя поддельную нотариальную доверенность.

– Вы выяснили, что общего у ограбленных клиентов?

– Да. Все они обслуживались в одном отделении банка. Кроме того, все они, положив деньги на счет, не обращались в банк на протяжении длительного срока.

– Ну что, ищите в первую очередь среди персонала отделения, причем скорее всего это будет кто-то из высокопоставленных сотрудников с высоким уровнем доступа к информации о счетах клиентов. Но мне интересно другое.

– Что именно?

– Ну не в руках же выносили информацию. Неужели у вас до сих пор никто не отслеживает отправляемую электронную почту? Или у вас до сих пор не смотрят за использованием внешних носителей? Чего вы ждете? Пока вынесут все отделение? Вместе с креслом заведующего?

– Ну зачем вы так? Все нужное оборудование и программное обеспечение закуплено. Осталось его просто внедрить. Правда это затягивается.

– Ну вот потому вы и получили то, что получили.

Прошло две недели.

– Потапыч? Это вас беспокоят из банка. Вы были правы. Это заведующая отделением передавала данные о счетах. А наблюдать за ее почтой администратор просто остерегался. Ну вы ж понимаете, для безопасности все равны, но некоторые равнее всех.

– Ну вот вы и получили.

Такая история может произойти практически в любом банке. Вы так не думаете?

Сказки о безопасности: Троян из техподдержки

Иоганн очень не любил зиму. И не потому, что было холодно. Чаще всего температура держалась около нуля, но ветер, снег с дождем и проникающая сырость могли свести с ума кого угодно. Да еще и вечное отсутствие солнца. Все время темно. Идешь на работу – темно, возвращаешься домой – темно! Но радовало одно. Еще какие-то два месяца и будет значительно светлее.

Вот и сегодня погода не задалась. С утра шел дождь, на улицах народ старался как можно быстрее добежать до места назначения, чтобы меньше вымокнуть. В такую погоду Иоганн вызывал служебный автомобиль, а не шел пешком.

– Доброе утро, шеф! Вас уже дважды спрашивали из городской полиции. Их представитель дожидается вас в конференц-зале.

– Ты не знаешь, что случилось?

– Я не спрашивала. Сидит – значит так надо.

– Принеси, пожалуйста, нам кофе.

– Доброе утро! Что привело вас к нам так рано?

– У нас убийство. Причем наши ребята заметили, что все записано на этом ноутбуке. Мы не выключали его и ничего не трогали. Я приехал к вам, может вы поможете. К сожалению, здесь записано само убийство, но лицо убийцы не разобрать.

– Хорошо, мы сейчас займемся вашей проблемой.

Прошло полчаса.

– Шеф! Эта запись выложена в DarkWeb и набирает все больше просмотров. Она выложена на специальном сервере, на который выкладываются ролики с реальными убийствами и насилием. За просмотр там платят деньги, причем не маленькие. Таким образом мы можем сказать, что это убийство было осуществлено с целью заработать.

– Погодите, но не мог же убийца сказать: «Погодите, я камеру включу, а потом буду вас убивать!»

– Конечно нет.

– Значит компьютер был взломан заранее. Займитесь ним.

– Хорошо.

Прошло два часа.

– Шеф, а компьютер не был взломан.

– Как? А кто ж тогда включил видео?

– Судя по всему, видео включили удаленно. Данный ноутбук обслуживает фирма М. Они осуществляют техническую поддержку.

– Придется проехать в эту фирму и уточнить, кто занимался этим компьютером. Вызывайте полицию и привезите того, кто это делал.

На следующий день комиссар полиции лично приехал в департамент интеллектуальных преступлений, чтобы поблагодарить Карла за хорошую работу. Как выяснилось, ПО для видеосъемки было установлено удаленно специалистом технической поддержки фирмы М. Он давно занимался незаконной видеосъемкой, продавая фильмы в DarkWeb. Ранее это была преимущественно домашняя порнография, а когда это стало приносить мало денег, уговорил своего друга на продажу убийств.

Мрачная история. Вывод, который нужно сделать весьма прост. Доверяя технической поддержке, все же смотрите, что вам устанавливают. Учитесь! Иначе вас могут легко обмануть…

Сказки о безопасности: Личная безопасность на поверку – 1

После нескольких попыток взлома персональной информации в империи задумались о необходимости тестирования систем персональной безопасности. В связи с этим решено было создать подразделение, которое бы тестировало безопасность частных лиц и потом доводило рекомендации до широкого круга граждан. Причем как высокого ранга, так и обычных. Так появился проект, названный «Взлом системы».

Главой вновь образованного отдела департамента интеллектуальных систем был назначен Роберт Ноланд, работавший до этого оперативным сотрудником.

Первым делом этого отдела стала проверка уровня защищенности руководителя подразделения государственной компании N г-на Грина.

– Итак, господа, мы должны проверить что мы сможем узнать о Джордже Грине. Время, поставленное на задачу всего неделя.

– Понятно, шеф!

– Г-н Грин уверен в своей безопасности. Попробуем его разочаровать. Вы, Жанна, должны будете проследить за его автомобилем. В напарники вам мы дадим Эльзу.

– Шеф, ну почему я не удивлена?

– Все верно. Две очаровательные молодые девушки всегда смогут отговориться невнимательностью. Какого цвета его машина?

– Белого!

– Поэтому вы возьмете тоже белое авто.

На следующее утро девушки занялись слежкой. И Джордж ее не заметил.

Как заметить слежку? Проще всего, увидев, что за вами следует какой-то автомобиль, повернуть направо, проехать два-три квартала и снова повернуть направо. Затем через пару кварталов снова повернуть направо и повторить то же самое. Таким образом вы опишете круг. Ни один обычный автомобилист не будет так делать и, если вы увидите, что за вами все время следует один и тот же автомобиль – за вами следят. Остановитесь, но ни в коем случае не выходите из авто. Вызывайте полицию.

Следующий этап проверки – место работы. Как ни странно, на работе большинство сотрудников уверены в своей безопасности. А совершенно зря! Ведь по статистике от 30 до 70% пользователей на работе банально воруют информацию, в том числе персональную.

– Джейсон, вы с Питером завтра отправляетесь на работу к г-ну Грину. Представитесь техниками по ремонту копировальных машин из компании «Copy Doctor». Униформу получите на складе. Не забудьте сделать себе пропуска.

– Но шеф, мы же не знаем, как выглядят пропуска этой компании.

– Ха! Именно в том и прелесть! Стандартной формы пропуска не существует. Загляните к ним на сайт, посмотрите, как выглядит их логотип и создайте себе пропуска с любым штрихкодом.

– Понятно. Наша задача проверить, что угрожает ему на работе?

– Все верно!

Джейсон и Питер приехали на работу к Джорджу Грину. Итак, первая линия обороны. Администратор. Пустит ли она их в офис?

– Привет! Вы сегодня очаровательно выглядите! Как у вас дела?

– Отлично, спасибо! Сегодня изумительный день! Что вас привело к нам?

– Мы техники из компании «Copy Doctor». Нас вызвали заменить прижимной валик на копире. А вы новенькая? Раньше я не видел тут такую хорошенькую девушку.

– Нет, я уже несколько месяцев здесь работаю.

– Наверное у нас смены разные. А вот Джейсон у нас новичок, он сегодня первый день.

Питер специально переводит тему на Джейсона, отвлекая внимание от себя. Мошенники, как правило, тоже стремятся вас отвлечь, чтобы сбить с темы разговора и полностью завладеть вашим вниманием.

Питер задал вопрос, ведь тем самым он вынуждает девушку отвечать и ставит ее в подчиненное положение. В данном случае его цель отвлечь девушку чтобы она не спросила пропуск. Но из этого у него ничего не вышло.

– Ваш пропуск?

Питер вытащил из кармана фальшивый пропуск и показал его.

– Проходите!

В чем состоит ошибка администратора? Она не перезвонила в фирму «CopyDoctor», и даже не перезвонила в свой технический отдел, чтобы уточнить, а вызывали ли вообще специалистов по копировальным аппаратам, и не попросила копию наряда на проведение работ, заверенную специалистами технического отдела. Более того, она не вызвала никого из техников, чтобы те проводили ремонтников, а пропустила их в здание самих! Нельзя, чтобы по зданию компании самовольно ходили посетители. Их должны сопровождать те сотрудники, к которым они пришли, вплоть до момента ухода с территории компании.

