Риски дистанционного банк-клиента

МЕТОДЫ ЗАЩИТЫ, ИСПОЛЬЗУЕМЫЕ РОССИЙСКИМИ БАНКАМИ

Несмотря на то, что банки уделяют серьезное внимание безопасности дистанционного обслуживания, эта сфера остается крайне уязвимой — только за прошлый год злоумышленники вывели безнаказанно 900 млн долл. С ростом популярности мобильных приложений эта цифра будет только увеличиваться. Виной тому во многом нерадивость разработчиков, допускающих многочисленные ошибки и оставляющих массу уязвимостей.

Дистанционное банковское обслуживание (ДБО) — давно уже must have для всех крупных и средних российских банков. Причины понятны: с одной стороны — продвинутые клиенты давно не хотят из-за каждой мелочи тащиться в отделение и предпочитают совершать транзакции через компьютеры, планшеты, смартфоны и другие популярные мобильные устройства. С другой — дистанционное обслуживание позволяет банку экономить на издержках. Операции выполняются информационной системой финансовой организации, экономится полезная площадь банковского офиса и рабочее время сотрудников.

По данным агентства Markswebb Rank & Report, сегодня в России 83% банков предоставляют клиентам удаленный доступ к счетам. При этом варианты дистанционной работы следующие: 80% доступа к счетам осуществляется через собственный веб-сайт; 18% — через веб-сайт партнера. Оставшиеся 2% предлагают пользоваться специального клиентским ПО. Не забыты и мобильные устройства: 52% банков предлагают сервисы SMS-банкинга и 27% — мобильного банкинга. В последнем случае 51% обеспечивает доступ к счету через мобильный сайт и в 49% — через мобильные приложения. 45% этих приложений написаны для Symbian, 32% — для iOS и 21% — для Android.

Естественно, что там, где происходит оборот денег, тут же появляются люди, желающие их неправомочным способом отобрать. Системы ДБО как наименее защищенные чаще всего подвергаются атакам хакеров. При этом злоумышленники всегда находятся «в тренде» и ловят модные тенденции на лету. К примеру, если в 2010 году под ОС Android создавалось всего 0,5% вредоносного ПО, нацеленного на взлом систем мобильного банкинга, то в 2011 году эта цифра подскочила до 46,7%. Android стал лидером печального рейтинга. И это при том, что ОС Android пока еще не завоевала лидерские позиции среди общего числа телефонов, находящихся в руках пользователей, — сказывается популярность Symbian, и — как следствие — все еще широкая распространенность этой платформы. Однако Android давно лидирует по продажам новых смартфонов, и мошенники уже развернули свою бурную деятельность. Справедливости ради отметим, что еще один фактор популярности вредоносных программ для Android — открытость платформы.

НАС ЖДУТ ВЕСЕЛЫЕ ВРЕМЕНА

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 трояны, третий совершает атаки, четвертый переводит украденные деньги на заранее подготовленный счет, пятый их обналичивает. 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.

По словам **Артема Сычева**, заместителя директора департамента безопасности «Россельхозбанка», большую часть всей криминальной прибыли делят между собой всего несколько группировок. «Их далеко не тысячи», — подчеркнул Сычев. По данным представителя «Россельхозанка» 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 безопасникам. «Веб-технологии развиваются уже более 20 лет, и в Сети давно существуют стандарты, рецепты решения типовых проблем, но все равно разработчики оставляют массу уязвимостей, — поделился наблюдениями **Илья Медведовский**, исполнительный директор Digital Security. — 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. Поэтому нас ждет «веселый» следующий год, будущее обещает быть очень тяжелым».

Алексей Раевский, генеральный директор компании Zecurion, ссылается на данные отчета RSA 2011 Cybercrime Trends Repost, согласно которым на сегодняшний день первое место в хит-параде инструментов для получения нелегального доступа к банковским счетам занимает троян Zeus. По информации аналитиков, он отвечает за 90% случаев банковского мошенничества в мире. «Лицензии на использование Zeus продаются за весьма внушительные суммы, клиентов, судя по всему, немало, функциональность совершенствуется от версии к версии. Существуют и конкуренты, которые предлагают сходный функционал. Такая конкуренция приводит к тому, что возможности вредоносного ПО по-

СИСТЕМЫ ЗАЩИТЫ ДБО ДЛЯ ФИЗИЧЕСКИХ ЛИЦ В КРУПНЕЙШИХ РОССИЙСКИХ БАНКАХ

Источник: CNews Analytics, 2012

Наиболее популярные средства ИБ в интернет-банкинге — пароль, логин и одноразовые пароли, по одному на каждую операцию. Различные дополнительные устройства — USB-токены, криптокалькуляторы широкого распространения не получили.

