телеком

Кредитка на крючке

интернет и банкинг

Кража денег с банковских карт захлестнула Россию. Мошенники, ранее облегчавшие кошельки жителей развитых стран, занялись обработкой россиян. «Ъ-Телеком» выяснил, что сейчас в интернете есть несколько русскоязычных сайтов, беспрепятственно торгующих данными чужих карт. Эксперты отмечают, что привлечь к ответственности мошенников практически нереально и держателям карт остается рассчитывать только на свою осмотрительность.

В конце сентября российские пользователи электронной почты получили небольшое письмо с адреса ibank@alfa-bank.ru. В сообщении говорилось, что «в целях обеспечения безопасности денежных средств вашей организации» необходимо получить некий «электронный ключ». Для этого пользователям предлагалось перейти по расположенной ниже ссылке, ведущей якобы на сайт уважаемой организации (банка, платежной системы и т. д.). В реальности пользователь попадает на сайт-клон, очень похожий на настоящий ресурс. Мошенники используют разнообразные предлоги, чтобы заманить человека на поддельный сайт: пишут о некой внезапно возникшей проблеме или же о свалившемся с небес выигрыше. Устоять довольно сложно, так как в обратном адресе письма всегда значится компания, которой пользователь доверяет. Этот e-mail может даже реально существовать — в интернете есть множество почтовых серверов, позволяющих рассылать письма с любых обратных адресов. А значит, любой более или менее грамотный пользователь ПК может поставить в графе «отправитель» любой адрес. Хоть bill.gates@microsoft.com.

Когда пользователь попадает на фальшивую страницу, то далее возможны два сценария. Он либо вводит свои приватные данные в поддельную форму, либо заражается вирусом, который встроен в данный сайт.

Купив поддельную карту всего за $100, можно снять в банкомате в среднем $2 тыс. ФОТО AP

Черные банкиры

Проблема фишинга, как ни странно, вытекает из технологий. Очевидно, если бы не развивался интернет-банкинг и различные платежные системы, то внимания к фишингу было бы гораздо меньше. Здесь возникает классическое противоречие между удобством пользователя и рисками, которые при этом возникают. Именно поэтому нельзя рассуждать о том, что для защиты от фишинга достаточно просто не отправлять приватные данные в интернете. Люди все равно будут это делать, поскольку хотят пользоваться онлайновыми системами. Проходя легальную авторизацию на настоящем сайте, человек оставляет информацию о себе, ее хватает для идентификации данного человека банком. Точно так же он может оставить аналогичные сведения и на сайте мошенников. А значит, мошенникам будет достаточно сведений для идентификации тем же самым банком.

Разумеется, под угрозой кражи находятся не только сведения систем интернет-банкинга, но и обычная информация о банковской карте. Чтобы сделать покупку в интернет-магазине, достаточно знать номер карты, имя ее владельца, срок действия карты и так называемый CVV-код (последние три или четыре цифры, написанные на обратной стороне карты). Чтобы получить эту информацию, мошенники используют не только фишинг, но и целый ряд других способов. Очень часто «кредитная» информация крадется из баз данных компаний, обрабатывающих трансакции банковских карт. Примерами таких компаний могут быть банки, крупнейшие розничные сети или государственные организации.

Для кражи «кредитных» данных мошенники подкупают сотрудников этих компаний, используют различные вредоносные программы (вирусы) или ищут их на украденных носителях (например, ноутбуках). Мировые масштабы проблемы действительно впечатляют. В качестве типичного примера можно привести американскую компанию TJX, которая потеряла 45 млн «кредитных» записей в декабре прошлого года. Хотя утечка произошла в США, от нее пострадали граждане во всех уголках планеты — Японии, Китае, Европе и России. Дело в том, что процессинговый центр TJX был одним из самых крупных в мире по обработке трансакций по картам Visa и MasterCard, поэтому в него стекались данные со всего света.

Спустя три месяца после утечки украденные сведения попали на черный рынок в интернет. А еще через три месяца стали появляться первые случаи снятия денег со скомпрометированных счетов через поддельные карты в банкоматах Китая и стран СНГ. По самым консервативным оценкам, мошенники смогли заработать несколько сотен тысяч долларов на этой утечке.

Описанный выше сценарий довольно типичен. Профессиональные мошенники редко занимаются «обналичкой», предпочитая продавать записи кардерам — преступникам, занимающимся изготовлением поддельных карт. Сегодня в сети существует огромное количество сайтов, предлагающих «кредитную» информацию по довольно низким ценам. В среднем в России можно купить десять кредитных записей всего за $3,5 с возможностью расплатиться через платежную систему WebMoney.

