персональные данные персональные данные персона № 6 (34), июнь 2011 данные
Информационно-аналитический журнал для операторов персональных данных

«Меры и средства защиты персональных данных»

Как мы спасали мир от Кибер-преступника

Журналистское расследование

Мир в опасности. Как, вы еще не в курсе? Война на копьях в привычном понимании уже давно сменила боевые орудия и перешагнула рубежи. КИБЕР-ВОЙНА... она вероломно захватила планету, включая даже страны, о которых мы, в принципе, и не слышали никогда. Все, кто имеет возможность пользоваться благами цивилизации, сотовыми телефонами, портативными и передающими устройствами, компьютерами, - втянуты в одну большую информационную борьбу. И цель ее - отнюдь не завоевание территории.

Спецслужбы не дремлют, но каждая ноу-хау разработка в области компьютерных технологий порождает новую волну кибер-атак. Побороть эту беду невозможно, но сузить рамки воздействия извне вполне реально, главное - закрепить эту мысль у себя в голове, потому что ни ФБР, ни Отдел «К», ни армии с пулеметами не спасут от глупостей, которые мы сами себе позволяем.

В качестве показательного примера мы предлагаем вам наше собственное расследование. А дело было, на первый взгляд, ерундовое. Второго июня этого года, на рассвете, некто разместил в соцсетях ссылку на торрентовский сайт и указал, что там можно скачать свежие базы данных ГИБДД и клиентов Билайна, что, само по себе, уже давно стало делом привычным в Сети.... Возможно, мы бы закрыли глаза и прошли мимо, но наше журналистское эго подсказывало, что «что-то здесь не так».

Мы перешли по ссылкам на странички, где были выложены якобы заявленные базы персональных данных. Конечно, первым делом возник совершенно человеческий вопрос - а не скачать ли и нам, вдруг там что-то интересное? Но совесть, разум и гражданская позиция внесли свои пять копеек и сказали твердое «нет». Нам понадобилось минут двадцать, чтобы понаблюдать за событиями на портале, когда появились первые реплики на форумах о том, что файлы с вирусами, при запуске требуют отослать СМС на непонятный номер, да и вообще на базы данных все это не похоже. Автор раздачи, очевидно, рассчитывая на наивность пользователей, тут же отписывал на форуме, что все отлично, внутри самые что ни на есть настоящие базы данных, какие просто так в полиции не найдешь. Выяснилось, что рассчитывал не зря: нашлось немало людей, которых ничего не смущало, а желание заиметь базы ГИБДД и Билайн просто зашкаливало.

Мы тут же попытались связаться с администраторами портала, но их безмолвие нас не смутило. Под видом обычных пользователей мы написали автору раздачи, на что он ответил сразу, ничего не скрывая, что база данных ГИБДД реальнее реальных, ее сделал его друг, который работает в ГИБДД (!)... Правильно, читатель, мы обратились в Управление. О том, как мы выходили на связь с сотрудниками спецслужб, можно было бы

написать отдельный материал, но мы приводим для вас краткий вариант нашей истории. Для того, чтобы обратиться в ГИБДД, необходимо заполнить определенное количество пунктов анкеты в он-лайн обращении. Других вариантов связи, кроме телефона начальника отдела организации межведомственного взаимодействия и пропаганды безопасности дорожного движения Департамента обеспечения безопасности дорожного движения МВД России, мы не нашли. Владимир Шевченко наш рассказ о выложенной на рутрекере базе ГИБДД воспринял с некоторым подозрением, сказал: «Разберемся» и бросил трубку. Или просто уронил. Такое тоже бывает.

Затем мы связались с представителями Билайна, и это тоже отдельная история, которая могла бы стать перлом на каких-нибудь Фишках. Но мы люди настойчивые, благо – сейчас много возможностей «подойти поближе» к источнику. Через социальные сети с нами связалась замечательная девушка Екатерина Турцева, менеджер по бренд-коммуникациям (PR) ОАО «ВымпелКом» («Билайн»), и пообещала держать в курсе событий. Мы снова и снова пытались связаться с ГИБДД, но трубку никто не брал, а писать письма через Почту России, сами понимаете, время не позволяло. Тогда мы обратились непосредственно в МВД, откуда нас перенаправили Отдел «К» ГУВД Москвы, где, опять же, посоветовали оформить сообщение через систему он-лайн заявок.

Рабочий день подходил к концу, а люди продолжали скачивать файлы. Лица, напрямую заинтересованные в истории, почему-то откровенно молчали и бездействовали. Оперативно отреагировал только Роскомнадзор, который тут же приступил к проверке информации. Отдельное спасибо хотим выразить коллегам-блогерам и специалистам по информационной безопасности из разных городов России, которые после публикации нашего сообщения в соцсетях вызвались проверить файлы. К концу дня мы уже знали, что данные базы на торренте не что иное, как вредоносная программа-вирус Hoax.Win32.ArchSMS.pic., похищающая конфиденциальную информацию пользователя, обрабатывающуюся в банковских системах, системах электронных платежей и пластиковых карт (MasterCard, MoneyMail, Yandex.Money, Liberty Reserve, WebMoney). Об этом мы написали на форуме, но глупость человека не имеет границ – люди продолжали скачивать файлы.

