ИСТОРИЯ ОДНОЙ КРАЖИ

Сегодня многие российские банки предлагают своим клиентам возможность дистанционного управления счетом через интернет или пери помощи телефона. Системы дистанционного обслуживания пользуются неизменным спросом, так как избавляют вас от необходимости посещать офис: с их помощью вы можете в любое время получать текущую информацию о состоянии счета, а также совершать банковские операции по счету.

Главное требование, предъявляемое к автоматизированным системам дистанционного обслуживания, - это обеспечение конфиденциальности и надёжной защиты информации, передаваемой в ходе электронных расчетов. Банки используют различные технологии, стремясь максимально защитить клиента от несанкционированного доступа к счету или потери информации. Но удаётся им это далеко не всегда.

В этой статье мы рассмотрим гипотетический пример одной кражи и те ошибки, которые были допущены самим банком и его клиентом. А также - приведём схему, по которой действовал злоумышленник, и рассмотрим возможные пути защиты от подобных преступлений.

КРАЖА

Главный бухгалтер компании N, выйдя из очередного отпуска, обнаружила пропажу значительной суммы денег с расчётного счёта, открытого в банке М. В то утро, войдя в никогда не запирающуюся комнату бухгалтерии и проверив, что флэшка с закрытым ключом электронной цифровой подписи (ЭЦП) находится в USB-порту системного блока, она включила компьютер. При входе в операционную систему ввода пароля не потребовалось – системный администратор поддался-таки на уговоры главного бухгалтера и отключил опцию проверки, так сильно ей мешавшую. Привычно закрыв окно оповещения системы безопасности ОС о необходимости установки обновлений, главбух запустила систему «клиент-банк», чтобы выполнить платёж по выставленному компании счёту: руководитель ожидал проверку и попросил приобрести хотя бы несколько копий лицензионных операционных систем.

Отключить запрос пароля в «клиент-банке» было нельзя, но главбух придумала способ упростить запоминание периодически сменяемого пароля. Несложная схема заключалась в том, что пароль вычислялся на основе даты и текущего месяца. Бухгалтер очень этим гордилась и даже несколько раз хвасталась своей смекалкой во время визитов в «курилку».

В момент проведения платежа пришёл отказ в связи с недостаточностью средств на расчётном счёте. В выписке о финансовых транзакциях быстро обнаружились несоответствия: во время отпуска главного бухгалтера от её имени было совершено несколько десятков мелких переводов на счета различных контрагентов, часть из которых сотрудничала с компанией N ранее, а часть была неизвестна. Сотрудник банка в телефонном разговоре подтвердил, что все платежи подписаны закрытым ключом ЭЦП и не являются результатом сбоя в системе. Руководитель компании, поставленный в известность о данном факте, принял решение не обращаться в правоохранительные органы – не хотелось предавать огласке неприятный инцидент.

Знакомый руководителя, имеющий соответствующие возможности, по его личной просьбе выяснил, что среди неизвестных контрагентов, в частности, было несколько так называемых фирм-однодневок. Достоверную информацию удалось получить об одной из них, зарегистрированной на некоего гражданина Х. Оказалось, что сам гражданин Х двумя неделями ранее обращался в правоохранительные органы по поводу утраты им паспорта.

Деньги, ошибочно перечисленные в адрес известных контрагентов, удалось вернуть, написав соответствующее письмо, однако существенная сумма была утрачена безвозвратно. Как выяснилось позже, странное, на первый взгляд, разделение финансовых потоков, имело простую цель – запутать следы. Знакомый руководителя вынес вердикт о том, что компания N стала жертвой мошенничества со стороны преступной группы, причём шансы найти её участников чрезвычайно малы, а без помощи правоохранительных органов – вообще равны нулю. Выяснить суть схемы, по которой действовали злоумышленники, также не удалось.

ОШИБКИ ПОЛЬЗОВАТЕЛЯ

Компания N попала в неприятную ситуацию во многом по своей вине, допустив ряд как организационных, так и технических ошибок.

Так, в программе «клиент-банк», которая использовалась в организации N, разработчики реализовали два варианта аутентификации пользователей при входе: парольную и с использованием «таблеток» - специальных магнитных устройств с дополнительным считывателем типа Touch Memory (аналог тех, что используются в домофонах). Последние не являются по сегодняшним меркам достаточно безопасными, но в сравнении с парольной аутентификацией они гораздо надежнее. Главный бухгалтер же использовала пароли, которые представляли собой простые последовательности клавиш, набираемых «через одну», в сочетании с номером месяца: qetuo1, qetuo2 и т. д. Именно эта схема «вычисления» пароля и была предметом гордости главного бухгалтера: достаточно было бросить взгляд на настенный календарь, чтобы вспомнить текущий пароль. Однако, облегчив таким образом себе жизнь, главный бухгалтер облегчила задачу и злоумышленнику.

Одна из проблем нелицензионного программного обеспечения – невозможность получения своевременных обновлений, в том числе критических. К сожалению, использование пиратского ПО пока продолжает оставаться обычной практикой. Впрочем, как и замалчивание инцидентов в области информационной безопасности. В приведённом примере злоумышленниками нанесён прямой ущерб организации, а решение руководителя не придавать огласке случившееся фактически наносит косвенный ущерб потенциальным жертвам преступников. Ведь после успешно проведенной мошеннической операции они вполне могут повторять её снова.

