Кибермошенников, похитивших деньги у камчатцев, задержали в Тюмени.
Еще несколько лет тому назад подобный заголовок вызвал бы у читателей, по меньшей мере, удивление. Но время движется вперед, и вместе с прогрессом, к сожалению, совершенствуется преступность. Теперь вполне реально забираться в кошельки граждан и красть их сбережения, не вставая с дивана, был бы компьютер под рукой. Благодаря этому, в наше время мошенничество стало одним из самых распространенных видов преступления.
В середине июня этого года в полицию обратился житель Вилючинска с заявлением, что с его банковской карты исчезли восемь тысяч рублей, а 1 июля подобное заявление написала жительница краевого центра, с карточки которой исчезли около четырех с половиной тысяч. И вот по подозрению в совершении этих преступлений задержаны двое 24-летних жителей Тюмени: девушка и парень. Сейчас сотрудники полиции устанавливают сумму причиненного ущерба, выявляют сообщников фигурантов, разыскивают всех потерпевших, каковых должно быть немало. В ходе обыска у задержанных обнаружено и изъято 190 сим-карт, 75 банковских карт Сбербанка, а также мобильные телефоны и компьютеры, с помощью которых совершались преступления.
Начальник отделения «К» УМВД России по Камчатскому краю майор полиции Алексей Тимошенко рассказал, что на территории Камчатского края данный вид телефонного мошенничества, которому подвержена операционная система «Android», впервые был зафиксирован в конце прошлого года. У населения растет популярность современных сотовых телефонов на различных операционных системах, особенно – «Android». И злоумышленники придумывают различные способы, чтобы взломать ее, чаще всего, под видом всевозможных «невинных» сообщений или рекламы рассылаются «смс-трояны».
В чем суть этого мошенничества? Сейчас получила популярность очень удобная услуга – управление банковским счетом посредством системы «Мобильный банк», то есть через сотовый телефон посредством смс-команд можно осуществлять перевод денег на другие счета и платежные системы.
Пользователь сотового телефона, переходя по различным ссылкам на интернет-сайты, либо устанавливая программное обеспечение себе на телефон, сам того не подозревая, загружает вирус типа «троян». При загрузке такой вирус дает возможность злоумышленнику удаленно управлять сотовым телефоном жертвы. Преступник может читать переписку в контактах, отправлять смс-сообщения, включать видеокамеру, а также дистанционно управлять банковским счетом без ведома владельца смартфона. Причем, вирус довольно умело скрывает свои «следы», абонент не видит, что с его телефона отправляются сообщения и не получает сообщения от банка на подтверждение перевода денежных средств. Ответы даются удаленно уже злоумышленником, то есть фактически зараженный вредоносным вирусом телефон является «посредником» между мошенником и банком. А истинный хозяин гаджета и денежного счета ничего не подозревает, пока не обнаружит пропажу денег.
Это серьезный вид мошенничества, который набирает обороты в последнее время в России и по всему миру. Подобные преступления практичес-
ки невозможно выявить на подготовительной стадии. Они отличаются значительным материальным ущербом, причиненным большому количеству потерпевших, которые живут в самых разных уголках страны. Тут расстояния не имеют никакого значения. Преступники обладают высоким профессиональным уровнем и используют в своей

деятельности новейшие информационные технологии. А еще данный вид преступности отличается высокой латентностью. Собственно, на это и рассчитывают злоумышленники: если взять у одного и много, то это точно станет поводом для вмешательства правоохранительных органов. А если понемногу у большого количества потерпевших, то многие из жертв предпочтут забыть о мелкой неприятности.
Тем не менее, полиция все быстрее наступает на пятки кибермошенников. В этом году правоохранительные органы при взаимодействии с подразделениями безопасности Сбербанка обезвредили пять преступных групп, осуществляющих массовые атаки на клиентов банка. Ранее полиция задержала группу из 22 мошенников, которые похищали деньги у клиентов Сбербанка с помощью звонков и рассылок sms из специально оборудованного колл-центра. Сотрудники МВД также в апреле сообщили о задержании подозреваемых в хищении 50 миллионов рублей со счетов клиентов нескольких российских банков. В числе задержанных – автор компьютерного вируса, с помощью которого преступники получали контроль над гаджетами граждан.
Но все же любое преступление лучше предотвратить заранее. Узнать о наличии угрозы в телефоне можно только с помощью антивирусного программного обеспечения или путем постоянного отслеживания транзакций по своему банковскому счету. Чаще всего «ловят» вредоносного вируса активные пользователи сети Интернет, которые управляют и проводят финансовые операции по своим счетам, посещают различные сайты, общаются в социальных сетях, получают и отправляют электронные письма и сообщения с вложениями, закачивают и устанавливают различные приложения (игры, программы, обновления к ним), не заботясь о защите своих мобильных устройств. Поэтому сотрудники полиции рекомендуют установить на мобильных устройствах лицензионное антивирусное программное обеспечение и регулярно его обновлять, скачивать и устанавливать игры, программы, обновления к ним только с проверенных источников. Для авторизаций, управления счетом и совершения операций с мобильных устройств используйте официальные приложения, предоставляемые банком, а лучше всего, купите себе для этого обычный, без «наворотов» телефон и пользуйтесь им только для работы с системой «клиент-банк». Запомните: этот телефон – ваш финансовый инструмент. И еще: при смене абонентского номера, не забудьте незамедлительно в банке, выдавшем карту, отключить услугу «Мобильный банк» по старому номеру телефона, пока вашей оплошностью не воспользовался его новый владелец. Такие случаи неоднократно бывали.
В заключение Алексей Тимошенко добавил: «Рекомендуется отключить в телефоне функцию «Установка со сторонних источников». Она есть практически на всех смартфонах. Устройство блокирует установку программного обеспечения с непроверенных интернет-площадок. И помните об установке антивирусного программного обеспечения. Это в обязательном порядке должен сделать каждый, кто покупает смартфон на базе Android. Пользоваться телефоном без «антивируса» в настоящее время очень рискованно. Даже если у вас не подключен «Мобильный банк», вирус типа «троян» позволяет осуществить массовую рассылку смс-сообщений на короткие номера, стоимость отправки на которых колеблется от 300 до 1000 рублей. Со счета деньги будут сниматься, и вы опять же не сразу обнаружите снятие денежных средств, потому что смс в книге сообщений телефона не будет регистрироваться».

Иван ТИМОФЕЕВ.