Прошел день. Компания Билайн признала факт наличия вредоносной программы в выложенном файле на портале, представитель сотового оператора сообщил, что юридический отдел готовит документы и готов судиться по данному факту, также к концу дня автор раздачи был забанен, а страница с логотипом Билайна – на третьи сутки закрыта. Что касается ГИБДД - мы так и не смогли связаться с Департаментом, банально никто не брал трубку. На проходящем 8 июня в Доме Правительства 7-м Евразийском форуме директор Департамента информационных технологий, связи и защиты информации МВД России Михаил Тюркин искренне удивился нашему рассказу о хакере и обещал «разобраться». После этого (или по стечению обстоятельств) страница с базой ГИБДД была также закрыта. Всего за почти неделю вредоносную программу скачало более ста пользователей (по сто на каждой странице). Администрация портала нам так и не ответила. Роскомнадзор отчитался о проверке и подтвердил информацию о наличии вирусов.

Вы скажете – таких историй полно? В данном случае нас интересовали два момента: оперативность соответствующих организаций и этический вопрос. Если бы в указанных файлах действительно находились базы персональных данных, история получила бы совсем другое развитие, ведь изначально люди клюнули именно на эти слова – «базы персональных данных». Когда же стало известно, что автор раздачи использует логотипы и названия лишь для привлечения внимания пользователей Интернета, организации в один голос ответили: «Но там же нет баз данных! Для чего нам суетиться? Это случай из миллиона таких же». Да, но если вредоносную программу украшает логотип вашей компании, - сможете ли вы спокойно на это реагировать?

Вопрос – чем грозит человеку, выложившему вирус, - остался без ответа. Потому что там не было настоящих баз. Проблема усугубляется и тем, что автор раздачи выступал под флагом республики Беларусь, а торрентовские файлы лежали на портале, зарегистрированном за пределами России.

По мнению руководителя Российского разведывательного агентства «Разведка в сфере бизнеса» (РСБ) Олега Криницына, спрос порождает предложение: «В условиях информационного вакуума и правовой импотенции бороться с поставщиками и дилерами баз данных, на мой взгляд,

сродни борьбе с ветряными мельницами. Как правило, ежеквартально на рынке появляется порядка 20-30 новых баз. В большинстве своем – это «выходцы из регионов». Дополнительно столько же появляется и «апгрейда». На красивой упаковке написано: «Базы данных пользователей такого-то сотового оператора за 2011 год». На самом деле, мы сталкиваемся со старой базой 2003 года, с измененной оболочкой и датами. Иногда «самоделкин», который готовит базу к продаже, добросовестно пытается исправить даты, фамилии... но, как правило, терпения у него не хватает, и мы видим несуразицу в датах и других идентифицирующих признаках. Вычислить производителей сложно - продажи осуществляются через дилерскую и субдилерскую сеть не только в Москве, но и в других городах и регионах, - но возможно. Но бывают и ситуации, когда вместо баз персональных данных вам предлагают комплект вирусов. Тогда почему бы не спросить у себя: а мне это нужно?».

Мы попытались спасти мир от хакера. Пусть таким банальным способом. Теперь у нас закрадываются сомнения: а так ли рьяно кидаются в бой непосредственно сотрудники обеспечения безопасности компаний и организаций, которым по роду службы положено это дело отслеживать? Кроме того, стоит отметить, что в нашей стране пока не очень развита культура приватности, что доказывается вышеописанным примером. Мы много говорим о защите персональных данных, сетуем, что наши пароли, ящики, сайты взламывают, персональные данные крадут и используют против нас. Вместе с тем мы сами даем себя обмануть: скачиваем ненужные, по большому счету, программы, файлы, архивы, выкладываем всю свою подноготную на общее обозрение в соцсетях и мечемся в поиске виновного, хотя источник опасности – в нас самих.

И в заключении. Все вышеописанное происходило без фанатизма с нашей стороны, но с одной лишь целью – увидеть результат. Всегда помните, что мошенники очень изобретательны, в их арсенале масса вкусных наживок под манящими обертками различных якобы баз персональных данных. Наша беспечность и желание подсмотреть в замочную скважину за соседом может сыграть плохую шутку: подсаживаясь на эти самые крючки, мы позволяем злоумышленникам не только «подарить» нам вредоносную программу, но и похитить персональные данные у нас самих.

Делитесь своими историями с читателями журнала, задавайте вопросы редакции и не поддавайтесь на провокации.

P.S. 9 июня этого года на сайте Роскомнадзора появилась информация о том, что Роскомнадзор, Прокуратура г. Москвы и ГУВД по г. Москве активизируют взаимодействие с целью пресечения нарушений законодательства о персональных данных путем распространения незаконных баз данных в местах розничной торговли.

Так, 8 июня 2011 года Роскомнадзор и ГУВД по г. Москве провели совместный рейд в ТК «Горбушкин двор». По результатам проведенных мероприятий выявлена схема незаконной реализации физических носителей баз данных и установлен факт продажи неустановленным лицом базы данных, предположительно содержащих сведения из ЗИЦ ГУВД по г. Москве по состоянию на 2009 г. В настоящее время ГУВД по г. Москве проводятся мероприятия по выявлению и задержанию лиц, осуществляющих незаконную реализацию баз данных на территории ТК «Горбушкин двор». Ранее, 1 марта 2011 года, ГУВД по г. Москве совместно с Роскомнадзором был проведен совместный рейд в ТК «Савеловский».

Кроме того, Прокуратура г. Москвы сообщила Роскомнадзору об инициировании сбора от районных прокуроров информации, касающейся состояния законности и прокурорского надзора в сфере исполнения законодательства о персональных данных в деятельности Царицынского, Савеловского, Митинского рынков и ТК «Горбушкин двор».

В настоящий момент ведется работа по организации совместного совещания Управления Роскомнадзора по Москве и Московской области и Прокуратуры г. Москвы для выработки форм и методов взаимодействия с целью пресечения незаконной деятельности по продаже баз данных, содержащих персональные данные граждан.

Материал подготовила Инга Чернышева,
журнал «Персональные данные»