Не закрывающаяся дверь и легкодоступный носитель закрытого ключа в рассмотренной ситуации - ещё две существенные ошибки. Стоит заметить, что на рынке давно уже присутствуют носители, простое копирование данных с которых затруднено необходимостью ввода ПИН-кода, а копирование закрытых криптографических ключей невозможно в принципе. Речь идёт о смарт-картах и электронных USB-ключах, иначе называемых токенами (см. рис 1). Работу с ними поддерживают ряд систем «клиент-банк», однако пользователи нередко предпочитают экономить и применять более дешёвые варианты.

РИС.1. ТОКЕНЫ ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ И НАДЕЖНОГО ХРАНЕНИЯ ЗАКРЫТЫХ КЛЮЧЕЙ ЭЦП.

ОШИБКИ БАНКА

С одной стороны, мысль о том, что банки сами должны быть заинтересованы в сохранности денег своих пользователей, кажется очевидной. Ведь банк может позволить себе оплатить работу квалифицированных специалистов, которые разработают надёжную систему обеспечения безопасности для проведения платежей через интернет.

Но, с другой стороны, затраты на такую систему фактически будут оплачивать сами пользователи, и банки опасаются этого. Желая сделать услугу массовой, некоторые кредитно-финансовые учреждения предпочитают экономить на всём, в том числе, на информационной безопасности.

Высокий уровень сокрытия любых инцидентов лишь способствует увеличению количества слабозащищенных систем. При этом эксперты по информационной безопасности и аналитики давно твердят о том, что пользователи готовы перейти на использование токенов по примеру западных соседей, вот только далеко не каждый банк или платёжная система готовы им предложить эту возможность.

Уже упоминавшееся желание скрыть инцидент с кражей свойственно не только клиентам, но и самим банкам. Зачастую в спорных ситуациях проще вернуть клиенту похищенные деньги, чем доводить ситуацию до суда с риском прослыть ненадёжной структурой. Юристы давно это поняли и активно используют такое «слабое место» банков. Другой опасностью для банков и самих клиентов является использование носителей сомнительного качества. Нередки случаи, когда разработчик банковского программного обеспечения, частью которого является система «клиент-банк», предлагает носитель, созданный им самим или некоей «карманной» компанией. Формально полученный сертификат вполне может говорить о грамотных юристах или хороших лоббистах, но как быть с безопасностью? Действительно надёжный токен используют сотни тысяч компаний, а не несколько сотен клиентов банков, которым такая услуга фактически навязывается.

ТЕХНОЛОГИЯ ВЗЛОМА 1

Допущеные ошибки, безусловно, существенны, но без наличия главного действующего лица - злоумышленника - деньги сами по себе со счёта компании не пропали бы. Что же скрылось от глаз упомянутого знакомого нашего руководителя?

Недовольный своей зарплатой сотрудник компании N при получении очередных выплат подсмотрел, как бухгалтер вводит пароль. Сам пароль увидеть не удалось, но способ ввода стал ясен. Так как дверь в бухгалтерию никогда не закрывалась, ему даже не пришлось делать слепок ключа с беспечно оставленной бухгалтером связки. В пятницу, под конец рабочего дня, сотрудник проник в не опечатываемое и не охраняемое помещение и, загрузив специально подготовленный диск, создал в операционной системе новую учётную запись с правами администратора. Перезагрузив компьютер, он вошёл в систему от имени привилегированного пользователя и скопировал себе на жёсткий диск содержимое папки программы «клиент-банк» и нужные ключи реестра. Не забыл сотрудник и про копию закрытого ключа ЭЦП с флэшки, подключенной к лицевой панели системного блока.

Потом, изучив в спокойной обстановке файлы, злоумышленник определил, где и в каком виде программа хранит пароли от «клиент-банка». Нужно отдать должное разработчикам: пароли хранились не открыто, а в виде хэш-функций, т. е. программа сохраняла специальным образом вычисленную комбинацию пароля и при входе в систему проверяла соответствие введённого с клавиатуры пароля и эталонной комбинацией. Зная примерный алгоритм того, как главбух выбирает пароли, сотрудник написал несложный генератор и получил словарь возможных паролей. Далее осталось проверить, какая из полученных комбинаций даёт ту, что совпадет с эталонной. За несколько часов атаки методом перебора, он получил пароль главного бухгалтера.

На следующей неделе на своём рабочем месте сотрудник установил «копию» «клиент-банка» с теми же учётными записями и ключами шифрования, что использовались в программе главного бухгалтера. Установленный на рабочем месте злоумышленника сниффер (специальная программа для перехвата и анализа всего сетевого трафика) был настроен таким образом, чтобы видеть активность работы программы «клиент-банка» на рабочем месте бухгалтера. В те моменты, когда настоящий «клиент-банк» не работал, сотрудник осуществлял переводы на разные счета со своего рабочего места, используя уже имеющихся в системе контрагентов, а также случайных, реквизиты которых находил в интернете. Такой подход позволил надёжно замаскировать одну-единственную транзакцию, которую он совершил, указав реквизиты предварительно зарегистрированной фирмы-однодневки. Благо, объявления о такой «услуге» он без труда нашел в интернете.