Сказки о безопасности: Личная безопасность на поверку – 2

После успешного преодоления первой линии обороны компании в лице администратора Питер и Джейсон получили пластиковые пропуска в здание и поехали на 24-й этаж, в отдел г-на Грина. Пропуска напоминали обычные пластиковые карты, и Питер решил, что на обратном пути они их оставят себе, а в машинку для сдачи временных пропусков выбросят самодельные заготовки. В результате у них останутся нормальные временные пропуски. Тем более что в большинстве бизнес-центров служба безопасности их не обнуляет ежедневно, а просто достает из машины и снова пускает в оборот.

Надеюсь, ваша служба безопасности обнуляет карточки временных пропусков? Вы проверяли?

В отделе Грина, как это часто бывает, особого порядка на столах не было. То тут, то там на столах валялись мобильники и даже кем-то успешно забытый кошелек. Короче, вору было бы, где разгуляться. По просьбе Питера Джейсон все фиксировал на миниатюрную камеру, которая в виде ручки торчала из его кармана. Но вот и кабинет Грина. Он отделен от общего зала стеклянной дверью. Но она открыта. На столе Грина лежат ключи от машины. Питер забрал их себе в карман. А вот и копировальная машина. Рядом как обычно валяется гора каких-то документов, но сегодня они не цель. Целью является жесткий диск, установленный в копировальной машине и содержащий копии откопированных материалов. Минута работы и жесткий диск заменили на новый.

– Питер, нам пора.

– Действительно пора. Давай переставим его автомобиль на соседнее парковочное место. Интересно, заметит ли он перестановку?

– Ага. А кроме того, я хочу подложить ему в машину старенький смартфон, чтобы отследить его маршруты. Интересно, куда он ездит и где бывает.

– Не забудь вернуть администратору ключи от его машины, скажем что увидели их на парковке рядом с автомобилем.

Так и сделали.

Как ни странно, но Грин не заметил, что его автомобиль переставляли. А вот мобильник в его автомобиле позволил отследить его маршрут и увидеть, что Грин почему-то не поехал после работы домой, а свернул на улицу, которая вела на другой конец города к дому 15 на 18-й улице. Там он пробыл два часа и вернулся домой. В доме 15 размещался маленький отель, который часто использовали влюбленные парочки.

– Питер, а вот это уже интересно. Что еще вы сможете узнать?

– Шеф, пока мы были в компании, мы успели скопировать его токен безопасности от панели управления облачным хранилищем смартфона. Давайте пороемся там.

– Да. И не забудьте порыться у него в мусоре. Мусорные баки стоят на неохраняемой территории. Там, увы, обычно, можно найти массу интересного.

Утром Питер нашел в баке несколько чеков из ресторана, предложение банка и даже чеки из гостиницы с 18-й улицы.

> *А вы знаете простейший способ уничтожения бумаг? А ведь все просто. Достаточно использовать воду, отбеливатель и строительный миксер. Поместите бумагу в воду, дождитесь пока бумага намокнет и включите миксер на 5—10 минут. Если хотите полностью избавиться от любых надписей, добавьте отбеливатель и снова включите миксер на несколько минут.*

– Джейсон, ты видишь?

– Что? Клавиатуру его домашней сигнализации?

– Да!

– А давай установим видеокамеру и отследим нажатия на клавиатуру.

– Давай!

Так и сделали, замаскировав видеокамеру.

К вечеру после анализа облачной копии смартфона в распоряжении Питера были пароли Грина к его домашнему и рабочему Wi-Fi и даже к его банковскому счету.

Но самое интересное обнаружилось после внимательно анализа жесткого диска. На нем обнаружилась копия водительских прав Грина, его номер социального страхования, копия свидетельства о рождении, копия диплома и других его документов. С этими данными уже можно было смело говорить о хищении и подмене личности.

– Джейсон, не забудь уничтожить те данные, которые нам не нужны.

Прошла неделя.

– Увы, г-н Грин! Как выяснилось, вы абсолютно открыты. Вот код вашей домашней сигнализации, пропуск от вашей работы, ваши маршруты передвижения, чеки из ресторана и даже чеки от гостиницы, в которой вы встречаетесь с милой Мери. Приятная у вас знакомая! Увы, все это можно использовать для шантажа, не так ли? Ведь ваша жена по контракту имеет право на большую часть вашего имущества, если заметит вас в измене? А вот копии ваших документов! Короче, будьте внимательнее!

