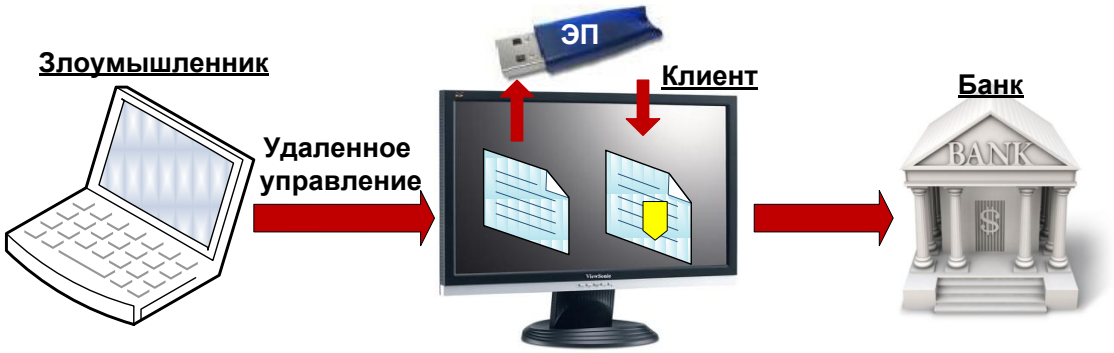
Уважаемые клиенты АО «СЕВЗАПИНВЕСТПРОМБАНК»

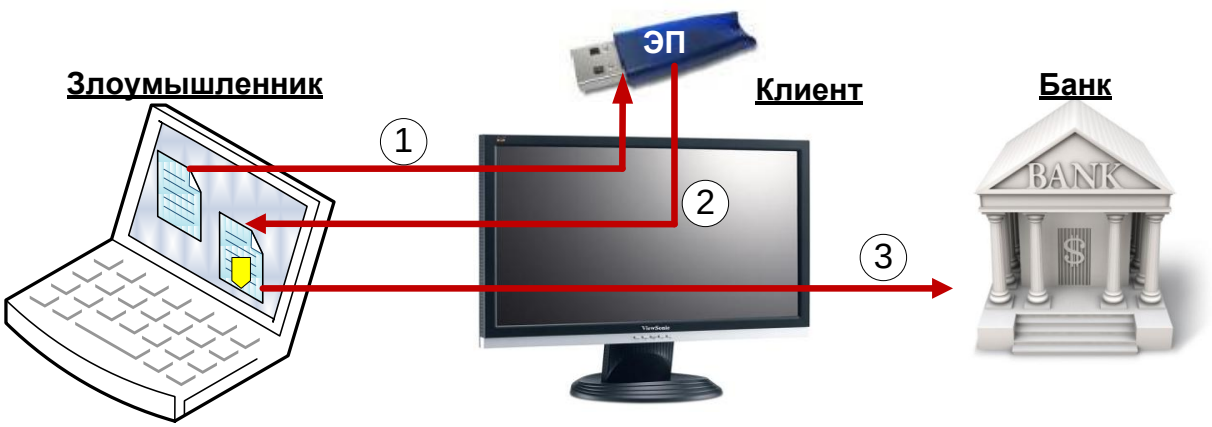
По данным нескольких российских банков были отмечены попытки хищения денежных средств у клиентов.

В большинстве случаев злоумышленники пользовались халатностью клиентов, не соблюдающих требования безопасности (своевременные обновления системы, антивирусного ПО и т.д.), а также оставляющих USB-токен «iBank2 key» бесконтрольно подключенным к компьютеру с доступом в Интернет, в частности:

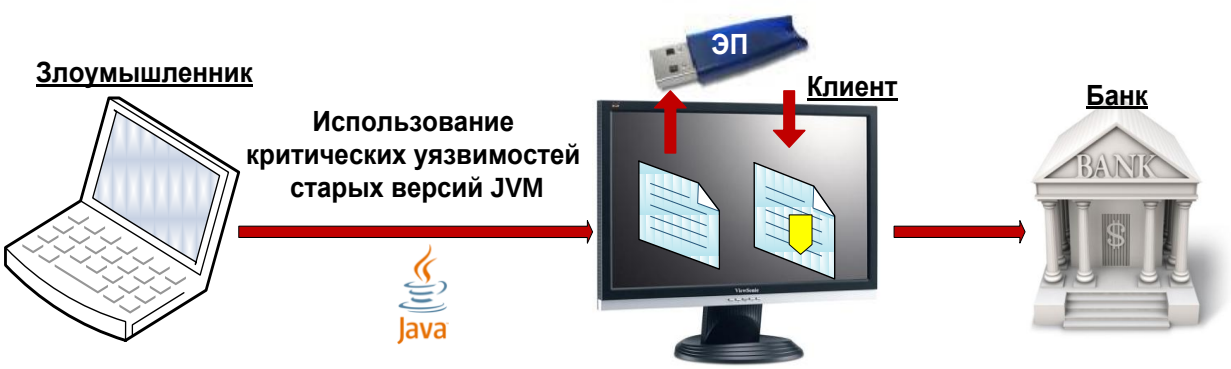
1. С помощью вредоносных программ (троянов) со встроенным механизмом удаленного управления злоумышленники подключались к консоли инфицированного компьютера корпоративного клиента, запускали браузер и загружали Java-апплет Интернет-Банкинга. Далее с использованием ранее перехваченного долговременного пароля и постоянно подключенного USB-токена «iBank2 key» злоумышленники от имени клиента заходили в Интернет-банкинг, создавали платежные поручения, подписывали ЭП и отправляли в банк.