Отметим, что кардеры иногда продают поддельные карты на черном рынке, предлагая своим клиентам самостоятельно их обналичить в банкоматах. Это связано с тем, что банкоматы обычно оснащены камерами, поэтому преступник всегда рискует оставить свое лицо на память оперативникам. Правда, этот риск существенно можно уменьшить, если снимать деньги в темное время суток, прикрыть голову капюшоном, лицо — черными очками и прижать подбородок к груди.

Согласно сведениям на сайте kredit-kard.biz, стоимость одной поддельной карты составляет от $100 до $200 (в зависимости от объема покупки). Этот сайт можно назвать апофеозом наглости мошенников. На нем имеется просто потрясающий раздел «ответы на вопросы», в котором написано, что этот вид деятельности «довольно безопасен». На этой же страничке указано, что «размах кардингового бизнеса просто огромен», а среднее количество денег, которые можно снять с одной карты, составляет от $1,5 тыс. до $2,5 тыс. Получается, что покупка поддельных карт приносит, как минимум, десятикратную прибыль.

Безопасный «бизнес»

Найти мошенников, занимающихся фишингом, невероятно трудно. Еще сложнее привлечь их к уголовной ответственности. Российское законодательство пока не готово противостоять новым типам киберугроз, а правоохранительные органы имеют слишком мало подобного опыта. Да и мошенников гораздо больше, чем оперативных сотрудников, способных их поймать и обезвредить.

«Рассматриваемой противозаконной деятельностью занимаются как одиночки, так и международная организованная преступность. В большинстве случаев преступления требуют не очень больших финансовых затрат и часто состоят из технически простых действий, рассчитанных в том числе на наивность пользователей. Даже если в ходе оперативных действий удается найти преступников (что случается редко, поскольку не остается «материальных» следов преступлений), то сбор доказательств, а затем доказательство их виновности в суде становятся крайне редко реализуемой задачей»,— комментирует Виктор Наумов, партнер юридической фирмы «Байтен Буркхардт».

Проблема поиска фишеров осложняется и тем, что среди них уже произошло разделение труда. «Сегодня существует настоящий черный рынок карточных данных. Первая категория мошенников добывает их и продает другим людям, которые либо перепродают их „конечным“ пользователям, либо обналичивают самостоятельно,— объясняет схему работы Василий Окулесский, начальник отдела IT-безопасности Банка Москвы.— Распутать всю цепочку от начала до конца намного труднее, чем поймать мошенника-одиночку». По его словам, преступнику-одиночке сложно заметать за собой следы. Ведь ему нужно иметь доступ к инсайдерам, сливающим приватные данные, а также к оборудованию для производства поддельных кредиток. Наконец, ему нужно самому обналичивать деньги в банкоматах и действовать чаще всего в пределах одной страны, а то и одного города.

Крайний — клиент

Если же кража произошла, то вернуть пропавшие средства практически невозможно. Во-первых, необходимо доказать банку, что деньги снял со счета кто-то другой. Во-вторых, надо понять, кто именно несет ответственность за кражу данных, а в подавляющем большинстве случаев сделать это невозможно. Понятно, что виновником утечки может оказаться банк, любая компания, которая принимала платеж по данной карте, или же сам клиент. Определить структуру, несущую реальную ответственность за кражу, к сожалению, практически нереально.

«Определить, кто именно стал источником утечки, очень сложно, а порой просто невозможно. Однако для банка в этой связи сильным аргументом является доказательство его невиновности. Например, если в банке используются средства защиты от утечек, а система информационной безопасности сертифицирована и проверена независимыми аудиторами или регулирующим органом, то такой банк может смело заявлять в суде о своей невиновности. Тем самым область поиска источника утечки существенно сужается»,— уверен Олег Смолий, руководитель группы защиты телекоммуникационных систем управления защиты информации и объектов банка ВТБ.

Спасение утопающих...

Несмотря на невозможность защититься на 100%, существует ряд рекомендаций, строгое выполнение которых поможет снизить вероятность кражи. Прежде всего перед отправкой приватных сведений в сеть необходимо убедиться в подлинности сайта-адресата. Другими словами, нужно использовать только тот сайт, адрес которого клиенту дали в самом банке.