– Интересно, а как ваши сотрудники относятся к безопасности своих персональных данных? Мы проверим это на следующей неделе.

Так, под громкие крики и возмущения в департаменте был создан новый отдел по проверке защищенности персональных данных.

Сказки о безопасности: Личная безопасность на поверку – 3

После успешного взлома личных данных г-на Грина настала очередь его сотрудников.

– Питер, а не попробовать ли нам развернуть фальшивую точку доступа в закусочной напротив офиса г-на Грина? В обеденный перерыв там бывает много народа.

– Отличная мысль. Завтра сделаем.

> *Учтите, когда вы работаете через открытую точку доступа, все ваши письма, запросы, фактически все ваше общение можно легко отследить. Вы готовы поделиться вашими данными?*

На следующий день Питер сидел в закусочной, притворившись что работает за своим ноутбуком. Фактически он развернул бесплатную точку доступа беспроводной сети и собирал данные посетителей. Те, обрадовавшись, что в кафе наконец-то появился бесплатный Wi-Fi, активно его использовали. Так прошел день.

На следующий день у Питера и Джейсона была масса работы. В перехваченном трафике нужно было выделить пароли от почты, работы, социальных сетей. Прочесть массу писем и вообще переварить полученную информацию. Особенно интересны были пароли, ведь очень часто пароли люди используют одни и те же и на работе, и для домашней почты, и в социальной сети.

А вы знаете, как обезопасить себя от хищения вашей информации при использовании бесплатного Wi-Fi? Для этого используйте два подхода:

1. Двухэтапная аутентификация. Все чаще это становится стандартом. На первом этапе вы используете пароль, а вторым фактором может быть SMS, которая присылается вам сайтом, или генератор кодов, установленный на вашем смартфоне. Учтите, если вы остановитесь на SMS, желательно использовать для этого отдельную SIM-карту, вставленную в простой мобильный телефон. Вы никогда не должны использовать эту карту для других целей. Еще один вариант – электронный ключ-токен, но это дороже.

2. Используйте VPN. Тогда весь обмен трафиком осуществляется по шифрованным каналам.

В результате атаки было собрано достаточно данных для последующих атак направленной социальной инженерии.

– Г-н Грин, вот пароли ваших сотрудников и данные о них. Учтите, они отдали это все добровольно!

– Что вы посоветуете сделать?

– В первую очередь позаботиться об осведомленности пользователей. Учите их! Ведь большинство атак сегодня происходит именно через ваших сотрудников. Делайте это регулярно, поощряйте желание учиться!

На этом проверка Грина была закончена, а отдел доказал свою незаменимость. Это было первое дело в истории отдела. Следующим, как уже решило руководство, будет атака на членов семьи. Кто-то скажет, что это некрасиво, может даже подло. Но! Шантажировать вас преступники могут и через ваших близких, подумайте об этом.

– Вы согласны, г-н Грин?

– Безусловно! Более того, предлагаю включить не только мою семью, а и семьи моих ведущих сотрудников.

Так начался следующий этап проверки.

Сказки о безопасности: Личная безопасность на поверку – 4

После успешной атаки на персональные данные г-на Грина было решено продолжить проверку того, насколько ответственно его сотрудники относятся к защите своих данных.

– Доброе утро, Иоганн! У нас идея!

– Доброе утро, Роберт! Что вы предлагаете?

– Мы предлагаем проверить сотрудников компании N, чтобы оценить, насколько они понимают, с какой информацией они работают и как ответственно относятся к ее защите.

– Что вы предлагаете?

– Как вы помните, напротив бизнес-центра, в котором расположена компания Грина, есть закусочная. Фактически это кафе, в котором обедают сотрудники этой компании. Сейчас она закрыта на ремонт. Мы предлагаем установить там передвижную закусочную, оборудовав ее подслушивающими устройствами, а потом проанализировать разговоры. Стоимость такой операции – копеечная. Но нужно сделать так, чтобы возле нее всегда была очередь, в которой и будут вестись нужные разговоры.

