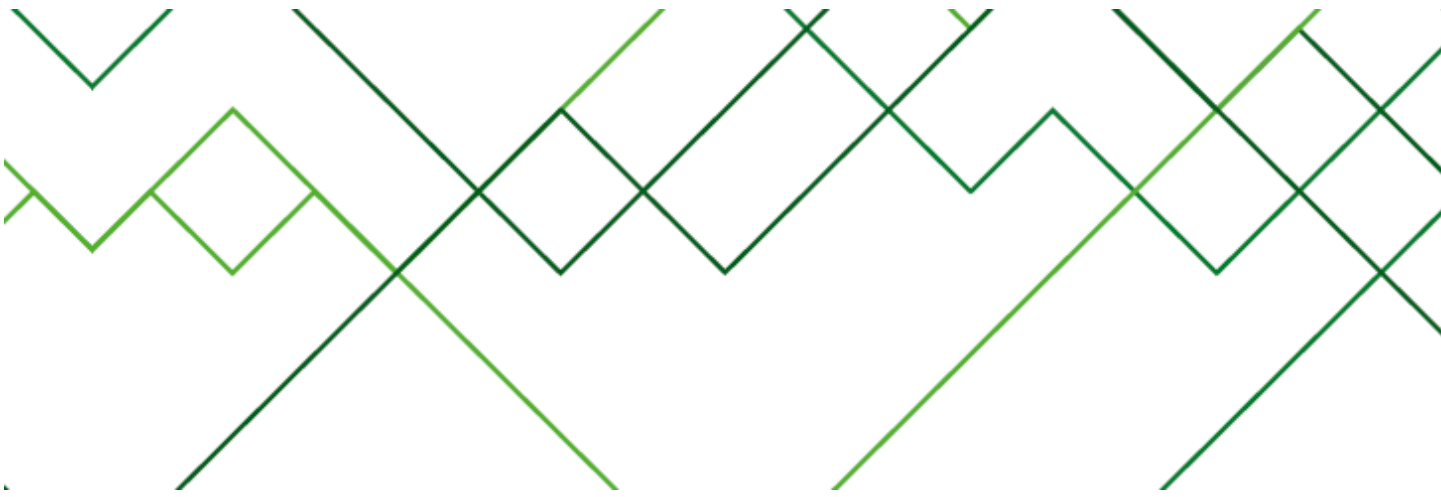
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический Центр InfoWatch
www.infowatch.ru/analytics

Глобальное исследование утечек данных о пластиковых картах в 2012 году



Оглавление

Аннотация

Количество эмитированных пластиковых карт превышает число жителей Земли. Только в России, по данным Центробанка по состоянию на январь 2013 года, выпущено 240 млн банковских карт[1]. Однако с точки зрения безопасности, «пластик» далек от совершенства.

Идентификация владельца карты проводится по подписи либо по ПИН-коду. При безналичной оплате продавцы редко сверяют имя, фамилию и подпись владельца на карте с данными в документе, удостоверяющем личность. Для оплаты в интернете сама карта вообще не нужна – достаточно платежных данных[2].

Эти данные - реквизиты карты, позволяющие осуществлять электронные платежи, - являются одним из наиболее «ликвидных» товаров на внутреннем рынке киберпреступности. По данным исследования McAfee[3], одна запись о кредитной карте может стоить от 15 до 200 долларов США (в зависимости от типа карты, наличия сведений о ПИН-коде и балансе карты)[4].

Злоумышленники всего мира атакуют организации, оперирующие платежными данными[5] - банки, розничные магазины, процессинговые компании, - стремясь заполучить как можно больше записей с данными пластиковых карт. Эти записи легко продать. Имея в распоряжении платежные данные, можно купить товары в интернете, изготовить поддельные карты и обналичить деньги через «дропперов»[6], вывести денежные средства со счетов владельцев карт на собственные счета.

Платежные данные сравнительно легко раздобыть. Самый простой случай – официант в кафе фотографирует карту клиента в момент оплаты. Случай сложнее – направленная атака на операторов по переводу денежных средств с целью взлома информационной системы.

Внешние атаки широко освещаются в СМИ, каждый факт получает широкую огласку. Однако на практике причиной утечки[7] платежных данных чаще является не внешняя

---

[1] Количество банковских карт, эмитированных кредитными организациями, по типам карт ЦБ РФ.

[2] Под платежными данными в этом исследовании мы понимаем реквизиты карты: номер и срок действия, фамилию и имя владельца, код CVC, - то есть информацию, достаточную для осуществления электронного платежа.

[3] Cybercrime Exposed. Cybercrime-as-a-Service.

