Уважаемые клиенты!

В начале июля 2011г. в российских банках были зарегистрированы попытки хищения средств клиентов с использованием новой разновидности вредоносной программы.

Нативная компонента вредоносной программы 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 ЭЦП клиента (в том числе с использованием подключенного USB-токена) и отправлялось в банк непосредственно на инфицированном компьютере клиента.

При этом все мошеннические действия выполнялись невидимо для пользователя.

После отправки мошеннического платежа в банк вредоносная программа предпринимала действия по сокрытию попытки хищения:

- При работе на инфицированном компьютере мошеннический платеж не отображался в списке платежных поручений. При работе с обычного компьютера мошеннический платеж отображался.

- При работе на инфицированном компьютере операция списания средств не отображалась в выписке. При работе с обычного компьютера проводка отображалась.

- При работе на инфицированном компьютере остаток на счете модифицировался – не уменьшался на сумму мошеннического платежа. При работе с обычного компьютера отображался реальный остаток.

В результате действия вредоносной программы корпоративный клиент не мог с инфицированного компьютера обнаружить факт несанкционированного списания и оперативно помешать злоумышленнику осуществить вывод похищенных средств.

Для противодействия новой угрозе необходимо принять следующие меры:

- соблюдать правила безопасной работы в системе iBank 2;

- использовать только лицензионное системное и прикладное ПО, оперативно его обновлять;

- использовать и оперативно обновлять персональный межсетевой экран (firewall), антивирусное ПО, средства обнаружения вредоносных программ;

- подключать ключевые носители USB-токены к компьютеру только на время работы с системой iBank2;

- при использовании двух секретных ключей ЭЦП (ключ ЭЦП директора с правом первой подписи, и ключ ЭЦП главного бухгалтера с правом второй подписи) осуществлять работу с системой "iBank 2" на двух отдельных компьютерах с хранением секретных ключей ЭЦП на двух отдельных USB-токенах.

--