ТЕХНОЛОГИЯ ВЗЛОМА 2

Настойчивость в достижении цели, хорошее знание работы компании изнутри, а также собственные навыки в области компьютерных технологий помогли злоумышленнику добиться успеха. Однако для кражи денег мог использоваться и менее рискованный способ.

Некто зарегистрировал на азиатском хостинге фишинговый (проще говоря, поддельный) сайт и разместил на нём единственную страницу - копию главной страницы банка М. Все ссылки с поддельного сайта вели на настоящий. Далее злоумышленник подготовил письмо с темой «Важно! Банк М. Повышение безопасности при использовании интернет-банкинга» следующего содержания:

«Уважаемый пользователь! Мы постоянно заботимся о повышении защиты транзакций, осуществляемых с использованием интернет-банкинга банка М. Пожалуйста, ознакомьтесь, с последними новостями на нашем сайте».

Письмо было выслано на основе корпоративного шаблона банка М и отправлено якобы с почтового ящика, принадлежащего банку. Попадая на поддельный сайт, посетители «заражались» троянской программой, которая устанавливалась незаметно для пользователя на его ПК, используя всё ту же уязвимость операционной системы, опубликованную несколько недель назад. Троянская программа выполняла незатейливые действия по копированию ключей шифрования программы «клиент-банка» и закрытых ключей ЭЦП пользователя с внешнего носителя при его подключении.

Собранная информация отправлялась злоумышленнику, после чего троянская программа полностью себя удаляла, не оставляя на компьютере пользователя никаких следов. Полученные данные злоумышленник использовал для перевода денег на различные счета. Делалось это автоматически в случайные промежутки времени с использованием анонимных прокси-серверов с чужих компьютеров, которые так же предварительно инфицировались другой версией троянской программы.

ЗАКЛЮЧЕНИЕ

Какой из двух вариантов взлома имел место – не так уж важно. Гораздо важнее то, что, несмотря на выдуманный пример, атаки и используемые для них технологии, к сожалению, вполне реальны.

Описанный в этой статье «клиент-банк» является вполне типичной, средне защищенной системой. На сегодняшний день, встречаются и гораздо менее безопасные решения, а вот более надёжных пока не так много. Точка зрения банков объясняется просто: чем система надёжнее, тем она дороже. К тому же времена пошли сложные, экономить нужно на всем.

И это, в принципе, правильно, только экономить нужно обдуманно. Хорошо известен золотой принцип информационной безопасности: стоимость средств обеспечения ИБ не должна превышать стоимости защищаемой информации. Подсчитать стоимость решения достаточно просто: например, цена одного токена, реализующего строгую двухфакторную аутентификацию, с учётом программного обеспечения вряд ли превысит 1500 – 2000 руб. Основной проблемой для банков становится правильное определение стоимости защищаемой информации. Упрощённо для её подсчёта необходимо построить модель угроз и правильно рассчитать вероятности их успешной реализации. С точки зрения банка, при краже денег клиентов даже в незначительном размере основные риски и основные потери будут репутационными. В самом деле, размер компенсации украденных с одного расчётного счёта денег гораздо меньше, чем упущенная выгода от не заключенных новых договоров на обслуживание или перехода существующих клиентов к конкурирующему банку. Парадокс же заключается в том, что сейчас банкам дешевле замолчать инцидент и нивелировать репутационные риски, чем заплатить за внедрение надёжного решения. Да и свою репутацию не все банки, видимо, так дорого ценят, раз до сих пор позволяют своим клиентам использовать пароли – в лучшем случае одноразовые, нанесённые на специальную скретч-карту.

Недостаточный уровень инвестиций в информационную безопасность - это существенный риск для любого бизнеса, превратившийся в опасную тенденцию современного рынка. По данным аналитического отчета компании IT Policy Compliance Group «Финансирование информационной безопасности и ИТ с учетом риска», выполненного на основе на опроса более 2600 фирм, 68 % из них недофинансируют информационную безопасность с учетом финансовых рисков и потерь. При этом риск утечки конфиденциальной информации занимает верхнюю строчку рейтинга: 19 % фирм каждый год имеют свыше 15 инцидентов потери или кражи данных, 68 % фирм работают с «нормальными» уровнями потерь, переживая в год от 3 до 15 таких инцидентов. Фирмы с наихудшими условиями расплачиваются за это

потерей и утечкой данных, эквивалентной 9,6 % годового дохода, а простои обходятся им почти в 3 % годового дохода.

До тех пор, пока обязательство о разглашении инцидентов информационной безопасности не будет вменено банкам законодательно, их клиентам остаётся надеяться на себя и, по крайней мере, максимально полно использовать те средства защиты, которые позволяет банк: не применять пароли, если есть поддержка Touch Memory, и не использовать Touch Memory, если есть поддержка аппаратных токенов.