Автор: Олег Хохлов © Коммерсантъ РАССЛЕДОВАНИЯ, ИРКУТСК 6431 29.03.2012, 12:29 818

ПИН да положь

Управлению К удалось взять группировку хакеров, которая уводила с банковских счетов граждан и компаний десятки, если не сотни миллионов рублей в год. Мошенничества с банковскими картами — глобальная проблема. На Западе это головная боль банков и платежных систем, а в России — их клиентов.

Кража денег на расстоянии

В истории о том, как на прошлой неделе в Москве арестовали участников хакерской группировки, ответственной за взлом банковских систем дистанционного обслуживания, много неясного.

О завершении операции одновременно сообщили следственный департамент МВД и компания—резидент фонда "Сколково" Group-IB, которая помогала расследовать дело управлению К и Центру информационной безопасности ФСБ. Оперативники задержали восьмерых участников преступной группы, организаторами которой называют уроженцев Санкт-Петербурга 1983 и 1986 годов рождения, родных братьев.

На протяжении двух лет они опустошали банковские счета компаний, взламывая компьютеры сотрудников, имевших к ним удаленный доступ через системы интернет-банкинга. Атаке подверглись клиенты более чем ста банков из разных стран. Управление К подсчитало, что лишь за последний квартал 2011 года им удалось похитить около 60 млн руб. По оценке же Group-IB, общий ущерб от мошеннических действий банды — как минимум в два раза больше. О том, какие именно банки и компании стали жертвами хакеров, управление К не сообщает. По собственной инициативе пока высказалась лишь пресс-служба Сбербанка: 27 хищений на сумму более чем 10 млн руб. Если эти цифры верны, речь идет о самом крупном раскрытом преступлении такого рода в российской практике.

Впрочем, достоверной статистики интернет-мошенничеств, совершаемых в России, нет. Центробанк учетом не занимается. МВД раз в год сообщает лишь о числе заведенных дел по ст. 187 УК "Изготовление или сбыт поддельных кредитных, расчетных карт и иных платежных документов". Банки тему комментируют неохотно. Лишь на условиях анонимности их представители признают, что речь может идти примерно об 1 млрд руб. в год. Это на порядок меньше, чем, например, в США, где статистикой время от времени делятся ФБР и ФРС.

"Чтобы вы примерно оценили масштаб: мы ежедневно фиксируем более 20 успешных случаев хищений со счетов физических и юридических лиц и столько же — неудачных попыток,— говорит Илья Сачков, генеральный директор Group-IB.— Мы общаемся с правоохранительными органами, банковскими службами, специализированными экспертными организациями. Если сопоставить данные из разных источников, получится, что в России ежедневно происходит порядка 90 успешных краж".

Уже успел обрасти бородой анекдот: "Чтобы стать кардером, нужна кувалда и ноут: разбиваешь банкомат и забираешь деньги.

— А ноут зачем?

— Какой же ты кардер без ноута?"

Но теперь высокотехнологичный гоп-стоп — проза. Кстати, и в прямом смысле тоже. "Робин Гуд современной эпохи, великий кардер, за которым по сей день охотится Интерпол. Человек, без зазрения совести обворовывающий западные банки,— Изя Питерский..." — это из аннотации к роману "Исповедь кардера", который издательство "Альпина Паблишер" выпустило тиражом 1,5 тыс. экземпляров еще в 2010 году. А недавно вышла "Исповедь кардера-2".

Троян вместо скимминга

Самые распространенные схемы мошенничества, не считая банального подсматривания ПИН-кода,— фишинг и скимминг. Скимминг — считывание с магнитной дорожки банковской карты информации оборудованием, которое мошенники устанавливают на банкоматах в отдаленных и плохо освещаемых местах.

Технологичнее — фишинг. Это вид мошенничества в интернете, цель которого — получить идентификационные данные пользователей. Данные карт своих клиентов могут воровать банковские клерки или, например, сотрудники интернет-магазинов. К фишингу относится запрос о данных карты по e-mail. Многие, впрочем, уже уяснили, что никто не имеет права требовать информацию о карте. Эффективнее другая разновидность фишинга — создание страницы, копирующей внешний вид сайта, с помощью которого пользователь оплачивает товары и услуги кредиткой. Помимо интернет-магазинов под ударом — сайты банков, платежных систем, авиакомпаний и, конечно, все, что связано с порно.

Все это классика, а главный тренд последних лет — атака на онлайновые представительства банков. Неудивительно, сервисы стремительно развиваются. "Только за 2011 год количество таких правонарушений увеличилось вдвое и продолжает расти,— констатирует Илья Сачков из Group-IB.— В прошлом году, по нашей оценке, российским интернет-мошенникам удалось похитить с банковских счетов юридических и физических лиц из разных стран около $900 млн. Физические лица потеряли примерно $130 млн".

Даже самый осторожный клиент банка может стать жертвой интернет-мошенничества, подобно тому как никто не застрахован от уличного ограбления. Правда, в первом случае есть реальная возможность вернуть украденное. Формально хищение денег со счета — это вообще проблема банка, которому вы доверили их хранение. Но в России это правило пока не работает. Часто доказывать свою добросовестность жертвам мошенников приходится в суде.