[4] По данным Ponemon Institute, в 2012 году ущерб компаний от потери одной записи о пластиковых картах составил (в зависимости от страны) в среднем 136 долл. США, при этом самими «дорогими» оказались утечки в немецких компаниях - 199 долл. США. - Ponemon Institute. 2013 Cost of Data Breach Study: Global Analysis.

[5] В терминах российского закона «О платежной системе» - операторы по переводу денежных средств. В данном исследовании мы выделяем три типа организаций, оперирующих денежными средствами – банки (эмитируют карты, осуществляют эквайринг карт в местах продаж товаров и в интернете), процессинговые компании (осуществляют информационное и технологическое взаимодействие между участниками расчётов), «ритейлеры» (продавцы товаров и услуг, принимающие в оплату пластиковые карты).

[6] Лица, осуществляющие снятие наличности по поддельным картам за определенный процент от снятой суммы.

[7] Утечка конфиденциальной информации (здесь – платежных данных) – инцидент информационной безопасности, действие или бездействие лица, имеющего легитимный доступ к конфиденциальной

атака, а действия сотрудников оператора по переводу денежных средств – хищение информации и последующее использование в собственных интересах.

> *infpol.ru: Сотрудник коммерческого банка республики Бурятии в течение нескольких лет использовал данные клиентов для кражи денежных средств. В силу своего служебного положения он имел доступ к личной информации вкладчиков. В общей сложности мошенник украл более 3 млн руб. Почерковедческая экспертиза подтвердила, что служащий банка подделывал подписи клиентов на платежных поручениях.*

В ряде случаев имеют место банальные ошибки - платежные и персональные данные клиентов оказываются скомпрометированными из-за невнимательности сотрудников ИБ-департамента, легитимных пользователей баз данных, веб-мастеров.

Самое неприятное, что от утечки платежных данных не застрахованы даже крупнейшие банки. В 2012 году в сообщениях СМИ о мошенничестве с пластиковыми картами и счетами клиентов фигурировали Bank of Montreal, Wachovia Bank, Credit Suisse, Barclays, Bank of America, Citibank, HSBC, JPMorgan Chase & Co, РайффайзенБанк.

Исследование утечек платежных данных проводится Аналитическим Центром InfoWatch впервые. Цель данного исследования – очертить масштаб проблемы, обратить внимание специалистов по информационной безопасности и владельцев бизнеса на особенности такого явления, как утечка платежных данных.

Методология

Исследование Аналитического Центра InfoWatch основывается на собственной базе данных, которая пополняется специалистами Центра с 2004 года. В базу InfoWatch включаются утечки данных, которые произошли в результате злонамеренных или неосторожных действий сотрудников и были обнародованы в СМИ или других открытых источниках (включая web-форумы и блоги). В настоящее время база утечек InfoWatch насчитывает несколько тысяч зарегистрированных инцидентов.

В исследованиях InfoWatch мы обычно не рассматриваем случаи нарушения конфиденциальности информации, произошедшие в результате внешних компьютерных атак, а равно иные инциденты ИБ (DDoS, фишинг, несанкционированный доступ к информации, саботаж сотрудников и пр.). Нас в большей степени интересуют преднамеренные или случайные действия сотрудников банков, процессинговых компаний или «ритейлеров», повлекшие утрату контроля над платежной информацией – утечки в классическом понимании, которые, в отличие от направленных атак, можно предотвратить с помощью тиражных решений (программных и/или аппаратных) и организационных мер. Однако в настоящем исследовании примеры внешних атаках приводятся, хотя и носят, скорее, справочный характер.

информации, которое повлекло потерю контроля над информацией или нарушение конфиденциальности этой информации.

Особенности классификации предмета исследования (сообщений в СМИ об утечках платежных данных) не позволяют прямо сопоставить собственно утечки платежных данных (реквизиты карт) и случаи манипулирования информацией о счетах клиентов (фрод) – эти данные также даются как справочный материал и не влияют на выводы исследования.

Авторы признают, что исследуемая выборка случаев утечек, обнародованных в СМИ, составляет незначительную (не более 1-5%) долю от реального количества утечек платежных данных, произошедших в мире. Однако данное исследование ориентировано на выявление наиболее общих трендов, что не предполагает повышенных требований к полноте выборки. Имеющееся в распоряжении авторов число зарегистрированных типичных утечек мы считаем достаточным, чтобы сделать выводы, валидные для генеральной совокупности.[8]

Основные тренды

В своем исследовании Аналитический Центр InfoWatch впервые попытался проанализировать ситуацию с утечкой данных о банковских счетах и пластиковых картах (платежных данных) на основании информации из открытых источников. Выявлен ряд закономерностей:

