

РИСКИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ КЛИЕНТОВ И ПУТИ ИХ СНИЖЕНИЯ

Т. П. Варламова

*Саратовский социально-экономический институт (филиал)
РЭУ им. Г. В. Плеханова, Россия
E-mail: taniavar@rambler.ru*

В представленной статье рассмотрены актуальная проблема снижения рисков банковского дистанционного обслуживания клиентов. В частности, рассматриваются некоторые наиболее часто встречающиеся на практике приемы сетевых атак на сайты и серверы кредитных организаций, а также способы неправомерного получения персональной информации пользователей систем дистанционного банковского обслуживания с целью получения дохода путем списания денежных средств клиентов с банковских счетов клиентов, а также пути снижения рисков ДБО.

RISKS OF THE REMOTE BANKING SERVICES AND WAYS OF THEIR REDUCTION

T. P. Varlamova

In the presented article considered issue of the day of decline of risks of bank remote service of clients. In particular, some are examined most often meeting in practice receptions of network attacks on web-sites and servers of credit organizations, and also methods of illegal receipt of the personal information of users of the systems of remote bank service with the purpose of receipt of profit by writing of monetary resources of clients from the bank accounts of clients, and also way of decline of risks.

В последнее время в российском сегменте сети Интернет участились сетевые атаки на сайты и серверы кредитных организаций, а также попытки неправомерного получения персональной информации пользователей систем дистанционного банковского обслуживания (пароли, секретные ключи средств шифрования и аналогов собственноручной подписи, ПИН-коды и номера банковских карт, а также персональные данные их владельца).

Наиболее распространенными являются распределенные атаки типа «отказ в обслуживании», при которых большое количество компьютеров (от нескольких сотен до сотен тысяч), программное обеспечение которых предварительно специальным образом дистанционно модифицируется лицами, предпринимающими попытки неправомерного получения персональной информации пользователей систем ДБО, по команде указанных лиц начинают одновременно направлять массовые запросы на атакуемый ресурс, серьезно нарушая либо полностью блокируя его работу. При этом владелец ресурса, как правило, не может самостоятельно, без помощи провайдера Интернета, восстановить работоспособность ресурса. Продолжительность атак может составлять несколько

суток, в течение которых оказывается невозможным ДБО множества клиентов кредитной организации, что может нанести прямой ущерб этой организации и ее клиентам.

В связи с изложенным Банк России считает целесообразным рекомендовать кредитным организациям включать в договоры, заключаемые с провайдерами Интернета, обязательства сторон по принятию мер, направленных на оперативное восстановление функционирования ресурса при возникновении нештатных ситуаций, а также ответственности за несвоевременное исполнение таких обязательств.

При совершении попыток неправомерного получения персональной информации пользователей систем ДБО клиентам кредитных организаций по системам электронной почты направляются сообщения, в которых под какими-либо предложениями (техническое перевооружение организации, обновление или сверка баз данных кредитной организации и т.п.) предлагается ввести с клавиатуры компьютера указанные коды в поля экранных форм в ходе имитируемых сеансов информационного взаимодействия с кредитной организацией (к примеру, через созданный дубликат ее web-сайта). Одновременно на компьютер клиента с web-сайта могут передаваться вредоносные программы, являющиеся компьютерными вирусами или «закладками», выполняющими в фоновом режиме работы скрытые функции, связанные с неправомерным получением персональной информации пользователей систем ДБО.

Наблюдаются случаи неправомерного получения реквизитов банковских карт при проведении операций через банкоматы. При этом используются накладные устройства на клавиатуру для ввода ПИН-кода или на устройство для приема карт в банкомат, а также специально приспособленные для этих целей «фальшивые» банкоматы, которые незаконно устанавливаются, как правило, в не контролируемых кредитными организациями местах и внешне не отличаются от банкоматов, используемых для ДБО клиентов кредитных организаций.

Неправомерно полученные различными способами реквизиты банковских карт используются для изготовления поддельных банковских карт, частично (так называемый «белый пластик») или полностью имитирующих подлинные. При использовании в банкоматах поддельные банковские карты предоставляют их обладателям все возможности подлинных банковских карт.

