Защита систем дистанционного банковского обслуживания (Интернет-Банк, Клиент-Банк)

Число преступлений, связанных с системами ДБО, за последние несколько лет выросло многократно. При этом используемые банками меры защиты не являются непреодолимым препятствием для злоумышленников. Практика показывает, что кибермошенники могут вмешаться в процесс обработки платежных операций на любом этапе.

ООО «Финтэк»
Авторизированный сервисный центр
Доктор Веб
426057, г. Ижевск, ул. Свердлова, д.28
т. (3412) 56-94-78, 95-85-13, 60-94-95,
8912-761-15-60
e-mail: drweb@udm.ru
http://dr-web.su

1. С кем боремся?

За истекший год специалистами компании «Доктор Веб» было выявлено множество вредоносных программ, предназначенных для кражи пользовательской информации, в том числе данных для доступа к системам «Банк-Клиент» и электронным кошелькам.

Наиболее распространены и опасны **Trojan.Winspy**, **Trojan.Carberp, Trojan.PWS.Ibank, Trojan.PWS.Panda,** которые передают злоумышленникам данные, необходимые для доступа к банковским сервисам, умеет красть ключи и пароли от различных программ, отслеживать нажатия клавиш, делать снимки экрана, объединяться в сети, обрабатывать поступающие от удаленного командного центра команды и выполнять на зараженном компьютере.

Кроме того, банковские троянцы могут перенаправлять пользователя на поддельные(фишинговые) сайты для кражи пользовательских паролей и ключей.

В настоящее время банковские троянцы существуют для ВСЕХ операционных систем.

Заражение компьютера может происходить различными способами:

- Посещение зараженного сайта
- Перенос вирусов на внешнем носителе(флешка, внешний диск, плеер, телефон и т.д.)
- Заражение по локальной сети
- Скачивание и запуск зараженных файлов из сети Интернет
- Заражение через систему автообновления популярных программ

Кроме троянов для получения доступа к системам ДБО активно используются средства социальной инженерии. Например, рассылка от имени банков писем по электронной почте с требованием(под разными предлогами) перейти по предлагаемой ссылке, где требуется ввести логин и пароль от системы ДБО. Ссылка ведет на поддельный сайт со схожим дизайном, а логин и пароль оказываются в руках злоумышленников. Зафиксированы и адресные атаки мошенников на конкретные предприятия.

2. Как это происходит?

После заражения компьютера и получения доступа к нему производится поиск следов использования ДБО и сбор информации. Собранные данные передаются на управляющий сервер, где проверяются на полноту и достаточность для совершения мошеннической операции.

Если фальшивое платежное поручение не может быть отправлено с другого компьютера, то используются средства удаленного администрирования, что позволяет отправлять платежные поручения непосредственно с компьютера бухгалтера. Троянами может производиться подмена легитимных платежных поручений на мошеннические при отправке их на подпись, при этом пользователь видит на экране и подписывает свое платежное поручение,

Как только мошенническая операция проведена, и платежное поручение отправлено, главная задача злоумышленников – ограничить доступ пользователя к системе ДБО. Для этого компьютер пользователя приводят в неработоспособное состояние путем удаления компонентов Windows или форматированием жесткого диска. Для дополнительного отвлечения внимания часто удаляются данные бухгалтерских программ.

3. На что следует обращать внимание?

- необычно медленная работа компьютера, зависания во врем сеансов ДБО или при попытке входа, произвольная перезагрузка
- перебои с доступом в систему ДБО
- невозможность авторизации в системе ДБО

- несоответствие порядковых номеров платежных поручений
- попытки авторизации в ДБО с других IP-адресов или в нерабочее время.
- неоднократное удаление антивирусным монитором одного и того же вируса
- выход из строя ПК, на котором установлена система ДБО
- DDoS-атака на вашу ИТ-инфраструктуру

В случае обнаружении вирусов или сбоев в работе компьютера следует немедленно приостановить работу с ДБО и провести полную проверку компьютера антивирусным сканером. Повторяющееся заражение одним и тем же или схожими вирусами может свидетельствовать о том, что вирус уничтожается не полностью, какая-то его часть продолжает функционировать и загружает из Интернета обновленные вредоносные программные модули. В такой ситуации следует провести более детальный анализ вирусной активности. **Если самостоятельно не удается установить источник заражения, необходимо обратиться в Службу поддержки пользователей разработчика антивирусной программы.**

При работе с системой ДБО следует исходить из соображений, что данный сервис должен функционировать абсолютно бесперебойно, поэтому всякое отклонение от нормальной работы следует воспринимать как сигнал тревоги.

К примеру, если Вы не можете войти в систему ДБО в течении 5- 10 минут, обязательно свяжитесь с банком и установите источник проблемы(в банке или в вашей сети). Если проблема в вашем оборудовании или программах и Вы не можете её быстро разрешить или локализовать, обязательно свяжитесь с банком, проверьте последние отправленные поручения и сообщите сотрудникам банка об имеющихся проблемах.

4. Как с этим бороться?

