РАЗДЕЛ XII. ЭКОНОМИКА

Бочарова Ж.Ю., Ужва А.Н.

Защита электронных каналов банковских услуг

*Национально исследовательский университет «БелГУ»
(Россия, Белгород)*

doi: 10.18411/sr-10-02-2018-35

idsp: 000001:sr-10-02-2018-35

За последние 10 лет произошёл существенный прорыв в части банковского обслуживания населения – население весьма активно пользуется банковскими услугами, развиваются интернет-каналы банковского обслуживания как бизнеса, так и частных лиц.

Развитие бизнеса, расширение спроса населения на рынке услуг требуют от банковской системы организации оперативной, эффективной системы обслуживания клиентов банка, создавая возможности обслуживания клиентов из дома, офиса или мультимедийного киоска самообслуживания.

Одновременно с развитием электронных каналов банковских услуг развиваются и преступления в данной сфере. Злоумышленники стремятся получить информацию о банковских счетах, информацию о личных данных клиентов банков с целью хищения денежных средств. Как следствие, мошенники с легкостью проходят любые проверки пользователя – кодовое слово, паспортные данные и пр., иногда такие операции совершают сами клиенты по указке злоумышленников. Использование вирусов и другого вредоносного ПО, инициирующего нелегитимные операции с рабочих мест пользователей.

Наиболее распространёнными способами атак на системы дистанционного банковского обслуживания (далее – ДБО) являются:

- вредоносное ПО (трояны, клиенты бот-сетей и т.д.);
- фишинг;
- использование атак типа Man-in-the-Middle для проведения подложных транзакций;
- внутренние атаки (для корпоративных клиентов);
- направленные атаки на клиентские места (опять же имеют смысл для корпоративных клиентов).

Соответственно, наиболее распространённые векторы атак на системы ДБО – это: хищение ключевой и/или аутентификационной информации с последующим ее использованием либо на месте, либо на удалённом компьютере; проведение транзакций непосредственно с компьютера клиента; подмена легитимных транзакций подложными.

Следует отметить, что одни виды мошенничества, такие как неправомерные операции по картам или каналам ДБО, являются вероятными рисками потерь, тогда как другие – кредиты и внутреннее мошенничество – в 95% случаев представляют собой фактические убытки. Потенциальные потери для канала ДБО банка из ТОП 15 в случае успешной реализации всех попыток мошенничества составляют 300–450 млн руб. в год, объем неправомерных CNP-операций (Card not present) – от 200 до 700 млн руб. в год в зависимости от применяемых технологий защиты.

Согласно результатам исследования «Лаборатории Касперского», проведенного среди 800 представителей финансовых организаций из 15 стран мира («Финансовые киберугрозы в 2016 году»), потери финансовых организаций от кибератак становятся все более ощутимыми: средний совокупный ущерб от одного инцидента достиг \$926 тыс. Помимо прямого ущерба эта цифра включает дополнительную расходы на заработную

плату персонала, привлечение внешних специалистов, репутационные издержки, упущенную выгоду, а также страховые выплаты и компенсации клиентам.

Самыми разорительными стали атаки на POS-терминалы: средний урон от них составил \$2,1 млн. Следом идут угрозы, связанные со взломом мобильных устройств (\$1,6 млн ущерба), и целевые атаки (\$1,3 млн).

Рост потерь вынуждает финансовые организации увеличивать расходы на кибербезопасность. Хотя основной причиной остается необходимость соблюдать требования регуляторов, 63% респондентов считают такое соответствие лишь отправной точкой в построении системы защиты. Другой фактор, который вынуждает компании увеличивать расходы в этой области, – усложнение инфраструктуры. Наконец, расходы на безопасность могут увеличиваться, когда компания осознает недостаточность собственных знаний в этой области, а также по указанию руководства или из-за расширения бизнеса. Резюмируя, можно сказать, что объем средств, выделяемых на информационную безопасность, будет расти и в дальнейшем: в этом уверены 83% опрошенных.

Средний годовой бюджет банков, который они тратят на кибербезопасность, достигает \$58 млн: это в три раза больше, чем у нефинансовых организаций. В большинстве случаев подобные траты оправдываются: представители банков сообщают о значительно меньшем количестве компьютерных преступлений, чем компании такого же размера в других отраслях.