- ✓ Небольшие компании, массово принимающие к оплате пластиковые карты (игровые сервисы, крупные оффлайн ритейлеры), становятся излюбленной мишенью киберпреступников. У таких компаний в достатке имеются платежные данные, а уровень информационной безопасности ниже, чем, например, в банках.
- ✓ Наибольшая опасность заключается в том, что не все компании, оперирующие платежными данными, понимают их ценность. Если банки и процессинговые компании действительно уделяют повышенное внимание защите такой информации, то большинство «ритейлеров» фактически закрывает глаза на слабость собственных систем защиты платежных данных клиентов, не выполняя даже минимальные требования регулятора и допуская хранение и обработку платежных данных в своей информационной системе.
- ✓ Более защищенные банки также проявляют себя не с лучшей стороны. Высокий процент умышленных утечек через давно известные и теоретически контролируемые каналы говорит о том, что банки излишне полагаются на технические средства защиты и уделяют меньше внимания, чем необходимо, мерам организационного характера, работе с психологией сотрудников.
- ✓ С другой стороны, доля случайных утечек платежных данных в банках и процессинговых компаниях невысока. Очевидно, что службы информационной и экономической безопасности в банковской сфере научились справляться с ошибками персонала с помощью технических средств защиты и контроля за перемещением данных.

[8] Для выявленных (1-5%) и оставшихся неизвестными случаев утечки платежных данных.

Результаты исследования

Ключевой вывод №1. Более трети утечек в коммерческих компаниях[9] приходится на платежные данные

Фишинг страниц интернет-магазинов, установка спецоборудования (скиммеров) в банкоматах и на входных дверях банков, перехват данных с ПК пользователя с помощью вирусного ПО, социнжиниринг – вот далеко не полный арсенал злоумышленников, стремящихся завладеть платежными данными.

Настоящее исследование показывает, что в 2012 году на долю утечек платежных данных приходится 34% от всех случаев утечки конфиденциальной информации (Рисунок 1), зафиксированных в коммерческих компаниях.

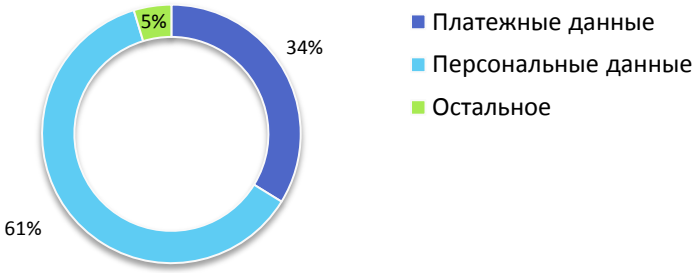


Рисунок 1. Типы утекающих данных, 2012 г.[10]

Причем число утечек платежных данных из банковских систем вследствие направленных атак (с использованием специального вредоносного ПО - Carberp, BIFIT_A, RanBuys) оказалось незначительным на фоне более многочисленных, хотя и не столь эффектных примеров мошенничества с платежными данными[11].

> *e-moneynews.ru: В Перми завершено и передано в суд уголовное дело в отношении организованной преступной группы. Один из участников преступной группы, являясь студентом, устроился на практику в один из банков, где получил конфиденциальную информацию – номера карт, персональные данные их держателей, а также коды CVV, необходимые для совершения операций. Второй участник группы, используя данную информацию, приобретал в интернет-магазинах дорогостоящую электронную технику. С банковских карт граждан списывались крупные суммы от 90 тыс. до 600 тыс. рублей с использованием виртуальной платежной системы. Третий участник от имени покупателя созванивался с почтовой службой доставки, получал заказанный товар и продавал его.*

---

[9] В данном исследовании термины «коммерческие компании» и «операторы по переводу денежных средств» употребляются как взаимозаменяемые. Из выборки были исключены коммерческие компании, не оперирующие пластиковыми картами.

[10] В категорию «Платежные данные» не включены утечки номеров социального страхования (SSN), которые в США используются в мошеннических схемах (возврат налоговых выплат) но не являются в явном виде данными, которых достаточно для перевода денежных средств.

[11] На долю злонамеренных атак с использованием вредоносного ПО приходится лишь 37% случаев утечки платежных данных - Ponemon Institute. 2013 Cost of Data Breach Study: Global Analysis.

Легкость, с которой студенты похищали деньги клиентов банка, наглядно показывает, насколько слабы системы обеспечения безопасности платежных данных даже в банковской отрасли.

> *По сведениям компании Group-IB, мошенничество с использованием платежных данных только в России приносит киберпреступникам 446 млн долл.[12] или чуть менее 25% от всех доходов злоумышленников. С другой стороны, «…специалисты Group-IB вынуждены констатировать, что обеспечение безопасности в системах ДБО и других интерактивных сервисах коммерческих банков очень часто находится на невысоком уровне и может представлять значительную угрозу самим банкам. Ситуация усугубляется также тем, что банки часто пытаются скрывать факты компрометации их ресурсов и утечки данных, что затрудняет сбор общей статистики инцидентов».[13]*

Стоит ли говорить, что у «ритейлеров» - компаний, принимающих в оплату пластиковые карты, - дела с безопасностью обстоят еще хуже?