		Уникальный номер клиента (логин) и пароль	Виртуальная клавиатура	Одноразовые пароли для каждой операции		Используется ли USB-токен
1	Сбербанк	✓	–	✓	на распечатке из банкомата или по SMS (можно отключить)	
2	ВТБ 24	✓	–	✓	на скретч-карте	
3	Альфа банк	✓	✓	✓	высылается на мобильный телефон по SMS	
4	Газпромбанк	✓	–	✓	распечатка из банкомата, SMS или специальное приложение устанавливаемом на мобильном телефоне	✓
5	Россельхозбанк	✓	–	✓	на скретч-карте	
6	Банк Москвы	✓	–	✓	по SMS	✓
7	Юникредит банк	✓	–	✓	на скретч-карте	
8	Росбанк	✓	✓	✓	(или вместо одноразовых паролей — аналог собственноручной подписи (АСП)	
9	Раффайзен банк	✓	✓		аналог собственноручной подписи (АСП)	
10	Промсвязьбанк	✓	–			
11	НОМОС–Банк	✓	–		АСП, для генерации кодов – специальный криптокалькулятор	
12	Уралсиб	✓	✓			✓
13	Транкредитбанк	✓	–	✓	(на SMS)	
14	МДМ банк	✓	–	✓	(на SMS)	
15	Банк «Санкт–Петербург»	✓	–	✓	(на SMS)	
16	Ак Барс	✓	–	✓	(распечатка из банка)	✓
17	Сити–банк	✓	✓		Нет	
18	Нордеа банк	✓	–	✓	на скретч-карте	
19	Московский кредитный банк	✓	–	✓	на скретч-карте	
20	Ханты–Мансийский банк	✓	–	✓	распечатка из банка или генерация одноразовых паролей на мобильном телефоне пользователя	
21	Петрокоммерц	✓	–	✓	распечатка из банка	
22	Зенит	✓				
23	Связь–Банк	✓	–	✓	на скретч–карте	
24	Русский стандарт	✓	✓	✓	по SMS (можно отключить опцию)	
25	Национальный банк «Траст»	✓	–	✓	на скретч–карте	

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.

стоянно растут, предлагаются новые функции и методы взлома. Это согласуется и с данными МВД, согласно которым ежегодный прирост числа попыток взлома составляет 30–50%, а сумма причиненного ущерба — в 2–2,5 раза», — отметил Раевский.

ГДЕ ЛЕЖАТ ДЕНЬГИ?

Алексей Синцов, руководитель департамента аудита ИБ компании Digital Security описал наиболее частые объекты атаки хакеров. «Где лежат деньги? — задался вопросом Синцов. — Где злоумышленник может заработать? Всего таких мест пять: это банковские пластиковые карты, ДБО, обслуживание торгово-сервисных предприятий (ТСП), процессинг (интернет-эквайринг) и АБС (автоматизированная банковская система). Так вот, самыми интересными областями для взломщиков является ДБО и АБС».

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.

ДЫРЫ В ЗАЩИТЕ

Приведенный пример — образец классического «фишинга». Однако троянами и фишерами нападения на банковские системы не ограничивается. Еще одна весьма перспективная с точки зрения злоумышленников область — эксплуатация уязвимостей и ошибок в ИТ-архитектуре системы.

По утверждению Алексея Синцова, в 90% отечественных ДБО были и есть такие уязвимости, как XSS (Cross Site Scripting — «межсайтовый скриптинг»), поэтому атаки типа CSRF (Cross Site Request Forgery — «подделка межсайтовых запросов») — весьма распространенное явление. Преимущество CSRF для хакера — у него отпадает необходимость внедрять в систему троян. «Почти всегда найдется скрипт в каком-либо приложении, которое работает одновременно с ДБО, но не требует аутентификации. Как результат — систему можно взломать», — заметил Синцов.