Рост вложений в киберзащиту имеет веские основания: в последние несколько лет количество угроз для финансовой индустрии неуклонно растет, они становятся все более сложными и чреваты серьезными последствиями, указали в компании. Так, 70% банков сообщили о том, что за последний год они понесли денежные потери в результате кибермошенничества. Больше всего опасений вызывают риски, связанные с мобильным банкингом: 42% респондентов считают, что в ближайшие три года им будет пользоваться подавляющее число клиентов, в то время как уровень киберграмотности пользователей останется низким. Это грозит увеличением количества инцидентов, связанных с кражей денег через мобильные устройства.

Среди других актуальных угроз для пользователей банки выделили фишинг: с ним в 2016 г. сталкивались клиенты 46% компаний. Еще одна сфера повышенного риска — банкоматы. Причем всего 19% банков обеспокоены угрозой атак на них, в то время как в 2016 г. объем вредоносного ПО для банкоматов вырос на 20% по сравнению с 2015 г.

По информации «Лаборатории Касперского», неосторожность пользователей и возрастающее количество атак заставляют банки пересмотреть приоритеты по обеспечению безопасности: 61% участников исследования назвали улучшение защиты приложений и сайтов одним из главных приоритетов. На втором месте (52%) оказалось внедрение более надежных систем авторизации.

В своём стремлении защитить средства клиентов и собственную репутацию, банками были разработаны вполне действующие системы безопасности:

- использование логина и пароля;
- одноразовый пароль;
- электронная цифровая подпись (ЭЦП);
- виртуальная клавиатура (как защита от фишинга);
- USB-токены (или смарт-карты);
- антивирусные средства и пр.

В то же время, кибер-преступники постоянно разрабатывают технологии, пишут программы для обхода всех разрабатываемых банками средств защиты.

Наиболее распространенные сейчас атаки можно свести к 4 видам:

1. Хищение ключей ЭЦП с незащищенных носителей – наиболее простая и отработанная технология, при помощи которой до сих пор реализуется большинство атак на клиентов систем ДБО, хранящих ключи ЭЦП на Flash-дисках, дискетах, в папке на жестком диске и т.д.;

2. Хищение закрытых ключей ЭЦП из оперативной памяти – чуть более сложная атака, по сравнению с первой. Обычно применяется в случае использования клиентом средства защищенного хранения ключей ЭЦП, которое позволяет извлекать их из закрытой области памяти. (Хотя, безусловно данная атака действует и против ключей ЭЦП, хранящихся в обычном файловом виде).

3. Удаленное несанкционированное управление ключами ЭЦП непосредственно с компьютера клиента – одна из наиболее опасных и перспективных атак. Реализуется либо при помощи средств удаленного управления компьютером клиента (класса TeamViewer), либо с использованием удаленного подключения к USB-порту (технология USB-over-IP). Ограничением данной атаки является обязательное подключение носителя с ключом в момент ее проведения. Данная атака позволяет несанкционированно использовать, в том числе, и ключи ЭЦП, хранящиеся на устройствах неотчуждаемого хранения и аппаратной выработки ЭЦП.

4. Подмена документа при передаче его на подпись – наиболее сложный и наиболее опасный на сегодняшний день вид атак. В данном случае пользователь видит на экране монитора одну информацию, а на подпись отправляется другая. Параллельно могут быть подменены данные об остатках на счете, выполненных транзакциях и т.д. Сочетание традиционных методов защиты (аппаратные средства СКЗИ для хранения и выработки ЭЦП, одноразовые пароли и т.д.) бесполезны, так как пользователь не может видеть то, что он подписывает.

Также следует отметить, что каждая из четырех перечисленных технологий эффективна не только на своем уровне защиты, но и на всех более «простых».

Однако пока что говорить о полном решении проблемы защиты ДБО от мошеннических действий рано. Происходит это из-за следующих причин. С одной стороны, банковское сообщество достаточно разнородно и вследствие этого всегда останутся банки, которые не будут в состоянии внедрить в своих системах ДБО наиболее совершенные средства защиты. С другой стороны, вопрос использования или наоборот неиспользования средств защиты не всегда определяется только банком. На этот процесс влияет также и клиент, которому в одном случае средства защиты могут быть неудобны для использования (например, клиентам выполняющим пакетное подписание платежей), а в другом случае неприемлемы из-за их стоимости (например, клиентам - физическим лицам).