В целях неправомерного получения персональной информации пользователей систем ДБО заинтересованные лица используют также различные варианты телефонного мошенничества. В частности, отмечаются случаи направления мошенниками на мобильные телефоны клиентов кредитных организаций SMS-сообщений о необходимости позвонить по номерам телефонов, которые в действительности не принадлежат этим организациям. Также имеют место звонки клиентам с сообщением автоинформаторов о предоставлении продуктов и услуг банка с предложением нажать определенные клавиши на телефоне для подтверждения согласия в их приобретении и т.п. Тем самым клиенты банка провоцируются к вступлению в контакты с мошенниками, целью которых в том числе может являться получение конфиденциальной клиентской информации

(например, номера банковской карты и ПИН-кода).

В связи с изложенным Банк России обращает внимание кредитных организаций на необходимость распространения предупреждающей информации для своих клиентов, в том числе с использованием представительств в сети Интернет (web-сайтов), о возможных случаях неправомерного получения персональной информации пользователей систем ДБО. В состав такой информации целесообразно включать описание официально используемых способов и средств информационного взаимодействия с клиентами, а также описания приемов неправомерного получения кодов персональной идентификации клиентов, информации о банковских картах и мер предосторожности, которые необходимо соблюдать клиентам, пользующимся системами ДБО. В качестве подобных мер кредитные организации могли бы рекомендовать клиентам:

- исключить возможность неправомерного получения персональной информации пользователей систем ДБО (не передавать неуполномоченным лицам);

- осуществлять операции с использованием банкоматов, установленных в безопасных местах (в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.);

- не использовать банковские карты в организациях торговли и обслуживания, не вызывающих доверия;

- при совершении операций с банковской картой без использования банкоматов не выпускать ее из поля зрения;

- не пользоваться устройствами, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат;

- не использовать ПИН-код при заказе товаров либо услуг по телефону/факсу или по сети Интернет;

- при наличии возможности, предоставляемой кредитной организацией, использовать реквизиты карты одноразового использования (так называемой «виртуальной карты») для осуществления оплаты товаров либо услуг через сеть Интернет;

- пользоваться услугой SMS-оповещения о проведенных операциях с применением ДБО (в случае возможности получения такой услуги);

- осуществлять информационное взаимодействие с кредитной организацией только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные web-сайты/порталы, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, получаемых непосредственно в кредитной организации [1].

По оценкам исследовательской фирмы Group-IB, в России за прошедший год в области ДБО заработок злоумышленников составил около 900 млн долл. Столь внушительные цифры объясняются тем, что нынешние хакеры – давно уже не вундеркинды-одиночки. Это хорошо организованные сообщества со строго распределенными ролями: один пишет вредоносное ПО, второй рассылает троянские вирусы, третий совершает атаки, четвертый переводит украден-

ные деньги на заранее подготовленный счет, пятый их обналачивает. Наконец, существует и своя служба безопасности, которая следит за соблюдением конспирации и отражает нападки как конкурентов по криминальному бизнесу, так и правоохранителей. Такая специализация, кстати, имеет еще один плюс для злоумышленников: некоторых из них просто не за что привлекать к ответственности, поскольку с юридической точки зрения они занимаются вполне легальным делом. Большую часть всей криминальной прибыли делят между собой всего несколько группировок. Их далеко не тысячи. Средняя сумма покушения оценивается в 400 тыс. рублей. При этом себестоимость атаки чаще всего составляет около 30 тыс. рублей. Развитие мобильных платформ прибавляет головной боли службе безопасности. Веб-технологии развиваются уже более 20 лет, и в Сети давно существуют стандарты, рецепты решения типовых проблем, но все равно разработчики оставляют массу уязвимостей, несложно представить, какой вал уязвимостей обрушится на мобильные платформы. Но от внедрения мобильных платформ никуда не деться, их устанавливают все крупные банки. Проблем добавляет тот факт, что мобильных ОС много и нужно писать отдельное приложение для каждой.