«Разработчику трудно исправлять все уязвимости, поскольку у него и без того работы выше крыши, — пояснил далее эксперт Digital Security. — 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, чтобы 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. В частности украинский «Приват-банк» готов платить за поиск уязвимостей в его ИТ-системе. Чего не скажешь о российских программистах. «От наших разработчиков даже благодарности не дождешься, они злятся, когда у них находят баги. Западники напротив, благодарят, потому что им выгод-

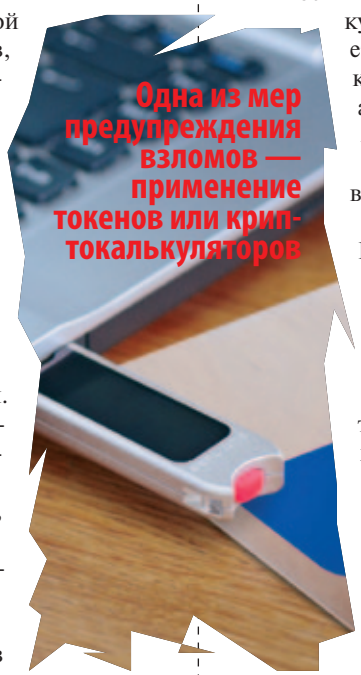
но, чтобы система была как можно лучше защищена», — заключил Синцов.

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.

ПОРОЧАЩИХ СВЯЗЕЙ НЕ ИМЕЕТ

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 более-менее надежной стратегией, страхующей от мошенников, может быть отсутствие «порочащих связей», — считает Алексей Раевский. — 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. Но 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.



Одна из мер предупреждения взломов — применение токенов или криптокалькуляторов

Но, разумеется, это не означает отказ от использования современных средств защиты от внешних угроз — антивирусов, межсетевых экранов и средств обнаружения или предотвращения атак для организаций. Все это существует и для домашних пользователей. Опять же надо понимать, что все эти средства отнюдь не панацея и не дают стопроцентной гарантии.

Если же не использовать отдельную виртуальную или реальную машину, то следует соблюдать ряд мер предупреждения взломов. Прежде всего, обязательно нужно задействовать второй независимый канал связи, например отсылку SMS на телефон держателя счета. Другой вариант — применение токенов или криптокалькуляторов. Хотя, как раньше уже было сказано, защиту токена можно обойти, все равно их применение повышает шансы оборониться от злоумышленников. Еще более надежную защиту предлагает токен со встроенным дисплеем — операции со счетом синхронно отображаются на его экранчике и внимательный пользователь без труда отследит расхождения с тем, что высвечивается на экране ПК.

НАЧАТЬ С РАЗРАБОТЧИКА

В распоряжении производителей ПО также есть немало средств повышения антихакерской защиты. К ним относятся, например, технология ASLR (Address Space Layout Randomization). При ее использовании случайным образом изменяется расположение в адресном пространстве процесса важных структур, а именно: образа исполняемого файла, подгружаемых библиотек, кучи и стека. Как результат ASLR значительно усложняет проникновение через несколько типов уязвимостей. Например, если при помощи переполнения буфера или посредством другого метода атакующий получит возможность передать управление по произвольному адресу, ему нужно будет угадать, где же именно расположен стек или другие места в памяти, куда он может поместить шелл-код. Сходные проблемы у хакера возникнут и при атаке типа «возврат в библиотеку» (return-to-libc), так как атакующий не знает адреса, по которому загружена библиотека. Если ему не удастся угадать правильный адрес, приложение, скорее всего, аварийно завершится, тем самым лишив атакующего возможности повторной атаки и привлекая внимание системного администратора.

Еще одна полезная технология — DEP (Data Execution Prevention — предотвращение выполнения данных). Эта функция безопасности встроена в семейство ОС Windows, она не позволяет приложению исполнять код из области памяти, помеченной «только для данных». Таким образом удается предотвратить некоторые атаки, которые, например, сохраняют код в области для данных с помощью переполнения буфера.

Также корпорация Microsoft ввела в своих продуктах новый функционал безопасности под названием «Защита от перезаписи обработчика структурных исключений» (SEHOP).

Сам по себе функционал SEHOP не очень надежно защищает от переполнения буфера в стеке. В то же время, решение весьма эффективно в связке с ASLR и DEP.

Однако есть еще один момент, который расхолаживает разработчиков и не вызывает у них желания вычищать свои приложения от возможных уязвимостей. Как утверждает Артем Сычев из «РоссельхозБанка», нынешнее законодательство не способствует решению проблем с безопасностью ДБО, поскольку вся ответственность перекладывается непосредственно на клиента.

С ним соглашается Алексей Раевский: «В любом случае клиентам банков стоит помнить, что безопасность — это комплексное мероприятие и проявление беспечности в этом вопросе может стоить дорого в прямом смысле, поскольку все договора на удаленное банковское обслуживание составляются, как правило, не в пользу клиентов и вернуть или компенсировать похищенные деньги за счет банка практически невозможно».