"Банки исходят из того, что техническая сложность и сопутствующие затраты отпугнут потребителей от борьбы за свои права,— комментирует председатель совета правозащитной организации "Финпотребсоюз", экс-руководитель Федеральной комиссии по рынку ценных бумаг Игорь Костиков.— Это притом, что банки свою деятельность страхуют и вообще-то ничего не теряют". Собеседник "Денег" исходит из собственного опыта. Несколько лет назад с его кредитной карты украли примерно €70 тыс.— фактически годовую зарплату. Деньги сняли в течение суток в нескольких банкоматах Санкт-Петербурга. Игорь Костиков в это время вместе с семьей находился в Великобритании, собирался лететь в Испанию. Звонок в банк не обнадежил: пишите заявление, собирайте документы, мы их в течение месяца рассмотрим.

"Интересно, как при наличии чипа, стрипа и пина, который я никому не доверял, кому-то удалось сделать дубликат? Я уверен, что информация была получена внутри банка,— говорит он.— Кроме того, для этой карты был установлен лимит: не более €600 наличных даже не в сутки, а в месяц. И тем не менее банк решил оставить меня и близких в канун Рождества без денег. Любой западный банк в такой ситуации на время расследования перевел бы клиенту пускай не все деньги, но хотя бы какую-ту сумму".

Игорь Костиков не стал ждать месяц, использовал административные рычаги и получил деньги уже через два дня.

"Мне удалось пообщаться с сотрудником банка, который занимался моим случаем. По его словам, это был первый случай, когда жалобу разобрали так быстро, обычно позиция банка — тянуть по максимуму",— говорит Костиков. Похожий случай произошел с корреспондентом "Денег". Два года назад с моей дебетовой карты Райффайзенбанка украли около 30 тыс. руб. Деньги вернули через пару недель. Думаю, помогло удостоверение сотрудника "Коммерсанта".

Борьба с банком

Юрист "Финпотребсоюза" Екатерина Радионова замечает, что случаев, когда решить проблему удается в досудебном порядке,— единицы. Суды первой инстанции, по ее словам, в подавляющем числе случаев принимают сторону банков. Второй инстанции — тоже, но уже немного реже.

В самом незавидном положении оказываются жертвы афер с использованием поддельных банковских карт, так называемого белого пластика. Если преступникам удалось проникнуть в систему дистанционного банковского обслуживания, шансов доказать непричастность клиента совсем мало.

В теории законодательство находится на стороне держателей карт. Согласно закону о защите прав потребителей, банк отвечает за безопасность услуг, которые он оказывает. Согласно Гражданскому кодексу, сохранность денег является основной обязанностью банка, и убытки, причиненные клиенту, он обязан компенсировать, если у него нет доказательств того, что ущерб возник по вине клиента. На практике банковские юристы строят свою аргументацию на том, что у них нет оснований верить клиенту: может, он сам себя обокрал или, например, сообщил пин-код постороннему лицу. При этом, поясняет Екатерина Радионова, они апеллируют к Гражданско-процессуальному кодексу: мол, стороны в суде должны доказать факты, на

которые ссылаются. А как доказать, что не расставался с картой, а пин-код хранишь в тайне?

"Ситуация не изменится, пока в полном объеме не заработает закон о национальной платежной системе, то есть до конца этого года, когда вступит в силу та его часть, которая посвящена электронным средствам платежа,— поясняет вице-президент Ассоциации региональных банков "Россия" Олег Иванов.— В новом законе говорится, что именно банк должен доказывать, что в мошеннической трансакции виноват клиент".

Это не единственная законодательная инициатива в данной сфере. Глава ассоциации "Россия" Анатолий Аксаков второй год призывает ужесточить ответственность за изготовление, сбыт и использование поддельных банковских карт. Ассоциация российских банков Гарегина Тосуняна хочет ограничить ответственность банков: выплачивать компенсации лишь тем, кто установит для своих карт или максимальную сумму остатка по счету (не более 300 тыс. руб.), или максимальную сумму операции (не более 100 тыс.). Первый заместитель председателя комитета ГД по финансовому рынку Владислав Резник в прошлом году предложил заставить банки уведомлять держателя о каждой операции с платежной картой и, если от клиента не поступит подтверждения, такую трансакцию блокировать.

Олег Иванов призывает не драматизировать сложившуюся ситуацию. По его словам, и сейчас реально отстоять свои права. Алгоритм простой. Нужно как можно раньше опротестовать мошенническую трансакцию и заблокировать карту. Такая возможность есть у тех, кто подписан на SMS-уведомления о состоянии счета. Большинство банков подключают держателей кредитных карт к этой услуге бесплатно. Но есть исключения. Например, ТКС-банк Олега Тинькова просит за это дополнительные 590 руб. в год.

А вот обратиться в управление К — задача не из тривиальных. Ни одна справочная не знает контактов управления, включая, кстати, и милицейскую горячую линию. На сайте МВД предлагается идти в отдел полиции по месту жительства и надеяться на то, что оттуда заявление к борцам с киберпреступностью рано или поздно попадет.

В отделении банка нужно написать официальную претензию (как правило, этот документ называют заявлением на межбанковское расследование). Можно отправить ее и по почте, но обязательно заказным письмом с уведомлением о вручении. Нужно передать в банк все имеющиеся документы, которые могут сыграть в вашу пользу. В первую очередь — документы из полиции, если вам удалось их получить. Если требуется доказать, что в момент совершения мошеннической трансакции вы были в России или, наоборот, находились за границей, понадобится копия загранпаспорта. До принятия новых норм, увы, нужно быть готовыми доказывать банку, что это не вы сами себя обокрали.

Автор: Олег Хохлов © Коммерсантъ РАССЛЕДОВАНИЯ, ИРКУТСК 6431 29.03.2012, 12:29 818
URL: https://babr24.com/?ADE=104202 Bytes: 10900 / 10879 Версия для печати Скачать PDF

Автор текста: **Олег Хохлов**.

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта