Новые механизмы безопасности

info@bifit.com
+7 (495) 797-88-89

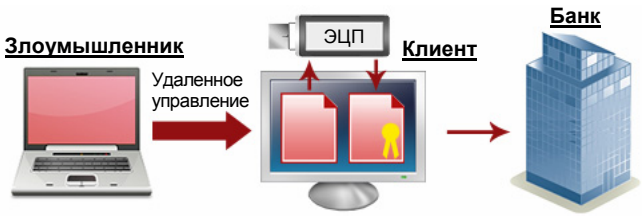
Новые угрозы

Весной 2010 г. в нескольких российских банках были зафиксированы первые попытки хищений в онлайне.

Во всех выявленных случаях злоумышленники пользовались халатностью клиентов, оставляющих USB-токен «iBank 2 Key» постоянно (круглосуточно) и бесконтрольно подключенным к компьютеру с доступом в Интернет.

С помощью вредоносных программ (троянов) со встроенным механизмом удаленного управления (RAdmin и др.) злоумышленники подключались к консоли инфицированного компьютера корпоративного клиента, запускали Web-браузер и загружали Java-апплет Internet-Банкинга.

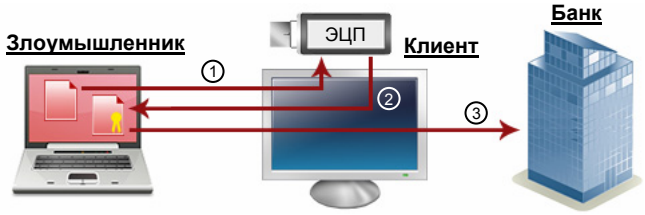
Далее с использованием ранее перехваченного долговременного пароля и постоянно подключенного USB-токена «iBank 2 Key» злоумышленники от имени клиента заходили в Internet-Банкинг, создавали платежные поручения, подписывали ЭЦП и отправляли в банк.



В ряде случаев корпоративным клиентам удавалось наблюдать процесс создания и подписи злоумышленниками платежных поручений у себя на мониторе.

Одновременно были зафиксированы попытки хищений с использованием троянов со встроенным механизмом удаленного доступа к USB-портам компьютера клиента.

При этом Java-апплет Internet-Банкинга загружался и исполнялся на компьютере злоумышленника, а для входа в систему «iBank 2» и формирования ЭЦП клиента под платежными документами использовался удаленный доступ к USB-портам компьютера клиента с постоянно подключенным USB-токеном (фазы 1 и 2).



Для преодоления механизма контроля доступа клиента с заданных IP-адресов троян осуществлял туннелирование TCP-трафика с компьютера злоумышленника до компьютера клиента внутри XMPP-трафика (Jabber и др.), производил трансляцию IP-адресов (NAT) и направлял TCP-трафик злоумышленника от клиента в банк (фаза 3).

Новые разновидности троянов не являются специфичными для системы «iBank 2» – удаленный доступ к USB-портам или удаленное управление компьютером клиента упрощают злоумышленникам задачу хищений в онлайне при работе клиентов **с любыми системами ДБО**.

Важно отметить, что ни в одном из инцидентов секретный ключ ЭЦП клиента не был похищен из USB-токена «iBank 2 Key». Благодаря применению USB-токенов и смарт-карт «iBank 2 Key» возможности злоумышленников по хищению средств сильно ограничены.

Как бороться

Для борьбы с новыми угрозами банкам рекомендуется:

- Информировать клиентов о новых угрозах и о необходимости строго соблюдать порядок работы в системе «iBank 2», в том числе о недопустимости постоянного и бесконтрольного подключения к компьютеру USB-токена и смарт-карты «iBank 2 Key»
- Использовать встроенные в систему «iBank 2» механизмы обнаружения подозрительных документов (фильтры по получателям, регионам и IP-адресам) и механизм идентификации компьютера корпоративного клиента (Device Fingerprint)
- Использовать на стороне банка внешние системы Fraud-мониторинга электронных платежей
- Использовать встроенное в систему «iBank 2» SMS-информирование клиентов о входе в систему, о поступлении в банк платежных документов, о движении средств по счетам клиентов
- Использовать встроенную в систему «iBank 2» расширенную многофакторную аутентификацию корпоративных клиентов (одноразовые пароли)
- Использовать встроенный в систему «iBank 2» механизм дополнительного подтверждения платежных поручений корпоративных клиентов одноразовыми паролями (дополнительно к ЭЦП)

Расширенная аутентификация

Расширенная многофакторная аутентификация корпоративных клиентов с использованием одноразовых паролей встроена в систему «iBank 2» начиная с версии 2.0.15.

Данный механизм поддерживается в Internet-Банкинге и Mobile-Банкинге при входе в систему, а также в PC-Банкинге при синхронизации.

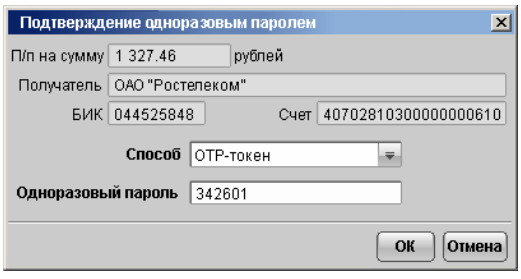
Дополнительное подтверждение документов

Дополнительное подтверждение платежных поручений корпоративных клиентов одноразовыми паролями встроено в систему «iBank 2» начиная с версии 2.0.22.

Данный механизм не заменяет ЭЦП, а является дополнительным подтверждением клиента под документом свыше пороговой суммы, настраиваемой банком индивидуально для каждого клиента.

После подписания платежного поручения необходимым количеством ЭЦП и при превышении пороговой суммы документ переходит в статус «Требует подтверждения».

Для доставки в банк такого документа корпоративному клиенту необходимо ввести одноразовый пароль.



Подтверждение одноразовым паролем в Internet-Банкинге может быть выполнено как сразу после подписания документа, так и позднее. В PC-Банкинге подтверждение документов выполняется в ходе синхронизации. Возможно подтверждение отдельного документа или группы документов. Ключевые реквизиты документов (количество, сумма, реквизиты получателя) отображаются в диалоге подтверждения.

Источники одноразовых паролей

В качестве источников одноразовых паролей в системе «iBank 2» используются SMS-сообщения и OTP-токены.

Привязка к корпоративным клиентам OTP-токенов и номеров мобильных телефонов для отправки SMS осуществляется только в АРМе «Администратор банка» при очном посещении клиентом банковского офиса.

К корпоративному клиенту может быть привязано произвольное количество OTP-токенов и номеров телефонов для отправки SMS. Один и тот же OTP-токен или номер телефона может быть привязан к нескольким корпоративным клиентам.

OTP-токены не привязываются к сотрудникам или ключам ЭЦП корпоративного клиента. Для входа в систему или подтверждения документа сотрудник корпоративного клиента может использовать любой телефон или OTP-токен, привязанный к его организации.

Использование SMS для получения клиентами одноразовых паролей позволяет банку максимально быстро и с минимальными затратами внедрить механизмы многофакторной расширенной аутентификации и дополнительного подтверждения документов.

К недостаткам SMS относится возможность задержки доставки сообщения по вине сотового оператора. Это может привести к невозможности для клиента оперативно войти в систему и совершить важные платежи.

OTP-токены обеспечивают гарантированное получение одноразового пароля. Клиент может приобрести у банка OTP-токены в том количестве, в котором это диктуется удобством и порядком работы организации.

SMS-Центр «ИБАНК2.РУ»

Наиболее простым способом организации отправки SMS-сообщений с одноразовыми паролями является подключение банка к SMS-Центру «ИБАНК2.РУ».

Поддержка SMS-Центра «ИБАНК2.РУ» встроена в систему «iBank 2», обеспечивает максимальную простоту подключения банка и защищенность взаимодействия.

SMS-Центр «ИБАНК2.РУ» размещен в Дата-центре на ММТС-9 и взаимодействует напрямую с SMS-Центрами российских сотовых операторов, что обеспечивает высокую производительность и надежность.

Ежемесячная абонентская плата при подключении к SMS-Центру «ИБАНК2.РУ» составляет 1050 руб. без учета НДС и включает в себя 3000 предоплаченных SMS по России. Стоимость одного SMS по России при превышении данного количества – **35 коп. без учета НДС**.

Возможно подключение к SMS-Центру «ИБАНК2.РУ» в режиме опытной эксплуатации на срок 2-3 месяца с предоставлением 1000 бесплатных SMS в месяц. По вопросам подключения к SMS-Центру обращайтесь по e-mail: info@ibank2.ru и тел. +7 (495) 797-88-89.

OTP-токены

Для расширенной многофакторной аутентификации корпоративных клиентов и дополнительного подтверждения платежных поручений одноразовыми паролями в систему «iBank 2» встроена поддержка OTP-токенов VASCO Digipass Go3 и ActivIdentity Mini OTP Token.

VASCO Digipass Go3 генерирует одноразовый пароль как функцию от времени и секретного ключа токена (time-based). Используется криптоалгоритм 3DES. Длина одноразового пароля составляет 6 цифр.

ActivIdentity Mini OTP Token генерирует одноразовый пароль как функцию от времени, значения счетчика состояния и секретного ключа токена (time-based + event-based). Используется криптоалгоритм 3DES. Длина одноразового пароля составляет 8 цифр.

Срок жизни OTP-токенов составляет 5-7 лет.

Для поддержки OTP-токенов компания «БИФИТ» заключила с ActivIdentity и VASCO Data Security эксклюзивные лицензионные соглашения о встраивании и распространении в составе системы «iBank 2» соответствующих программных компонент указанных вендоров.

Благодаря этому банки, приобретающие у компании «БИФИТ» OTP-токены для использования в системе «iBank 2», избавлены от необходимости приобретать ПО вендоров ActivIdentity 4TRESS Authentication Server или VASCO IDENTIKEY Server с лицензионной политикой per-user и стоимостью в десятки/сотни тысяч долларов.

Для осуществления официального ввоза OTP-токенов в РФ компания «БИФИТ» получила в ФСБ РФ все необходимые разрешительные документы (нотификации).

OTP-токены VASCO Digipass Go3 и ActivIdentity Mini OTP Token официально закуплены и импортированы компанией «БИФИТ». OTP-токены поставляются со склада компании в Москве партиями от 10 штук.

Для партий до 2000 штук цена за один OTP-токен – **413 руб. с учетом НДС**. По вопросам приобретения OTP-токенов обращайтесь в компанию «БИФИТ» по e-mail: info@bifit.com и тел. +7 (495) 797-88-89.

Планы по развитию

В ближайших версиях системы «iBank 2» планируется:

- Встраивание для корпоративных клиентов поддержки скретч-карт и конвертов одноразовых паролей
- Встраивание поддержки механизма EMV CAP на базе внешнего Сервера Аутентификации Thales SafeSign и аппаратного криптомодуля Thales HSM
- Встраивание поддержки MAC-токенов ActivIdentity и VASCO Digipass для подтверждения документов MAC (Message Authentication Code генерируется на основании вводимых в MAC-токен критичных реквизитов документа и секретного ключа MAC-токена)
- Система Fraud-мониторинга электронных платежей