Утверждено
Решением Правления
ООО КБ «Центрально-Европейский Банк”
(протокол № 43/2017 от 01.12.2017г)

ПАМЯТКА
о рисках при работе в Системе «iBank2»

Настоящим Коммерческий Банк “Центрально-Европейский Банк” (общество с ограниченной ответственностью) информирует Вас о повышенном риске при использовании системы дистанционного банковского обслуживания (далее – ДБО) и о возможных рисках несанкционированного доступа к персональной информации пользователей систем ДБО: логинов, паролей, ключей электронных подписей.

Анализ выявленных случаев хищения денежных средств с расчетных счетов Клиентов, проведенный Центральным банком Российской Федерации совместно с уполномоченными органами, показал, что хищения осуществляются:

- ответственными сотрудниками Клиентов, имевшими доступ к носителям ключевой информации (далее - НКИ) и ключам ЭП. Как правило, это уволенные руководители, бухгалтеры и их заместители, а также совладельцы организаций;
- штатными ИТ-сотрудниками Клиентов, имевшими технический доступ к НКИ, а также доступ к электронным устройствам Клиента (персональные компьютеры, ноутбуки, планшетные компьютеры и т.п.), с помощью которого осуществляется работа в системе дистанционного банковского обслуживания;
- нештатными, приходящими по вызову ИТ-специалистами, обслуживающими электронные устройства Клиентов, с которых осуществлялась работа в системе дистанционного банковского обслуживания (далее – ЭУ), в том числе специалистами, осуществляющими профилактику и подключение к сети Интернет, установку и обновление бухгалтерских и информационно-правовых программ, установку, обновление и настройку другого программного обеспечения;
- злоумышленниками путем заражения через сеть Интернет ЭУ Клиентов вредоносными программами. Используя уязвимости системного и прикладного программного обеспечения, ЭУ Клиентов заражаются троянскими программами с последующим дистанционным похищением ключей ЭП Клиента и паролей. Также с помощью троянских программ злоумышленники могут получить удаленный доступ к ЭУ Клиента и соответственно к ключам ЭП Клиента.

Обращаем Ваше внимание на то, что в ряде кредитных организаций были зафиксированы попытки хищения денежных средств у Клиентов, использовавших устройства с неизвлекаемыми ключами электронной подписи - USB - токенами. Во всех выявленных случаях злоумышленники пользовались халатностью Клиентов, оставляющих USB-токен постоянно и бесконтрольно подключенным к ЭУ, имеющему доступ в сеть Интернет. С помощью вредоносных программ со встроенным механизмом удаленного управления (RAdmin, TeamViewer, VNC и др.) злоумышленники подключались к консоли инфицированного ЭУ Клиента, запускали Web-браузер и подключались к порталу кредитной организации. Далее с использованием ранее перехваченного пароля доступа и постоянно подключенного USB-токена злоумышленники от имени Клиента заходили в систему ДБО, создавали расчетные документы, подписывали их и отправляли в кредитную организацию.

Одновременно были зафиксированы попытки хищения денежных средств со счетов Клиентов с использованием вредоносных программ, обеспечивающих дистанционный доступ к USB-портам ЭУ Клиента. При этом вход в систему ДБО осуществлялся с компьютера злоумышленника, а работа с USB - токеном, подключенным к ЭУ Клиента, происходила дистанционно. Для преодоления механизма контроля доступа Клиента в систему ДБО с заданных IP-адресов вредоносная программа осуществляла туннелирование TCP-трафика с компьютера злоумышленника до ЭУ Клиента внутри XMPP-трафика (Jabber и т.п.), производила трансляцию IP-адресов (NAT) и направляла TCP-трафик злоумышленника от Клиента в кредитную организацию.

Кроме вышеперечисленных сценариев хищения денежных средств при использовании системы ДБО в российских банках были зарегистрированы попытки хищения денежных средств Клиентов с использованием новой разновидности вредоносной программы, нативная компонента которой устанавливалась на ЭУ Клиента, используя критические уязвимости в старых версиях Java-машин (JVM). Вредоносная программа не только предоставляла возможность дистанционного управления ЭУ клиента, но и подменяла вызовы JVM для сокрытия мошеннических действий.

Расчетный документ создавался от имени Клиента, подписывался и отправлялся в кредитную организацию непосредственно с инфицированного ЭУ Клиента. При этом все мошеннические действия и их результаты оставались скрытыми от Клиента:

- При работе на инфицированном ЭУ Клиента мошеннический платеж не отображался в списке расчетных документов. При работе с обычного ЭУ мошеннический платеж отображался.
- При работе на инфицированном ЭУ Клиента операция списания денежных средств не отображалась в выписке из счета Клиента. При работе с обычного ЭУ операция отображалась.
- При работе на инфицированном ЭУ Клиента остаток на счете модифицировался – не уменьшался на сумму мошеннического платежа. При работе с обычного ЭУ отображался реальный остаток.

В результате таких действий хищение денежных средств могло длительное время оставаться скрытым от сотрудников Клиента.