Очевидно, что в целом злоумышленников, нацеленных на извлечение прибыли, может остановить высокая цена ее достижения из-за повышения технической сложности или высокий риск привлечения к уголовной ответственности. С учетом отмеченной выше невозможности максимально защитить все системы ДБО и всех клиентов, у банковского сообщества остается только движение по пути обеспечения неотвратимости наказания для мошенников.

Ожидаемыми мероприятиями на пути обеспечения неотвратимости наказания за компьютерные преступления в сфере ДБО являются следующие мероприятия:

- совершенствование уголовного и уголовно-процессуального права в части касающейся компьютерных преступлений в сфере ДБО;
- определение Банком России правил взаимодействия кредитных организаций в момент совершения мошеннических платежей;
- сбор информации о мошеннических платежах в единый центр и распределение полученной информации по всем кредитным

- организациям (механизм схожий с предоставлением информации о подозрительных платежах в Росфинмониторинг в рамках закона 115-ФЗ);
- обеспечение развития отношений с правоохранительными органами и законодателями других стран в сфере противодействия компьютерным преступлениям в сфере ДБО.

Обеспечение неотвратимости наказания за мошенническую деятельность в сфере ДБО является безо всякого преувеличения задачей государственной важности. Сегодня подавляющее большинство платежей осуществляется через системы типа Интернет-банк. Как говорилось в начале статьи, банки помимо обычных платежей предоставляют с помощью систем Интернет-банка ряд других финансовых услуг и сервисов.

1. Бортников, Г.П., Седых А.Е. Интеграционный подход к управлению каналами доставки банковских продуктов [Текст] / Г.П. Бортников, А.Е. Седых // Управление в кредитной организации. - 2010. - № 5.
2. Ваганова О. В. Моделирование интеграционных отношений субъектов инновационного процесса / О. В. Ваганова // Вестник Астраханского государственного технического университета. Серия: Экономика. – 2012. – № 2. - С. 122–130.
3. Крылов А. Анализ стратегий продвижения банков в медианосителях [Электронный Ресурс] / А. Крылов / Городская Банковская газета. – Режим доступа к ресурсу: <http://banker.ru/analytics/manager/41/60497>
4. Отчет о развитии банковского сектора и банковского надзора в 2014 году [Электронный ресурс] / Центральный Банк Российской Федерации. Режим доступа: http://www.cbr.ru/publ/archive/root_get_blob.aspx?doc_id=9878
5. Титов А.Б., Ваганова О.В. Методический подход к определению перспективных отраслей региона в условиях турбулентности экономики // Сетевой научно-практический журнал Научный результат. – 2015. - № 3. – с. 56-63

Толстяков Р.Р., Гобунов И.Н.

Терминологический анализ понятия «вирусный маркетинг»

*Тамбовский государственный технический университет
(Россия, Тамбов)*

doi: 10.18411/sr-10-02-2018-36

idsp: 000001:sr-10-02-2018-36

Аннотация

В статье приведен анализ существующих трактовок понятия «вирусный маркетинг» в зарубежной и отечественной литературе. Выделены составляющие термина, на основании построенной терминологической матрицы проведено их ранжирование по частоте включения в авторские интерпретации термина.

Ключевые слова: вирусный маркетинг, социальные сети, медиа вирус, маркетинговая коммуникация.

Сегодня только ленивый не пишет о вирусном маркетинге и вирусных постах в социальных сетях. Многие видят в этом «панацею» маркетинговых коммуникаций, при этом тиражируя шаблонные фразы «заразить пользователя», «лавинообразное распространение», «эмоциональный самораспространяющийся контент» и т.д. Предлагаем рассмотреть термин «вирусный маркетинг» с научной точки зрения, а именно провести терминологический контент анализ данного понятия, описанный в научных публикациях российских и зарубежных ученых.

Выборка исследования составила более 40 публикаций, имеющих в названии, либо в ключевых словах фразу «вирусный», кроме этого наиболее интересны публикации (их оказалось не более 10) были подвергнуты перекрестному исследованию на предмет использованных в них библиографических источников.