Ключевой вывод №2. Картина утечек платежных данных неоднородна

В нарушение всех требований и предписаний регуляторов, многие «ритейлеры» не только аккумулируют платежную информацию клиентов, но и хранят ее в одной базе с персональными данными. Нередко заявленная в СМИ утечка кредитных карт на деле означает потерю базы со всеми персональными данными клиента, историей его взаимоотношений с банком или онлайн-магазином.

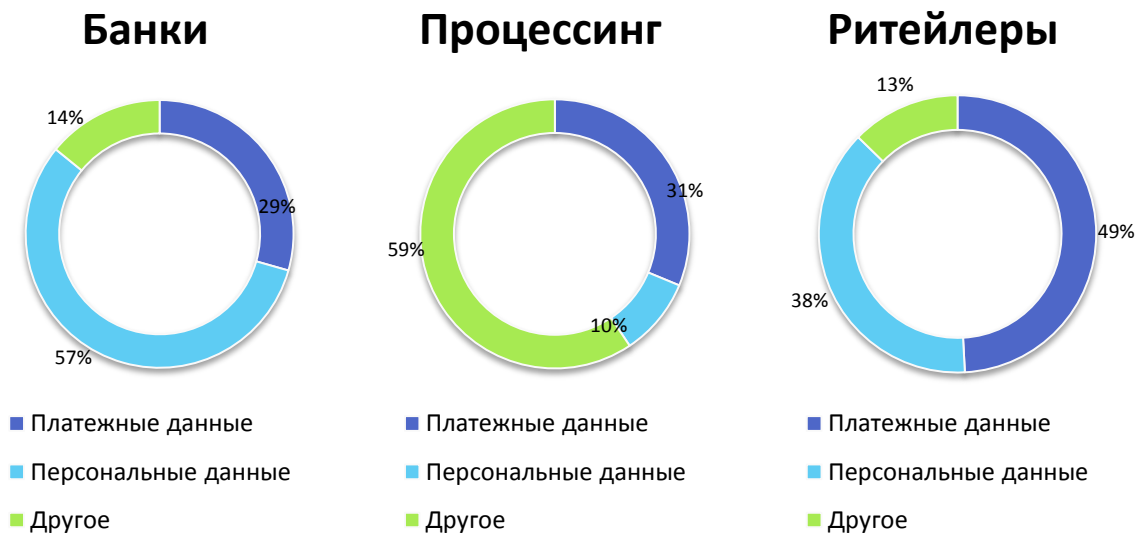


Рисунок 2. Утечки из коммерческих компаний. Типы данных. 2012 г.

Наше исследование показывает, что доля утечек платежных данных от всех утечек разнится в зависимости от типа организации. Так в банках с утечкой платежных данных связано немногим меньше трети всех утечек - (29% см. Рисунок 2). Чуть

[12] Group-IB Total intelligence report 2012-2013.
[13] Group-IB Total intelligence report 2012-2013.

большая доля утечек (31%) приходится на платежные данные в процессинговых компаниях, и почти половина утечек (49%) связана с потерей платежных данных у «ритейлеров».

«Ритейлеры» давно превратились в излюбленную мишень киберпреступников. Последние легко получают доступ к агрегированной информации о клиентах, включая персональные и платежные данные. «Ритейлеры» в большинстве случаев просто не воспринимают всерьез возможные последствия утечек в виде репутационных и финансовых потерь, не предпринимают усилий для повышения уровня защищенности данных клиентов.

> *Агентство Verizon зафиксировало в 2011 году 855 случаев раскрытия персональных данных в результате взлома, хакерских атак, действий инсайдеров. Причем кибермошенники нацеливались в основном на мелкие компании, где с успехом получали доступ к платежным данным и иной информации о клиентах. В отчете Verizon подчеркивается, что практически все компании, ставшие жертвами утечки, не смогли впоследствии пройти проверку на соответствие требованиям стандарту PCI DSS.*[14]

Большинство утечек связано с незаконной деятельностью внутренних нарушителей – то есть самих сотрудников пострадавших компаний.

> *news29.ru: Архангельские студенты похищали деньги с чужих карт, расплачиваясь ими в интернете. В июне 2012 года двое студентов и безработный, используя персональные данные и другую информацию о законных держателях банковских карт, похитили более 100 тысяч рублей со счетов клиентов одного из архангельских банков. Один из аферистов работал в свое время охранником в банке, где получил доступ к конфиденциальной информации. В другом случае мошенник добыл необходимые сведения, когда трудился официантом в ресторане.*

Нередки случаи, когда утечки платежных данных происходят по вине процессинговых компаний, чьи сотрудники тайком от партнеров организуют «теневой» мошеннический бизнес.

