ОАО «ЧЕЛЯБИНВЕСТБАНК»

Типичный сценарий хищения через систему ДБО и меры по снижению рисков несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств.

1. **Подготовка к заражению.**

   Злоумышленник размещает вредоносный код (далее «вирус») на популярных страницах интернета используя уязвимости серверов публикующих данные страницы. Как правило, используются тематические форумы бухгалтерской направленности, доски объявлений о покупке-продаже на «очень» выгодных условиях, объявления о «горящих путёвках».
   Целью злоумышленников является размещение «вируса» на максимально посещаемых сайтах. Кроме того, возможна рассылка как ссылок на заражённые страницы, так и непосредственно «вируса» через электронную почту (спам).

2. **Заражение.**

   Сотрудник предприятия, работающий с системой ДБО (для примера - бухгалтер), с компьютера с установленной системой ДБО посещает заражённый сайт в интернете, либо открывает заражённый документ, полученный по электронной почте. «Вирус», используя уязвимости операционной системы либо другого программного обеспечения (почтовый клиент, браузер), получает контроль над компьютером.

   Меры противодействия:

   1) **Не использовать компьютер с системой ДБО для работы с интернетом и электронной почтой.**
   2) **Использовать лицензионное программное обеспечение со свежими обновлениями, устраняющими уязвимости.**
   3) **Использовать антивирусное программное обеспечение со свежими обновлениями.**

3. **Связь со злоумышленником.**

   После получения контроля над компьютером, «вирус» сообщает хозяину-злоумышленнику об успешном заражении. Обычно для связи используются специальные интернет-сервера расположенные вне России. «Вирус» передаёт «хозяину» информацию об обнаруженных на компьютере системах ДБО, списки хозяйственных и бухгалтерских документов, баз, и прочих ценных данных вплоть до фотографий. Современные «вирусы» достаточно универсальны и «узнают» десятки распространённых систем ДБО. Злоумышленник получает возможность скачивать любые файлы и с компьютера, сетевых дисков, USB-носителей (флэшек), просматривать происходящее на экране и набираемое на клавиатуре (в т.ч. пароли). В случае обнаружения системы ДБО, известной вирусу, передаются номера счетов и остатки по ним, выписки, платёжные документы.

   Меры противодействия:

   1) **На межсетевом экране предприятия настроить запрет на взаимодействие компьютера с неизвестными интернет ресурсами (так называемый «белый список»).**
   2) **Внимательно относиться к подозрительной активности компьютера, сообщать системному администратору предприятия о странном поведении компьютера.**

4. **Кража.**

При наступлении подходящего случая для совершения преступления – в частности появления на счёте предприятия значимых средств, злоумышленник даёт команду «вирусу» осуществить платёж на свои реквизиты (обычно на счёт физического лица или фирмы «однодневки»). «Вирус» получив команду, ожидает появление ключа ЭЦП подключённого к компьютеру, создаёт платёжное поручение, подписывает ЭЦП (используя подключенный ключ и пароль подсмотренный ранее) и отправляет в банк.

Некоторые разновидности «вируса» подменяют реквизиты получателя в создаваемых платёжных поручениях, причём бухгалтер видит правильные реквизиты, а во время проставления ЭЦП реквизиты подменяются, и в банк уходит платёжное поручение с искажёнными реквизитами получателя.

В случае использование системы ДБО не известной «вирусу», возможно создание платёжного поручения злоумышленником в «ручном режиме» посредством дистанционного доступа – злоумышленник запускает систему ДБО (или использует уже запущенную), создает платёжное поручение и т.д. при этом на экране видны все действия мошенника – как двигается указатель «мышки», набираются символы. Но может всё скрываться запускаемым «хранителем» экрана или симуляцией «зависания» компьютера.

Меры противодействия:

1) **Не подключать ключ ЭЦП к компьютеру, кроме как для осуществления платежей.**
2) **Подключить СМС-уведомления о платежах.**

5. **Сокрытие следов.**

После отправки мошеннического платёжного поручения «вирус» может осуществлять сокрытие следов своей деятельности с целью отсрочки обнаружения кражи и затруднения последующего расследования преступления :

- сокрытие мошеннического платёжного поручения: платёжное поручение не отображается в списке отправленных, операция не отображается в выписке (но на другом, не заражённом компьютере с ДБО данные операции видны);
- маскировка искаженных реквизитов: в случае использования схемы с подменой реквизитов платежа, «вирус» при попытке просмотра/печати искажённых платёжных поручений подставляет обратно правильные реквизиты (на заражённом компьютере с ДБО будут видны реальные реквизиты получателя);
- уничтожение следов: «вирус» стирает следы своей деятельности в системе, все свои файлы, журналы работы и самоуничтожается - в результате компьютер выглядит как «чистый»;
- вывод компьютера из строя: от простого стирания информации на всех дисках компьютера, до симуляции ошибок в работе (в т.ч. с целью отвлечение внимания и времени на восстановление работоспособности компьютера).

Меры противодействия:

1) **Использовать регулярное резервное копирование.**
2) **После обнаружения попытки/факта кражи – немедленно выключить компьютер, сообщить в банк и обратиться в правоохранительные органы.**