2. Были зафиксированы попытки хищений с использованием троянов со встроенным механизмом удаленного доступа к USB-портам компьютера клиента. При этом Java-апплет Интернет-Банкинга загружался и исполнялся на компьютере злоумышленника, а для входа в систему «iBank2» и формирования ЭП клиента под платежными документами использовался удаленный доступ к USB-портам компьютера клиента с подключенным USB-токеном.



3. Также были зафиксированы попытки хищений с использованием вредоносной программы, которая устанавливалась на компьютер клиента, используя критические уязвимости в старых версиях Java-машин (JVM). Вредоносная программа встраивалась в JVM, подменяла вызовы JVM для сокрытия мошеннических действий и предоставляла злоумышленнику удаленное управление компьютером клиента. С помощью новой вредоносной программы мошенническое платежное поручение создавалось, подписывалось ЭП клиента (с использованием подключенного USB-токена) и отправлялось в банк непосредственно с инфицированного компьютера клиента. При этом все мошеннические действия выполнялись невидимо для пользователя.



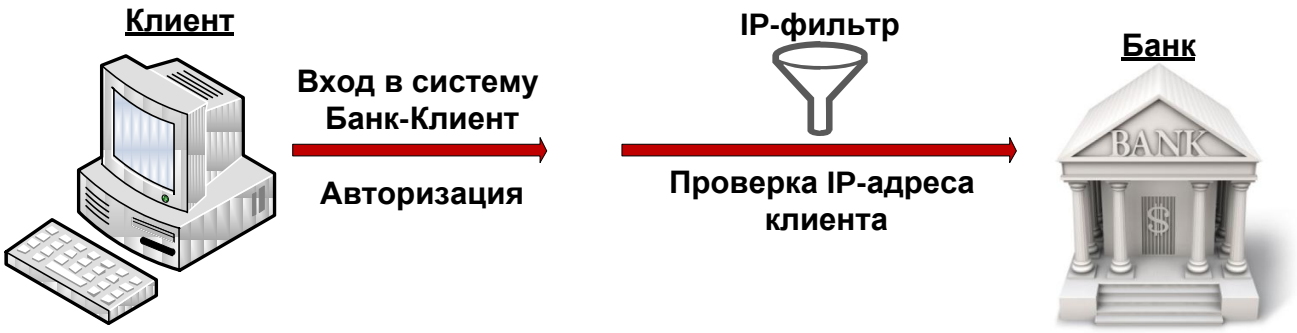
Методы защиты, предлагаемые клиентам АО «СЕВЗАПИНВЕСТПРОМБАНК»

Токены iBank2 key

Позволяют исключить копирование злоумышленником ключа ЭП клиента.

В АО «СЕВЗАПИНВЕСТПРОМБАНК» работа клиентов осуществляется исключительно с использованием токенов iBank2 Key.

Фильтр IP-адресов



Позволяет исключить возможность работы в системе Интернет-банк со сторонних IP-адресов. Это снизит вероятность работы злоумышленника с удаленным доступом к компьютеру клиента и использования его USB-портов.

Данную услугу можно подключить, обратившись в отдел по обслуживанию клиентов АО «СЕВЗАПИНВЕСТПРОМБАНК».

Дополнительное подтверждение документов

В системе iBank2 используется механизм дополнительного подтверждения платежных поручений корпоративных клиентов одноразовыми паролями через SMS (многофакторная аутентификация). Это позволит клиенту отслеживать исходящие платежные документы, а также обнаруживать несанкционированную отправку платежей вирусами и троянским программами, т.к. платежное поручение не будет проводится без подтверждения одноразовым паролем, полученным через SMS.

Услуга SMS-информирования бесплатна и ее можно подключить, обратившись в отдел по обслуживанию клиентов АО «СЕВЗАПИНВЕСТПРОМБАНК».

Отдел по обслуживанию клиентов: +7 (812) 622-11-60 (доб. 362, 363, 370)