> *securitylab.ru: Новозеландский ASB Bank обвинил платежную систему POLi Payments в незаконном дублировании своих сайтов и принуждении пользователей вводить на поддельных ресурсах банковские реквизиты, таким образом, компрометируя их конфиденциальную информацию.*

Несмотря на то, что стандарт PCI DSS прямо запрещает хранить критичные аутентификационные данные после авторизации (полное содержимое дорожки, CVC, ПИН), некоторые процессинговые компании и «ритейлеры» агрегируют эту информацию[15].

> *Известия: Крупнейший портал по бронированию отелей разглашает данные кредитных карт. Пользователь Facebook Роман Мамонов выложил на своей страничке скан факса, который получил его приятель от турецкого отеля*

[14] 2012 Data BREACH Investigations Report.
[15] См. Стандарт безопасности данных индустрии платежных карт (PCI DSS).

The Marions Suite. Том запросил от отеля подтверждение брони, совершенной через популярный сервис booking.com. В полученном письме содержались все данные банковской карты клиента: номер и срок действия, CVC-код.

Ключевой вывод №3. Утечки платежных данных носят, в основном, злонамеренный характер

Специалисты Аналитического центра InfoWatch разделяют утечки на умышленные и неумышленные[16]. В настоящем исследовании распределение по умыслу получилось очень интересным (см. Рисунок 3).

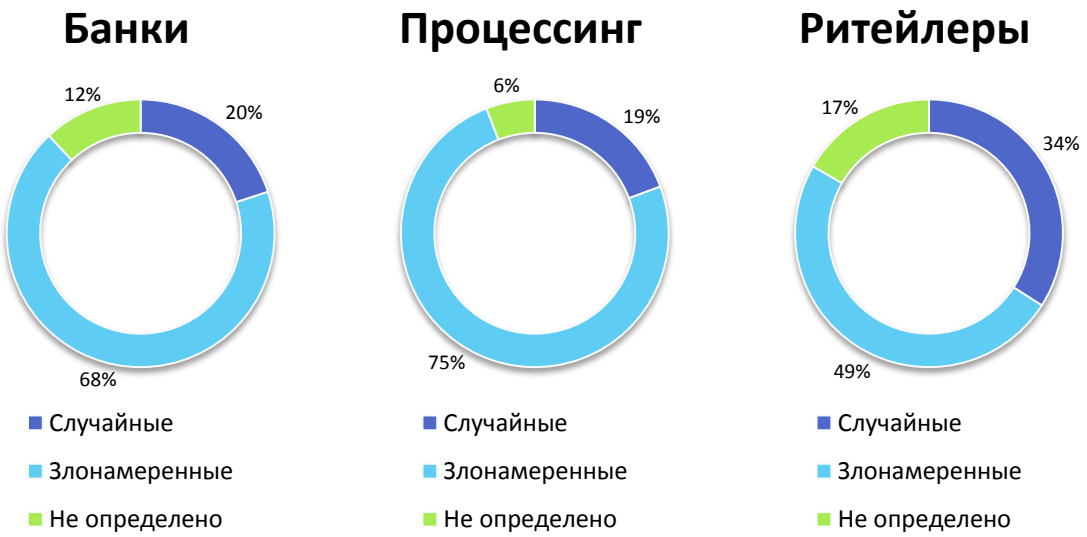


Рисунок 3. Распределение утечек по умыслу, 2012 г.

Если для глобальной картины утечек считается нормальным[17] распределение умышленных и неумышленных утечек в отношении 50/50, то для утечек платежных данных из коммерческих компаний (выборка настоящего исследования) характерно преобладание злонамеренных утечек. Особенно ярко это проявляется в отношении процессинговых компаний (75% злонамеренных), где доля случайных утечек

[16] Умышленные (злонамеренные) утечки – к таковым относятся случаи утечки информации, когда пользователь, работающий с информацией, знал или предполагал возможные негативные последствия своих действий, был предупрежден об ответственности, однако, в нарушение установленных правил работы с информацией, он совершил поступок, повлекший утрату контроля над информацией и нарушение конфиденциальности информации. При этом неважно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя.

Неумышленные (случайные) утечки – к таковым относятся случаи утечки информации, когда пользователь не знал и не предполагал наступления возможных негативных последствий, не был предупрежден об ответственности. При этом неважно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя.

[17] Аналитический Центр InfoWatch год от года регистрирует примерно равное соотношение умышленных и неумышленных утечек. Колебания за весь период наблюдений (с 2004 года) незначительны.

совсем небольшая (19%). Аналогично в банковских организациях – 68% умышленных против 20% случайных.