Анализ происшедших инцидентов с ДБО позволяет сделать однозначный вывод о том, **что успеху злоумышленников способствует пренебрежение пользователями (а иногда и сотрудниками банка) элементарных правил безопасной работы с системами ДБО**. Типичный пример такого поведения – хранение ключей ЭЦП на жестком диске или постоянно подключенных к компьютеру флешках, токенах, отказ от дополнительных мер безопасности, предлагаемых банком.

Основные правила безопасной работы с ДБО.

- Хранить ключи ЭЦП на съемных носителях и извлекать их по окончании сеанса
- Не оставлять включенным сеанс ДБО сверх необходимого времени.
- На компьютере с системами ДБО ограничить работу в сети Интернет минимальным необходимым количеством сайтов.
- Не использовать на компьютере с ДБО средств удаленного доступа и администрирования.
- Доступ к ресурсам компьютера с системами ДБО из локальной сети должен быть закрыт, папок общего доступа быть не должно.
- Не устанавливать без особой необходимости системы ДБО на мобильные устройства, которые могут покидать офис и подключаться к другим сетям.
- На компьютере с системами ДБО желательно не использовать сеть Wi-Fi. В случае необходимости – устанавливать максимально возможный уровень защиты сети.
- Поддерживать систему антивирусной защиты в работоспособном и актуальном состоянии
- Не пользоваться ДБО в случае возникновения проблем с антивирусной защитой
- Не пользоваться ДБО при повторяющихся сбоях в работе компьютера

Технические аспекты защиты

- Должны быть установлены все актуальные обновления безопасности Windows
- Антивирусная защита должна включать, кроме обычных функций, модули проверки почты, входящего http трафика, Брандмауер, СПАМ фильтр и обновляться не реже одного раза в час. Желательно использовать Централизованное управление антивирусной защитой. Пользователь ДБО должен быть лишен возможности управления антивирусной защитой и возможности её отключения.
- На компьютере с ДБО не должно быть установлено программ не являющихся необходимыми на данном рабочем месте
- Обновление программ(Adobe Reader, браузеры и т.д) должно проводиться только вручную с официальных сайтов. Автообновление необходимо отключить.
- Пользователь не должен работать с правами Администратора

- Исключить прямой доступ в Интернет без использования межсетевого экрана
- Пользовательские пароли должны быть сложными и периодически изменяться
- Доступ к ресурсам сети Интернет должен быть ограничен фиксированным списком доверенных сайтов, не допускать использование месседжеров типа ICQ, Skype и др.
- Не допускать использования социальных сетей
- Использовать только корпоративную почту через почтового клиента.
- Использовать СПАМ фильтр с жестким ограничением
- Отключить службы сервера, удаленного доступа и др. связанные с удаленным администрированием.
- Применение внешних устройств должно быть ограничен набором флешек (Токенов) с ключами ЭЦП.

В случае если требования безопасности не могут быть выполнены в полном объеме на компьютере бухгалтера, необходимо взвесить риски и, возможно, принять решение о выделении отдельного компьютера для работы с ДБО. Именно такой вариант рекомендуется многими банками.

Учитывая тот факт, что **работники бухгалтерий не являются специалистами в области информационной безопасности**, они бывают недостаточно информированы о рисках и могут недооценивать необходимость дополнительных мероприятий по защите систем ДБО. Поэтому **разъяснение правил безопасной работы является одним из важнейших составляющих общей системы безопасности**.

Для повышения уровня ответственности и дисциплины, общие правила безопасной работы с ДБО следует оформить соответствующим приказом руководителя предприятия.

5. Если произошел инцидент

В случае обнаружения факта (или попытки) мошенничества необходимо максимально быстро сообщить о происшествии в банк с целью остановки платежа и блокирования доступа к системе ДБО.

Компьютер с системой ДБО необходимо выключить. Если в компании имеется межсетевой экран или прокси-сервер, на котором ведутся логи, то необходимо сохранить их на внешнем устройстве. В случае проведения самостоятельного расследования или привлечения для этих целей консультантов, следует иметь в виду что работа с оригиналами носителей информации может повредить целостности доказательств, хранящихся на них.

Даже если мошенничество не было завершено, и вы успели остановить его, инцидент остается уголовным преступлением, которое попадает под ряд статей, начиная с создания и распространения вредоносного программного обеспечения и заканчивая попыткой хищения в особо крупном размере. Поэтому следует обязательно написать заявление в правоохранительные органы с требованием возбудить уголовное дело.

6. Заключение.

На сегодняшний день **не существует ни одной системы ДБО со стопроцентной надежностью**, но само осознание этого факта и применение даже самых простых мер по повышению уровня безопасности может существенно снизить риски финансовых потерь. Необходимо понимать, что ежедневно появляются сотни новых вирусов и их модификаций и несмотря на то, что, например, обновление вирусных баз Dr.Web® выходят каждые тридцать минут, всегда есть риск заражения **новым вирусом**. Поэтому при выборе системы антивирусной защиты следует принимать во внимание не только стоимость, но и устойчивость антивируса к заражению неизвестными вирусами, а также наличие эффективной службы поддержки пользователей.

Учитывая, что **сумма ущерба может оказаться равной сумме остатка на расчетном счете**, необходимые затраты на повышение безопасности вероятно следует отнести к не самым плохим инвестициям

Подготовлено с использованием материалов Компании Доктор Веб.