О НЕКОТОРЫХ ТЕНДЕНЦИЯХ РАЗВИТИЯ КИБЕРПРЕСТУПНОСТИ В ФИНАНСОВО-КРЕДИТНОЙ СФЕРЕ РОССИЙСКОЙ ФЕДЕРАЦИИ*

Фролов Д.Б.,
Центральный банк Российской Федерации
d_frolov@list.ru
Персанов Д.Ю.,
Группа компаний QIWI

Аннотация. *В статье проведен анализ открытых источников по вопросу выявления преступлений в финансово-кредитной сфере.*

Ключевые слова: *финансово-кредитная сфера, банковские операции, обналичивание, легализация*

SOME TRENDS OF CYBER CRIME IN THE FINANCIAL AND CREDIT FIELD OF THE RUSSIAN FEDERATION

Frolov D.B.,
The Central Bank of the Russian Federation
Persanov D.Y.,
QIWI Group

Abstract. *This article analyzes public sources on the revealing of crimes in the financial and credit sector.*

Keywords: *financial and credit sector, banking, cashing, legalization.*

Оценка и анализ данных, полученных из различных открытых источников, позволяют сделать вывод о том что, как и ранее, в структуре выявленных преступлений в финансово-кредитной сфере (ФКС) преобладали:

- сомнительные банковские операции по «обналичиванию» денежных средств и легализации доходов, полученных преступным путем, имеющих крупномасштабный характер (с использованием ранее известных и неизвестных схем);
- мошенничество (незаконная банковская деятельность, незаконное получение кредитов, использование высоких информационных технологий, финансовые пирамиды и т.п.);
- злоупотребление служебным положением со стороны руководителей и служащих КО, создающих, тем самым, условия для мошенничества, хищений, вывода денежных средств из легального оборота и за рубеж;
- хищение денежных средств из банкоматов, как путем их взлома, так и с использованием поддельных пластиковых карт, а также установка нештатного оборудования (скимминг);
- разбойные нападения на структурные подразделения КО и лиц, перевозящих ценности и денежные средства;
- фальшивомонетничество.

Зафиксированы случаи разбойного нападения на кассовые узлы.*

Отмечается заметная активизация использования современных технических приемов для хищения денежных средств физических и юридических лиц, как в крупных, так и в особо крупных размерах, и все активнее используются технологии безналичных пе-

* I Международный конгресс по информационной безопасности национальных экономик в условиях глобализации «InfoSecurityFinance». Под научной редакцией: **Царегородцева А.В.**

реводов, снятия наличных денежных средств, внедряемых не только через широкую сеть банкоматов и платежные терминалы, но и через сеть Интернет.

В 2011-2012 годах, как и прежде, все совершаемые в ФКС мошенничества, отличались адаптацией злоумышленников к обновлению и усложнению механизмов функционирования банковской деятельности, изобретением новых форм маскировки преступлений, умелым использованием в противоправной деятельности подложных финансовых документов, подставных лиц, как правило, находящихся в сговоре со злоумышленниками или в служебной от них зависимости, технических новаций, а также недостатков законодательной базы. Все большую актуальность приобретают многокомпонентные и многоходовые мошеннические комбинации, осуществляемые организованными преступными группами. Используя знания об организации информационных систем и применяемых технологиях обработки и защиты информации, преступники вырабатывают новые способы совершения преступлений, используя мобильные устройства, социальные сети и специально разработанные вредоносные программы.

Динамика покушений на хищения денежных средств клиентов КО начинает приобретать угрожающий для банковской системы характер, особенно в системе дистанционного банковского обслуживания (ДБО). Выявленные факты покушений, как правило, были связаны с неправомерным доступом к компьютерной информации клиентов банков, пользующихся услугами ДБО, что обусловлено сверхдоходностью и отсутствием примеров неотвратимости наказания за совершенные преступления (в масштабах государства речь идет о хищениях сотен миллионов рублей). Пострадавшими от подобного рода преступлений являются клиенты подразделений практически всех крупных банков страны.

Мошенничества с использованием высокотехнологичных методов или киберпреступления сегодня оказались в центре внимания, их масштабы не ограничиваются пределами России – данный вид противоправной деятельности транснационален и динамично развивается.

На сегодняшний день стремление кредитных организаций налаживать свои собственные терминальные сети и организовывать собственные платежные системы объясняется желанием не потерять прибыльную долю рынка. В то же время обширная терминальная сеть обеспечивает потенциальные возможности для проведения серии сомнительных операций через неучтенные платежные терминалы.

Большинство случаев мошенничеств через банкоматы приходится на скимминг (комплекс устройств нацеленных на незаконное получение конфиденциальной информации, например, данных банковской карты), менее популярными являются физические атаки на банкомат (взлом или хищение) и установка вредоносного программного обеспечения.

Рост количества пластиковых карт у населения спровоцировал увеличение фактов правонарушений в этой области. По итогам 2011 года количество преступлений такого рода выросло на 36% в сравнении с 2010 годом. Ущерб оценивается более 1.6 млрд руб.