Разумный пользователь никогда не будет нажимать на ссылки, полученные от неизвестного адресата, даже если этот адресат представляется известной компанией. В крайнем случае достаточно просто позвонить в банк и узнать, действительно ли он осуществлял рассылку своим клиентам. Подчеркнем, что номера телефонов необходимо брать только с официальных сайтов.

Существует также целое семейство вирусов, занимающихся поиском данных о банковских картах на дисках зараженных компьютеров. Для того чтобы обезопасить себя от этой угрозы, пользователь должен использовать и постоянно обновлять антивирус, а также стремиться вообще не хранить подобную информацию на компьютере, подключенном к интернету.

По мнению директора по маркетингу российской компании InfoWatch Дениса Зенкина, все эти меры снижают вероятность кражи, но не исключают полностью ее возможность. «К сожалению, утечка данных может произойти по вине тех структур, которые когда-либо работали с вашей картой. В этом случае клиент совершенно не виноват, однако именно он несет максимальные потери,— отметил господин Зенкин.— В настоящее время многие организации внедряют системы защиты от утечек, однако их число пока невелико. Согласно результатам исследования InfoWatch „Внутренние IT-угрозы России-2006“, только 8% российских компаний имели работающую систему защиты от утечек по состоянию на конец 2006 года. Все остальные фирмы являются отличной мишенью для злоумышленников».

Таким образом, каждый владелец кредитки может стать жертвой мошенников. Однако если не быть наивным и не открывать поддельные ссылки в браузере, вероятность пострадать от утечки представляется мизерной.

Алексей Доля

ВЫДЕРЖКИ С САЙТА KREDIT-KARD.BIZ

«Конечно, снимать деньги с карт противозаконно, но если принимать меры, то это довольно безопасно. Посмотрите новости: задержания при таком виде кардинга случаются пару раз в год, и то в основном по глупости человека, который снимает деньги, а размах этого бизнеса просто огромен. То есть задержания при таком виде кардинга происходят не более чем в одном случае из тысяч, и то задерживают только тех, кто сам делает ошибки. Так что это один из немногих видов заработать большие деньги при практически нулевом риске. Мы можем дать и некоторые рекомендации как снять деньги безопаснее».

«Сами мы, конечно, не ходим по банкоматам и не снимаем деньги — уже не тот уровень у нас. Мы посылаем для этого специально обученных бойцов. Однако мы платим им свой процент, да еще и многие из них так и норовят обмануть нас. Хоть это и выгоднее, но ненамного. Кроме того, иногда у нас бывает слишком много дампов (данных о банковских картах.— „Ъ“), поэтому мы излишек продаем. В общем, это наш бизнес: как выгоднее на данный момент, так и поступаем. В данный момент у нас бывают иногда очень большие поступления дампов, поэтому достаточно много мы продаем».

«Мы не будем передавать ни при каких условиях заказ лично в руки, мы не будем передавать заказ ни Вашему человеку, ни Вашему знакомому проводнику и т. д. Если Вы заказываете доставку через проводника, мы сами найдем такового в нужном Вам направлении. Мы не будем класть пакет с картами в какое-то место или камеру хранения, определенное Вами. В случае выбора такой доставки мы сами выберем камеру хранения и после того, как карты будут там, сообщим где это и код для камеры».

NO COMMENT | THE NEW YORK TIMES

What's russian for «hacker»? Как по-русски будет «хакер»?

By Clifford J. Levy
Клиффорд Леви

Возможно, самым известным мошенником советской эпохи был говорливый, ловкий, двуличный бродяга по имени Остап Бендер. Это был вымышленный персонаж, антигерой сатирического романа о поисках спрятанных сокровищ под названием «12 стульев». Тем не менее его презрение к закону отражало широко распространенный здесь цинизм.

«Это деяние хотя и предусмотрено Уголовным кодексом, все же имеет невинный вид детской игры в крысу»,— говорит Бендер о плане, используя украденный документ для того, чтобы выдать одного человека за другого.

Если бы Бендер занимался своим делом сейчас, он, несомненно, сидел бы перед монитором компьютера, рассылая электронные письма, в которых выспрашивал данные о кредитных картах, или продавал лекарства от импотенции, или делал бы еще что-то в этом роде. Россия стала главным источником всех бед интернета, домом для легионов высокотехнологичных негодяев, которые действуют с видимой безнаказанностью, выходя в интернет из спален Новосибирска или полуподпольных интернет-кафе Санкт-Петербурга.

