БЕЗОПАСНОСТЬ

Кардинг, скимминг и др.

В банковской сфере пышным цветом расцветает киберпреступность

Татьяна Власенко

Рост безналичных расчётов на рынке товаров и услуг сопровождается негативом, который снижает доверие юридических и физических лиц к электронной финансовой деятельности банков. Учащаются случаи взлома информационных систем, в результате чего злоумышленники получают доступ к банковским картам клиентов и их реквизитам.

По словам начальника отдела управления безопасности и защиты информации ГУ Банка России по Пермскому краю Станислава Попова, наиболее распространёнными нарушениями являются изготовление дубликатов платёжных карт и вещевой кардинг.

Классическая преступная схема представляет собой изготовление дубликатов кредитных или расчётных (в том числе выпущенных в рамках зарплатных проектов) карт, которые в дальнейшем перепродаются для обналичивания денежных средств или перевода денег на счета мобильных телефонов, зарегистрированных на вымышленных лиц.

Вещевой кардинг связан с приобретением различных товаров в интернет-магазинах с помощью полученных преступным путём банковских реквизитов. Прежде так называемые кардеры преимущественно имели дело с иностранными банками и их клиентами, но в последнее время переключились на российский рынок банковских услуг.

Преступники действуют и на территории Пермского края. Это хорошо организованные межрегиональные группы, которые распределяют между собой роли, поэтому обнаружить их и привлечь к ответственности достаточно сложно.

Среди них есть спецы, которые занимаются только взломом и получением информации о банковской карте. Полученная ими информация передаётся лицам, содержащим подобие интернет-магазина, который перепродаёт банковские реквизиты производителю поддельных пластиковых карт. Тот, в свою очередь, распространяет подделки, продавая или передавая их последнему звену цепочки — «дрогу». «Дрог» — это физическое лицо, которое организует непосредственно съём денег в банкоматах. Он обладает наименьшим объёмом информации, часто его используют «втёмную».

Общение между участниками преступной группы происходит через различные интернет-сервисы: Сеть пестрит объявлениями о «простом и доступном» заработке. И это провоцирует значительный рост таких преступлений.

Станислав Попов, начальник отдела управления безопасности и защиты информации ГУ Банка России по Пермскому краю:

— Организаторы такого бизнеса — люди образованные — как с технической, так и с юридической стороны. Они зачастую имеют несколько высших образований, знакомы в том числе с криптографией, что значительно затрудняет их поиск. На территории края действует несколько устойчивых преступных групп, которые занимаются кардерской деятельностью. Они пропагандируют лёгкий заработок, якобы не грозящий наказанием, ведут свою деятельность с помощью SIM-карт, зарегистрированных на подставных лиц, что зачастую приводит розыск злоумышленников в тупик.

Негативно отражается на оперативной обстановке и свободная продажа оборудования, в том числе через интернет, которое позволяет изготавливать пластиковые карты с магнитной полосой.

Ещё один вид преступлений — мошенничество с платёжными картами посредством скимминга (перехват информации с магнитной полосы платёжных карт с использованием специального устройства — скиммера, устанавливаемого на банкомат). Скиммер накладывается непосредственно на картридер, куда ничего не подозревающая жертва вставляет свою карту. Преступники снимают данные и в любой момент могут опустошить банковский счёт клиента или изготовить поддельную копию карты.

Самый простой способ получить PIN-код — подсмотреть его, стоя поблизости от владельца карты. Мошенники могут также распылять на клавиатуру банкомата специальный спрей, в этом случае будут чётко видны нажатые клавиши. Они могут установить и накладную клавиатуру, которая практически ничем не отличается от собственной клавиатуры банкомата, навесить микрокамеры, которые вполне можно не заметить.

Существуют даже специальные панели, которые накладываются на всю поверхность банкомата, где считываются одновременно и PIN-код, и номер банковской карты. При этом скиммеры свободно продаются в интернете и стоят порядка $200. Некоторые продавцы за определённую плату предлагают даже обучить изготовлению скиммеров.

Специалисты по банковской безопасности рекомендуют: прежде чем воспользоваться банкоматом, стоит внимательно его осмотреть. На нём не должно быть выступающих частей, особенно отличающихся по цвету. Возле банкомата не должно быть подставок с буклетами, следует обратить внимание и на людей, находящихся поблизости.

«Многие банки начали вести видеонаблюдение за банкоматами, использовать специальную сенсорную сигнализацию, устанавливать антискримминговые накладки, устраивать плановые проверки банкоматов на предмет установки таких устройств», — поясняет Станислав Попов методы борьбы с преступниками.

По данным специалистов антивирусных компаний, в последнее время наблюдается расцвет интернет-мошенничества. Такие действия подпадают под статью Уголовного кодекса РФ «Создание и использование, распространение вредоносного программного обеспечения».

Станислав Попов:

— Для противодействия разработчики защитного программного обеспечения пытаются совершенствовать свои продукты. Правоохранительные органы взялись за эту разновидность киберпреступности, которая, развиваясь, приобретает новые формы.

Самое популярное средство у мошенников — так называемые банковские «трояны». Они ориентированы на получение неавторизованного доступа злоумышленников к счетам физических лиц посредством системы дистанционного банковского обслуживания, которая набирает обороты.

Но есть и просто мошенничество. Пользователи банковских карт могут получить сообщение якобы от службы безопасности кредитной организации, где для повышения безопасности карты и во избежание блокирования клиенту предлагается вставить её в любой банкомат, набрать PIN-код и позвонить с мобильного телефона по указанному в SMS-сообщении номеру. Затем выполнить ряд действий, которые будет диктовать оператор. Это будет набор цифр определённой последовательности. После завершения этих манипуляций человек, как правило, обнаруживает, что деньги с карты уже переведены на другие банковские счета. И это далеко не все схемы мошенничества.

С 1 января 2014 года вступают в силу основные положения ст. 9 «Порядок использования электронных средств платежа» федерального закона №161. В соответствии с этим документом, банки будут обязаны уведомлять клиента о совершении каждой операции с использованием его электронного средства платежа (например, телефонной связи, SMS-сообщений, электронной почты и т. п.).

В случае утраты карты и её использования без согласия клиента он обязан направить соответствующее уведомление кредитной организации незамедлительно после обнаружения пропажи. Клиент тоже должен быть заинтересован в доведении информации о факте мошенничества, это в его интересах: только в этом случае оператор по переводу денежных средств будет обязан возместить клиенту сумму указанной операции. И уже потом банк будет разбираться, в результате чьих злоумышленных действий были похищены деньги. ■

Скимминг

Схема: вы совершаете любую операцию в банкомате и, ничего не подозревая, уходите по своим делам. В то время как мошенники с помощью скиммера считали всю информацию о вашей карте и в любой момент сделают её дубликат и обнулят ваш банковский счёт.

Откуда мошенники узнают PIN-код?

Варианты:

— самый элементарный способ — человек, стоящий за вами в очереди, просто подсмотрит пин-код из-за вашей спины;
— мошенники могут распылить на клавиатуру специальный спрей, на котором будут чётко видны нажатые вами клавиши;
— мошенники могут установить накладную клавиатуру, которая почти ничем не отличается от самой клавиатуры банкомата;
— установка на банкомат микрокамеры, вы её не заметите, потому что она будет спрятана за пачкой рекламных буклетов.