В настоящее время актуально использование типичного набора «отмычек» - способов получения злоумышленниками неправомерного, несанкционированного доступа к персональной информации пользователей систем ДБО:

- заражение компьютеров пользователей шпионскими и троянскими программами;
- фишинг;
- скимминг;
- рассылки электронных сообщений, предлагающих ввести определенную информацию в поля экранных форм, либо содержащих во вложениях вредоносное программное обеспечение;
- преступный сговор с инсайдерами, недобросовестными сотрудниками банков, которые располагают нужными полномочиями;
- «перехват» ответов на запросы персональных данных клиентов ДБО внешними структурами – представителями государственной власти, правоохранительными органами или отраслевыми регуляторами.

В соответствии с принятой Центральным банком Российской Федерации стратегией развития пла-

тежной системы одним из важнейших направлений ее реформы является сокращение наличных денег в обращении и переход на безналичный расчет. В настоящее время в России совершается более 2 млн. операций в день по банковским картам. Возросшее количество случаев хищения денежных средств отмечается в сфере электронных платежей путем взлома системы «электронный банк», внедрения вредоносного кода в банковское оборудование. Информация о счетах, компьютерных паролях стала своеобразным криминальным товаром.

Отмечается рост различных схем хищений с использованием мобильного телефона клиентов КО.

Укрепляющиеся тенденции, которые прослеживаются на рынке киберпреступности в ФКС, свидетельствуют о следующем. Фиксируется тренд к укрупнению и повышению организованности кибергруппировок, укрепление взаимосвязей с традиционной преступностью. Например, на рынке незаконного обналичивания денежных средств в настоящее время работают как непосредственно «банковские» мошенники, так и кардеры, поставляющие виртуальные деньги для «коллег по цеху». Корневая причина указанной тенденции заключается в том, что рынок компьютерной преступности становится все более финансовоемким, что не может не интересовать традиционных представителей криминального мира.

Следующий тренд - консьюмеризация рынка киберпреступности. В терминологии Group-IB это так называемый рынок c2c (cybercrimetocybercrime), т.е. платные услуги для внутреннего потребления мошенниками. Причем, следует отметить тенденцию к появлению нетрадиционных для виртуального мира услуг (как правило, c2c направления включают в себя ИТ-аутсорсинг, например бот-сетей), таких как страхование рисков уголовной ответственности, предлагаемых некоторыми печально известными хакерами. Более того, для кардинг-сообщества давно известны услуги по аренде дропов (физических лиц, используемых в схемах с незаконным обналичиванием).

С технологической точки зрения, по нашему мнению, текущий и последующие годы для ФКС ознаменуются повышенным вниманием к мобильным устройствам и средствам дистанционного доступа к банковским счетам. В связи с взрывным ростом использования iOS- и Android-устройств в качестве средств дистанционного банковского обслуживания, вектор угроз будет смещаться от традиционных вирусов и троянов, похищающих данные с пользовательских рабочих мест под управлением Windows и других операционных систем, в сторону заражения мобильных устройств. Стоит отметить, что в случае с мобильными устройствами негативный эффект может быть значительно серьезнее в силу эффекта масштаба.

Для банковской системы в целом характерной угрозой является распространение специализированного вредоносного ПО, «заточенного» под конкретные автоматизированные банковские системы. С ростом популярности использования методов двухфакторной аутентификации для подтверждения платежа (например, одноразовые пароли в СМС), эволюцию будут претерпевать и вредоносные программы. Например, одна из известных модификаций банковского трояна имела возможность перехвата управления интерфейса ввода кода подтверждения, генерируемого OTP-токеном, после чего помимо легитимного платежа одновременно проводила дополнительный, затирая сведения о нем в выписке системы дистанционного банковского обслуживания.

На стыке банковской и ритейл-индустрий находится технология бесконтактных платежей. Следует ожидать появления устройств и методов перехвата платежных сообщений и аутентификационных данных в связи с проникновением указанных технологий в торговые сети и точки оплаты, оборудованные соответствующими банковскими POS-терминалами.

Также следует отметить, что банковский сектор усиленно готовится к вводу в действие соответствующей статьи ФЗ «О национальной платежной системе», обязывающей кредитные организации компенсировать финансовый ущерб клиенту в случае несанкционированного использования его денежных средств, до момента получения официального решения от правоохранительных органов о первопричинах и субъектах преступления. С точки зрения кибермошенничества, указанная статья создает

определенные условия для лавинообразного роста заявлений недобросовестных клиентов в виде отказа от совершения cardholder-not-present транзакций, например, при использовании интернет-магазинов. В этом случае риски банка возрастают, т.к. именно на банк ложится бремя доказывания легитимности совершенной операции и нарушения клиентом правил доступа к его банковскому счету.

Прогнозируется, что дальнейшее развитие криминогенной обстановки в стране будет основываться на уже сложившихся ее элементах, дополняться новыми устремлениями криминального сообщества, и определяться совокупностью экономических предпосылок.

Для ФКС вопросы защиты информации традиционно являются одними из ключевых. С развитием и усложнением систем дистанционного банковского обслуживания, проникновением новых, зачастую не до конца изученных технологий в банковскую систему с одной стороны, и ростом преступных организаций с другой стороны, банковское сообщество обязано принимать во внимание меняющийся профиль рисков при построении новых и обслуживании старых бизнес-моделей.