– Мысль интересная, но мне нужно согласовать это с представителями контрразведки. Ведь это их дело. Но мне это нравится.

Прошла неделя.

– Роберт, мы получили добро на проведение операции. Но вместе с вами в группу будет включен и представитель контрразведки. Мешать он не будет, его дело – анализ речевых данных.

Прошло две недели.

Результаты проверки были настолько плачевны, что в компанию в срочном порядке были отправлены сотрудники контрразведки. Как оказалось, персонал компании в обеденный перерыв обсуждал производственные процессы, вопросы оплаты и т. п. совершенно открыто. Но самое печальное было то, что часть этих вопросов относилась к государственной тайне.

Обсуждались не только производственные вопросы, а и сведения, которые можно было бы отнести к персональным данным и которые можно было бы использовать для шантажа тех или иных сотрудников.

Интересно, а если бы такой эксперимент поставили в вашей компании, то многое бы вы услышали? Ваши сотрудники в курсе, что производственные дела нужно обсуждать только на территории компании?

Сказки о безопасности: Личная безопасность на поверку – 5

Прошло две недели с момента организации мобильной точки сбора информации о сотрудниках компании г-на Грина. Закусочная уже работала в нормальном режиме, а Питер придумал новую атаку на сотрудников и, в частности, на самого Грина.

За пару дней вместе с Джейсоном они прослушали домашнюю Wi-Fi точку Грина и убедились, что она надежно защищена. Но ломать ее никто и не собирался. Нужно было лишь получить ее идентификатор. После этого на территории компании мистера Грина была развернута фальшивая точка доступа с тем же идентификатором, что и домашняя, но без пароля. Смартфон Грина находил знакомую точку и цеплялся к ней. В результате Питер получил пароль Грина к социальной сети и домашней и служебной почте.

– Роберт, вот ваши пароли. Вот домашний, вот рабочий, вот пароль от социальной сети.

– Ребята, а скрыть от вас что-то можно?

– Безусловно! Есть два способа. И первый – это применение везде, где можно двухэтапной аутентификации.

– Это когда вы предъявляете пароль, а вам приходит SMS с кодом? И вторым шагом является ввод кода?

– Да! Это гораздо надежнее, чем просто пароль.

– Я знаю. Но иногда, насколько я понимаю, SMS приходит поздно, а это неудобно, верно?

– Конечно! Но для этого есть еще два способа. Первый – вы устанавливаете себе генератор одноразовых паролей на смартфон, а второй – вы распечатываете порядка десяти кодов с сайта заранее, а потом распечатываете следующие 10.

– Впрочем есть и еще один способ. Кода вы входите на сайт вашей почты, вы указываете что работаете в недоверенной среде. Например, на чужом ПК. В этом случае вы можете ввести только вторую часть пароля. Без первой вообще. А так как каждые 30 секунд она меняется, то пусть перехватывают эту информацию. Это называется OTP (One Time Password).

– Здорово. Но как быть, если почтовый клиент не понимает двухэтапную аутентификацию?

– На самом деле и это не страшно. Вы можете заранее сгенерировать себе пароль для этого приложения. Даже если его и перехватят, он будет работать только на этом ПК и только

в этом приложении. А вы после работы в недоверенной среде его просто измените. Вот и все! Есть еще и аутентификация вашей Wi-Fi точки по сертификату. Тогда вообще атака точки будет невозможна.

– Спасибо! Я никогда не подозревал, что нужно столько знать.

– Знать нужно намного больше. Увы, атаки совершенствуются ежедневно! Учиться и учиться вот что нужно! Г-н Грин, заведите себе за правило, что ваш специалист по информационной безопасности должен регулярно обучать ваших сотрудников! Да и сам учиться у нас в Академии.

А вы готовы к таким атакам? Точно?

Сказки о безопасности: Атака на целостность и доступность

Маленький Зайка пришел из школы хмурым и на все вопросы, мол, как у него дела, отвечал односложно, что все хорошо. На самом деле все было не так хорошо, как он говорил, но зачем об этом знать маме? Вчера он с друзьями так набегался и наигрался, что просто забыл выучить домашнее задание. А сегодня, как назло, его вызвали к доске. Вот и получил плохую оценку.