Ситуация с низким процентом случайных утечек в банках легко объяснима. Небольшая доля случайных утечек вообще характерна для сегментов с высоким уровнем развития информационной безопасности. Требования регуляторов, с одной стороны, и понимание важности защиты данных клиента, с другой - обусловливают постоянное совершенствование систем защиты. Неудивительно поэтому, что практически в каждом сообщении СМИ об утечке платежных данных из банков фигурирует и сам злоумышленник, и способ совершения преступления - современные системы защиты информации (класс DLP и им подобных) позволяют провести тщательное расследование инцидента.

> *WINSTON-SALEM: Кассир банка SunTrust подделала банковские документы и подпись клиента, благодаря чему смогла снять с чужого счета 11 тыс. долларов США. Девушке грозит до двух лет лишения свободы. Ей также придется возместить ущерб, причиненный клиентам банка.*

Причем способ мошенничества, как правило, прост и незатейлив, как в примере выше. Даже под угрозой сурового наказания персонал банков решается на противоправные деяния. Виной тому - легкость, с которой кассиры, операционисты, прочие рядовые специалисты получают доступ к платежным данным клиентов банков. Впрочем, бывают и более изобретательные мошенники.

> *www.tampabay.com: Сотрудница Bank of America воспользовалась персданными клиентов, «заработав» 180 тыс. долл. 36-летняя Люсиана Альварадо призналась в краже 180 тыс. долл. с клиентских счетов банка. Как сотрудник отдела претензий, она имела доступ к личной информации клиентов, чем и смогла воспользоваться. Путем подмены данных об адресах клиентов, кредитной информации, ей за несколько лет удалось перевести чуть менее 200 тыс. долл. с клиентских аккаунтов на личные счета. После увольнения из банка, Люсиана продолжала «трудиться» на ниве мошеннических электронных переводов, используя логины и пароли, оставшиеся у нее со времени работы в банке. Интересно, что аферистка творчески подходила к выбору жертв и «облегчала» электронные счета тех клиентов, чьи имена и фамилии были схожи по звучанию с ее собственными.*

Ключевой вывод №4. Кража оборудования – основная причина утечек платежных данных[18]

Распределение утечек платежной информации серьезно варьируется в зависимости от типа организации. Для банков, где, как мы уже показали, доля случайных утечек незначительна, в распределении преобладают характерные для умышленных утечек каналы: потеря или кража оборудования (в том числе ноутбуков) – 42%, утечки по сети - 21% и через съемные носители - 6%. Высок уровень утечек, где канал определить невозможно (одна пятая от общего количества).

[18] Канал утечки – сложный сценарий (действия пользователя корпоративной информационной системы, направленные на оборудование или программные сервисы), в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. На данный момент мы различаем 8 самостоятельных каналов утечки. См. Глоссарий

С незначительными изменениями картина повторяется применительно к процессинговым компаниям. Пожалуй, существенным нюансом можно назвать немного меньшую долю утечек, пришедшихся на кражу и потерю оборудования - 34%.

Преобладание умышленных утечек, характерное для финорганизаций, проявляется и применительно к «ритейлерам» (см. Рисунок 3). Однако у «ритейлеров» внушительная доля утечек относится к случайным. Как результат - распределение по каналам утечки платежных данных у «ритейлеров» более однородное – «течет» практически отовсюду.