Основная тенденция в сфере попыток взлома ДБО – это использование новых методов мошенничества на основе концепции *man-in-the-browser*, которая является продолжением и развитием концепции *man-in-the-middle*. Данная концепция заключается в том, что троян уже не похищает логин и пароль пользователя для входа личный кабинет, чтобы переслать информацию злоумышленнику. Тем более что большинство современных систем ДБО обеспечивают защиту от такого мошенничества путем использования одноразовых паролей, присылаемых из банка на мобильный телефон или генерируемых с помощью специальных токенов. Новые трояны манипулируют содержимым веб-страниц, отображаемых пользователю сервером банка. Например, троян ждет, пока пользователь зайдет в клиент-банк и выводит на экран фальшивое сообщение о том, что на счет клиента были ошибочно зачислены денежные средства и счет будет заморожен до тех пор, пока эти средства не будут перечислены обратно по указанным реквизитам. Коварная программа предлагает уже готовую форму для перевода с заполненными реквизитами. Продуманы все мелочи: сумма перевода определяется трояном автоматически, исходя из доступного остатка денежных средств. В этом случае стандартные средства защиты от мошенничества не срабатывают и ухищрения с аутентификацией бессмысленны, поскольку пользователь сам совершает операцию. К примеру, о таком виде мошенничества с использованием трояна *URL Zone* сообщила в прошлом году немецкая криминальная полиция – за 22 дня мошенникам удалось похитить почти полмиллиона долларов [2].

Разработчику трудно исправлять все уязвимости, поскольку у него и без того достаточно работы. И он часто перекладывает все проблемы ИБ на плечи заказчиков. Практика показывает, что разработчики не готовы пользоваться современными средствами поиска «дыр», которые рекомендуются к обязательному применению. Как результат – в коде полно лазеек для хакеров. Кстати, что-

бы хоть как-то исправить столь неприятную ситуацию, некоторые крупные поставщики ПО платят деньги добровольцам за поиски уязвимостей в их продуктах. В частности Google официально заявил, что готов заплатить от 20 до 60 тыс. долл за каждый удавшийся взлом браузера Chrome. Аналогичным путем идут некоторые банки.

Помимо огрехов в программном коде, опасность представляют ошибки в архитектуре или сделанные при внедрении. В этом случае у мошенников опять появляется возможность обойти процесс аутентификации и провести нежелательную операцию со счетом клиента. Более того, тут уже не спасут даже такие надежные средства, как токен с неизвлекаемым ключом, и даже токен со встроенным дисплеем.

Абсолютной защиты ДБО от злоумышленников не существует – как нет абсолютно надежной автосигнализации. Как известно, угонщики могут взломать даже сверхдорогую систему со спутниковым позиционированием – было бы время и средства. Однако средства для повышения уровня безопасности и снижения вероятности взлома существуют и их обязательно нужно применять.

Единственной относительно надежной стратегией, страхующей от мошенников, может быть отсутствие «порочащих» связей. В идеале это означает наличие отдельного компьютера, который используется только для банковских операций, браузер которого посещает только сайт ДБО банка, и из флешек к нему подключается только одна проверенная, не используемая ни для каких других целей, содержащая ключ ЭЦП пользователя. Понятно, что такое может позволить себе только приличных размеров организация. Для частных лиц тоже существует вариант – они могут использовать отдельную виртуальную машину, отвечающую всем вышеперечисленным требованиям, благо мощность современных компьютеров это позволяет, а ПО для запуска виртуальных машин или уже входит в состав ОС или стоит не очень больших денег.

Разумеется, это не означает отказ от использования современных средств защиты от внешних угроз – антивирусов, межсетевых экранов и средств обнаружения или предотвращения атак как для организаций, так и для домашних пользователей. Однако все эти средства не дают стопроцентной гарантии.

СПИСОК ЛИТЕРАТУРЫ

1. Риски ДБО. Синко-Банк. [Электронный ресурс]. URL: http://sinko-bank.ru/korporativnym_klijentam/internet_banking/riski_dbo/ (дата обращения 28.08.2019).
2. Риски дистанционного банк-клиента. Методы защиты, используемые российскими банками // CNEWS. 2018. № 60. С. 94-98.