Хакеры пользуются такими именами, как ZOMBiE или «Команда рыцарей ада». Потусторонний мир, в котором они обитают, настолько силен, что на другом конце света фирмы, занимающиеся интернет-безопасностью в таких местах, как Силиконовая долина, вынуждены были начать специализироваться на русской хакерской культуре. Эти фирмы не получают серьезной помощи со стороны российского правительства, которое, как кажется, почти не заинтересовано в искоренении этого, как если бы чиновники тайно получали удовольствие от того, что их соотечественники измываются над миллионами людей на Западе. И на самом деле, минувшей весной российские хакеры стали кем-то вроде национальных героев, когда из России началась волна интернет-атак на вебсайты в бывшей советской республике Эстонии. Инциденты начались после того, как эстонцы разгневали Кремль, переместив военный памятник времен СССР.

Мотивом для большинства преступлений, однако, остается алчность. В 2005 году русские проникли на сайт штата Род-Айленд, а потом заявили о том, что похитили информацию о 53 тыс. трансакций по кредитным картам. Представители штата подтвердили факт кражи, хотя и заявили, что масштабы хищения были меньше. Преступников редко ловят, если такое вообще случается. Однако не так уж сложно вычислить их прошлое. Россия известна своей системой обучения точным наукам и математике. И до относительно недавнего подъема в экономике у всех этих толп умников, выходивших из школ, были весьма печальные перспективы в том, что касается работы.

В то же время они вступали в жизнь в обществе, в котором десятилетиями накапливался глубокий скептицизм по отношению к такой добродетели, как следование правилам. При коммунизме дебри ограничений, контролировавших практически каждый аспект жизни, воспринимались настолько бессмысленными, что считалось, что только дураки могут им следовать.

«Закон в советские времена выполнял совершенно иную функцию,— говорит Георгий Сатаров, президент фонда „Индем“, независимой организации в Москве.— Закон был ориентирован не на защиту интересов граждан. Для защиты интересов граждан существовала партия — и все».

Одним из результатов этого было то, что коррупция в советские времена была вездесущей, и она выжила, а то и стала еще большей. Россия занимает 143-е место из 180 стран и территорий — на уровне Гамбии, Того и Индонезии — в недавнем отчете о государственной коррупции, составленном некоммерческой организацией Transparency International (чем ниже место, тем выше уровень коррупции). Отношение таково: если провинциальные губернаторы или транспортная полиция, да и все остальные воруют, то почему я должен быть честным?

Эксперты в области интернет-безопасности говорят, что США и Китай соперничают с Россией по масштабам хакерской деятельности. Однако в России, по приблизительным подсчетам, всего 28 млн пользователей интернета, в то время как в США их 210 млн, а в Китае — 150 млн, из чего следует, что в России более высокий процент мошенников. Компания интернет-услуг VeriSign считает российских хакеров самыми опасными отчасти потому, что у них есть связи с организованными преступными группировками, которые похищают деньги с помощью украденной информации о кредитных картах и банковских данных.

Представители руководства технологических компаний в России говорят, что при президенте Владимире Путине Кремль наглядно показал, что если он хочет добиться чего-то, то он этого добивается. «Проблема в том, что у нас население очень образованное, а законодатели абсолютно невежественные и глупые,— говорит Антон Носик, представитель руководства компании, которая курирует сайт Livejournal.ru, русскую версию популярного портала.— У правоохранительных органов нет стимула и причин для уголовного преследования. Они говорят „К нам не поступают жалобы“ или „Жалобы, которые к нам поступают, неправильно оформлены“. Они находят предлоги для того, чтобы не преследовать в судебном порядке». Блоги на российском портале Livejournal регулярно похищаются, и обычно теми людьми, которые крадут пароли. Но даже в такой ситуации складывается ощущение, что российские хакеры доставляют Западу проблем больше, чем сама Россия, поэтому стоит ли с ними возиться?

На прошлой неделе на сайте российского Livejournal газета The New York Times задала вопрос пользователям, почему за русскими закрепилась слава интернет-преступников. «Не вижу в этом большой трагедии,— написал пользователь, называющий себя Lightwatch.— Западные страны сыграли не самую маленькую роль в развале Советского Союза. Но у русских есть одна очень забавная черта: они способны подниматься с колен при любых условиях и в любых обстоятельствах».

А как насчет Запада? «Вы получаете по заслугам».

Перевел Иван Никольский