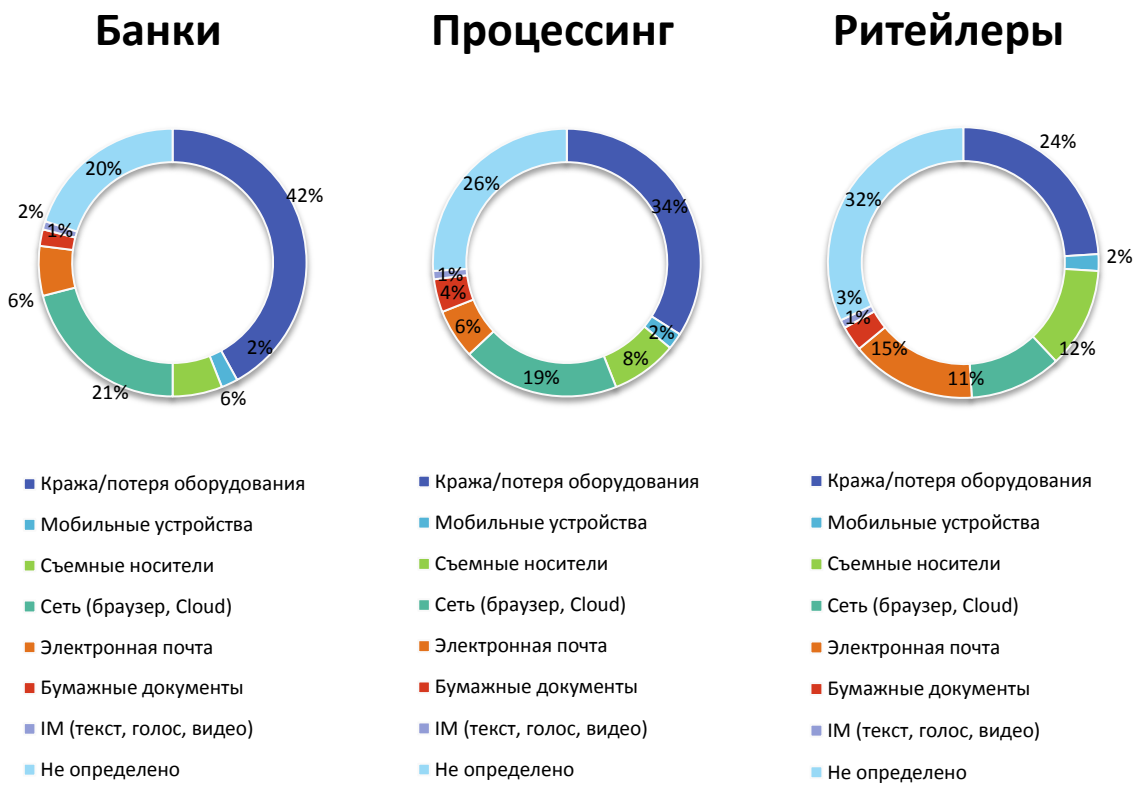


Рисунок 4. Распределение утечек по каналам, 2012 г.

Интересен пример, когда американец получил доступ к платежным данным, позволяющим украсть у держателей карт более 4 млн долл. Данные он добывал не в относительно «благополучных» (с точки зрения информационной безопасности) США, а в Мексике.

> *The Monitor: Житель города МакАллан (Техас, США) приговорен к пяти годам тюремного заключения за мошенничество с кредитными картами. Сообщается, что он намеревался похитить более 4 млн долл. Используя украденные данные о кредитных картах и банковских счетах, Марио Вонг покупал в интернете дорогую технику и продавал ее в Мексике. Данные о картах он получал от своего сообщника. При обыске в его квартире нашли флэшки с украденными данными о банковских счетах, устройства для считывания и перекодирования пластиковых карт и сами карты.*

Незащищенность «ритейлеров» порождает к ним понятного рода интерес злоумышленников. Очевидно, интернет-магазин, турагенство или иной онлайн-сервис, агрегирующий платежные данные клиентов, защищен хуже среднего банка.

В информационной системе «ритейлера» могут храниться десятки и сотни тысяч записей о клиентах, данные об их пластиковых картах. Неудивительно, что в последние несколько лет именно «ритейлеры» все чаще оказываются «под прицелом» злоумышленников.

Заключение

Низкий уровень защищенности пластиковых карт – обратная сторона преимуществ этого платежного инструмента. Идея «пластика» заключалась в том, чтобы осуществлять платежи практически мгновенно, в любом магазине, на любом интернет-сайте. Однако, выбирая между безопасностью и удобством клиента, регуляторы и компании, оперирующие пластиковыми картами, выбрали, к сожалению, удобство.

Сегодня никого не удивляет ситуация, когда банки присылают готовые к активации пластиковые карты обычной почтой. Пользователи расплачиваются кредитками в ресторанах и кафе, снимают наличность в банкоматах, совершают покупки в интернете.

Злоумышленникам нужно приложить минимум усилий, чтобы перехватить данные карты – сфотографировать сам пластик при оплате, установить скиммер на банкомат или перенаправить покупателя на фишинговый сайт.

Однако частные случаи воровства платежных данных – скорее экзотика. Киберпреступники массово похищают номера карт и платежные данные пользователей в промышленных объемах – более трети всех утечек из коммерческих компаний связаны с потерей контроля над платежными данными.

Повышенный интерес злоумышленников к «ритейлерам», агрегирующим платежные и персональные данные клиентов, можно объяснить низким уровнем информационной безопасности платежных данных в этих компаниях. Интернет-сайты, игровые порталы, различные онлайн-сервисы, турагентства и пр. защищены слабо и не хотят что-то менять в этом отношении.

Теоретически в этом ряду могли бы оказаться процессинговые компании, и единичные случаи взлома баз данных этих компаний известны. Но статистика говорит, что процессинг пока остается вне внимания киберпреступников.

Уровень защищенности платежных данных в целом довольно низок по всему миру. Это грозит серьезными последствиями вплоть до подрыва доверия к системе платежных карт со стороны клиентов.

Для высокой доли утечек платежных данных есть и объективная причина - в подавляющем числе случаев утечки такой информации происходят при непосредственном участии сотрудников пострадавших компаний, а с внутренним нарушителем бороться всегда сложнее.