И тогда Зайка решил схитрить, просто вырвав страницу из дневника. И теперь очень волновался по этому поводу. Как это примет мама? Решил он ничего не говорить. А рассказать потом, когда исправит плохую отметку.

– Зайка, что случилось? Почему ты такой хмурый? Если из-за плохой отметки по физике в школе, то не отчаивайся, исправишь! Я ведь знаю, что ты не выучил уроки.

– Откуда? Я ведь тебе ничего не говорил!

– Да-да, конечно, не говорил! И даже страницу вырвал из дневника! Я знаю.

– Но откуда?

– Да все просто. Знаешь, как папа называет такие действия на своем взрослом непонятном языке? Ты ведь помнишь, кем он работает?

– Да, конечно, помню. Наш папа – руководитель департамента информационной безопасности.

– Да-да. Так вот! Он говорит, что это атака на целостность и доступность информации и что это очень плохо!

– А ты откуда знаешь, что я страницу вырвал?

– Да потому что я, опять-таки, в папиных терминах, всегда перепроверяю полученную информацию по нескольким независимым каналам. Я просто позвонила тетушке Сове, твоей учительнице, и она мне все рассказала. Если хочешь, чтобы тебя впредь не могли атаковать так, как ты меня сегодня, всегда пользуйся несколькими независимыми каналами связи. Тогда ты сможешь получать объективную информацию. Понял?

– Да, мама! Хорошо, что у нас папа такой умный, а ты такая добрая. Я исправлюсь!

А вы тоже пользуетесь несколькими независимыми каналами связи? Или нет? Подумайте!

Сказки о безопасности: Чудо-фонарь

Вот и прошел Новый Год. Праздники позади, снова пора на службу. В последнее время Иоганн все чаще понимал, что империи нужны новые технологии. Увы, но все чаще и чаще полиция и служба безопасности обращались к нему за помощью в поисках тех или иных людей. Как просто пропавших, так и преступников. Он понимал, что сил его сотрудников катастрофически не хватает, как и техники на дорогах. Но что делать? Не вешать же камеры на каждом столбе? Мысль неплохая, но кто ж это будет делать? Ведь тогда нужны и микрофоны с динамиками, включаемые выборочно по команде. Да и датчики оружия пригодились бы. Ах, эти мечты-мечты…

Придя на службу, Иоганн первым делом поздоровался с дежурным, прослушал доклад о том, что ночью все прошло спокойно и поднялся к себе в кабинет.

– Доброе утро, шеф! Вам кофе принести?

– Я только пришел. Откуда ты знаешь, когда меня ждать? Меня это постоянно удивляет!

– Ха! Чего проще? Я попросила наших техников вывести мне датчик с видеокамеры на воротах. Как только в воротах появляется ваш автомобиль или камера фиксирует ваше лицо, мне сразу же приходит сигнал, что пора ставить кофе J Все просто!

– Софи, вы гений! Я всегда знал, что наша Академия воспитывает гениев!

– А если серьезно, шеф?

– А если серьезно, то берите чашку и расписание на сегодня. Что там у нас? Надеюсь, нет скучных совещаний ни о чем?

– Да нет. К вам просилась с утра Рита с какими-то молодыми людьми. Говорила, что у них очень интересный проект, а сами они никак не могут пробиться в департамент финансов для получения финансирования. Нужна ваша помощь.

– А ребята уже здесь?

– Да. Ждут вашего разрешения.

– Пригласите их в комнату для переговоров.

– Доброе утро, шеф!

– Доброе утро, Рита!

– Доброе утро, коллеги! Что вас привело ко мне?

– Мы разработали и хотим представить на выставке «Безопасность» модульные светодиодные уличные фонари, которые станут частью концепции «умного» города. Они не только могут оповещать об опасности, меняя цвет, а также раздавать Интернет, но и следить за прохожими и записывать их разговоры.

– Так! Где можно посмотреть образец?

– Пока только у нас в лаборатории. Мы еще не показывали его никому. Простите, у нас просто нет денег на производство, а попасть в департамент финансов нет связей.

– Рита, с этого дня эти молодые люди до окончания проекта становятся членами нашей спецлаборатории. А вы привезите нам опытный образец для тестирования. Учтите, с этого дня проект проходит под грифом «Секретно». Что еще может ваш фонарь?

Конец ознакомительного фрагмента.