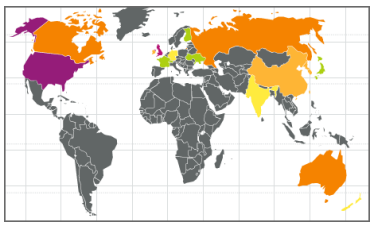
Исследование показывает, что ущерб от мошенничества с платежными данными можно снизить. Для этого необходимо, во-первых, ужесточить требования к порядку обработки и хранения платежных данных как на глобальном уровне, так и на уровне отдельных стран. Строгое выполнение участниками рынка (в особенности «ритейлерами») правила PCI DSS, предписывающего не хранить платежные данные в информационных системах, способствовало бы кардинальному изменению ситуации в лучшую сторону.

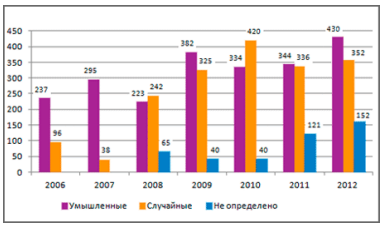
Во-вторых, операторам по переводу денежных средств пора всерьез задуматься о том, как противодействовать внутреннему нарушителю. Средства DLP могут с легкостью блокировать утечку номеров кредитных карт по маске, контролировать действия потенциальных нарушителей. Однако платежные данные утекают, средства DLP те же «ритейлеры» не используют. Такую ситуацию нельзя признать нормальной.

Мониторинг утечек на сайте InfoWatch

На сайте Аналитического Центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Кроме того на сайте представлены статистические данные по утечкам информации за прошедшие годы, оформленные в виде динамических графиков.





Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Twitter
- RSS

Аналитический Центр InfoWatch

www.infowatch.ru/analytics

Глоссарий

Платежные данные - *реквизиты карты: номер и срок действия, фамилию и имя владельца, код CVC. То есть информация, достаточная для осуществления электронного платежа.*

Утечка конфиденциальной информации *– инцидент информационной безопасности. Под утечкой мы понимаем такое действие или бездействие лица, имеющего легитимный доступ к конфиденциальной информации, повлекшее потерю контроля над информацией или нарушение конфиденциальности этой информации.*

Конфиденциальная информация *– (здесь) информация, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. В данном отчете в категорию КИ мы включаем информацию, подпадающую под определение государственной, коммерческой, иных видов тайн.*

Умышленные утечки *– к таковым относятся случаи утечки информации, когда пользователь, работающий с информацией, знал или предполагал возможные негативные последствия своих действий, был предупрежден об ответственности, однако, в нарушение установленных правил работы с информацией, он совершил поступок, повлекший утрату контроля над информацией и нарушение конфиденциальности информации. При этом неважно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя.*

Неумышленные утечки *– к таковым относятся случаи утечки информации, когда пользователь не знал и не предполагал наступления возможных негативных последствий, не был предупрежден об ответственности. При этом неважно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя.*

Канал утечки *– сложный сценарий (действия пользователя корпоративной информационной системы, направленные на оборудование или программные сервисы), в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. На данный момент мы различаем 8 самостоятельных каналов утечки:*

- ✓ *Кража/потеря оборудования (сервер, СХД, ноутбук, ПК), – компрометация информации в ходе обслуживания оборудования. Нелегитимное использование оборудования не предполагается.*
- ✓ *Мобильные устройства – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства.*
- ✓ *Съемные носители – потеря/кража съемных носителей.*
- ✓ *Сеть – утечка через браузер (отправка данных в личную почту, формы ввода в браузере), нелегитимное использование FTP, облачных сервисов.*
- ✓ *Электронная почта – утечка данных через корпоративную электронную почту.*

- ✓ *Бумажные документы – утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации).*
- ✓ *IM – мессенджеры, сервисы мгновенных сообщений (утечка информации при передаче голосом, текстом, видео при использовании сервисов мгновенных сообщений).*
- ✓ *Не определено - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки».*

Источники

1. Cybercrime Exposed. Cybercrime-as-a-Service. http://www.mcafee.com/de/resources/white-papers/wp-cybercrime-exposed.pdf
2. Group IB Total intelligence report 2012-2013 http://report2013.group-ib.ru/
3. Ponemon Institute. 2013 Cost of Data Breach Study: Global Analysis. https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf
4. Verizon 2012 Data BREACH Investigations Report http://www.verizon.com/enterprise/2012dbir/us
5. Количество банковских карт, эмитированных кредитными организациями, по типам карт. http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet007.htm
6. Стандарт безопасности данных индустрии платежных карт /PCI DSS 2.0 https://www.pcisecuritystandards.org/security_standards/pcidss_agreement.php?association=pcidss