Dr.WEB®
с 1992 года

Внимание, угроза:
банковские троянцы!

Один из сценариев заражения компьютера банковским троянцем

Реальный случай, который произошел в одной из московских компаний.

1. Бухгалтер с рабочего компьютера, на котором установлена система ДБО, читает в Интернете статьи на сайте о здоровье.
2. Браузер зависает, появляется окошко с предупреждением о некорректной работе программы.
3. Бухгалтер машинально жмет на одну из кнопок окошка, чтобы ей ничего не мешало читать важную статью.
4. Но браузер продолжает «висеть», и бухгалтер зовет системного администратора.
5. Системный администратор заходит на компьютер бухгалтера под своим администраторским ДОМЕННЫМ паролем и решает проблему с браузером — можно дальше читать важную статью. Троянец, который НЕЗАМЕТНО проник на компьютер бухгалтера с сайта о здоровье и был активирован самим бухгалтером (она нажала на кнопку в окошке браузера — см. п. 3), только этого и ждет — пароль ко всей сети банка уже в руках мошенников, равно как и пароль к системе ДБО.
6. Бухгалтер несколько дней не заходит в систему ДБО, а вместе с тем за это время совершено несколько мошеннических транзакций на миллионы рублей.

Банковскому троянцу, например, **Trojan.Carberp**, необходимо всего 1–3 минуты, чтобы похитить пароли и денежные средства со счета жертвы.

Что такое банковские троянцы?

Это исключительно вредоносные программы, которые могут:

- похищать пароли для доступа к банковским и платежным системам, а также деньги с банковских счетов компаний любого масштаба;
- загружать другие вредоносные программы, в том числе свои дополнительные модули;
- по удаленной команде злоумышленника полностью парализовать работу компьютера.

У многих банковских троянцев имеются версии модулей для кражи денег из всех распространенных систем дистанционного банковского обслуживания (ДБО).

Внимание! В связи с особенностями схемы, применяемой злоумышленниками для заражения, наибольшей опасности подвергаются компании малого и среднего бизнеса.

На сегодняшний день самыми опасными банковскими троянцами в мире считаются представители семейств **Trojan.PWS.Papras**, **Trojan.PWS.Panda** (также известные под именами Zeus и Citadel), и кроме того — разновидности самого маленького по размеру банковского троянца, **Trojan.PWS.Tinba**.

Новые модификации банковских троянцев семейства **Trojan.Carberp**, некогда считавшихся одной из наиболее распространенных угроз, в наши дни уже почти не встречаются, однако их место заняли опасные бэкдоры **BackDoor.Anunak**, созданные вирусописателями на основе исходных кодов Carberp.

Защита при помощи СМС с паролями — не панацея!

Считается, что защита банковских транзакций с помощью одноразовых паролей, присылаемых в СМС-сообщениях на «привязанный» к банковскому счету номер мобильного телефона (так называемая двухфакторная аутентификация), способна обезопасить пользователя системы банк-клиент от действий злоумышленников. Это давно уже не так! Киберпреступники научились успешно обходить такую защиту.

Один из сценариев обхода защиты с использованием одноразовых паролей

1. На компьютер проникает банковский троянец, способный встраивать в просматриваемые веб-страницы постороннее содержимое, то есть выполнять веб-инжекты.
2. При попытке жертвы зайти на сайт банка или открыть страницу банковского сервиса обосновавшийся на компьютере троянец подменяет содержимое этой страницы. Теперь на экране демонстрируется сообщение о том, что для продолжения работы с системой банк-клиент пользователь должен скачать и установить на свой мобильный телефон специальную банковскую программу. При этом оформление сайта и адрес веб-страницы в адресной строке браузера остаются неизменными и не вызывают никаких подозрений.
3. Жертва устанавливает на свой смартфон скачанное по ссылке приложение, которое на самом деле является мобильным банковским троянцем.
4. Мобильный троянец перехватывает отправляемые системой банк-клиент СМС с одноразовыми паролями и передает их злоумышленникам, а троянец, работающий на компьютере, с помощью этих паролей крадет деньги с банковского счета.

Что крадет банковский троянец?

Деньги.

Другое его владельцев не интересует.

Перед кражей владельцы троянца собирают информацию о жертве: они в любой момент времени знают состояние баланса компании до копейки, суммы и формулировки оснований перечислений (эти же формулировки потом используются в мошеннических платежках), мгновенно получают информацию обо ВСЕХ совершаемых бухгалтером компании платежах — перед опустошением счета за жертвой ведется круглосуточное наблюдение. Мошенники получают следующие данные:

Владелец троянца обладает полной информацией о счете жертвы и имеет доступ к любой информации на зараженном компьютере.

Если похищен пароль к ДБО

- Банковский счет
- Баланс счета
- Сумма перевода («залива»)
- Основание платежа
- Название скомпрометированной системы ДБО
- WWW-адрес системы ДБО
- IP-адрес компьютера жертвы
- Используемый браузер
- Другие сведения, необходимые для осуществления транзакции

Если скомпрометирована банковская карта

- BIN банка
- Счет клиента-жертвы
- Адрес системы электронных платежей, в которой была скомпрометирована карта
- Номер карты
- Дата окончания срока ее действия
- Имя и фамилия держателя
- В некоторых случаях - CVV2/CVC2

Кому это нужно?

Современные вредоносные программы разрабатываются вирусописателями-профессионалами, и это — хорошо организованный криминальный бизнес. В него вовлечены высококвалифицированные разработчики ПО.

Созданием и «продвижением» банковских троянцев занимаются организованные преступные группы: зачастую разработчики находятся в одной стране, серверы, с которых распространяется троянец, — в другой, организаторы — в третьей, «партнеры» — преступники, которые покупают услуги владельцев троянцев и обслуживающих их бот-сетей для совершения хищений, — сразу в нескольких странах.

Авторы постоянно совершенствуют свои программы, выпуск новых версий троянцев поставлен на поток.

Факты

- Ежесуточно для исследования в вирусную лабораторию «Доктор Веб» поступает в среднем около 2 млн файлов, из которых порядка 60 000 признаются вредоносными.

Вирусные аналитики — не волшебники, и мгновенно обработать такое количество ежедневно поступающих подозрительных файлов не могут. Поэтому риск заражения еще не известным антивирусу троянцем есть всегда.

Троянец подкрался незаметно?

А он вообще не подкрадывался к вам! ВЫ САМИ К НЕМУ ПРИШЛИ.

Банковские троянцы нередко проникают на компьютеры **во время просмотра взломанных сайтов**. Не нужно предпринимать вообще никаких действий, чтобы «получить троянца», — **заражение происходит автоматически**.

Ресурсы, которые чаще всего являются источниками вредоносного ПО

1. Сайты, посвященные технологиям и телекоммуникациям.
2. Новостные порталы, бухгалтерские сайты и форумы, интернет-курсы/лекции.
3. Женские сайты (о здоровье, кулинарии).

Другой очень распространенный способ заражения — через съемные устройства.

Внимание!

К съемным носителям информации относятся не только флешки, но и вообще **любые подключаемые к компьютеру через USB-порт устройства!** Передать вирус с одного компьютера на другой можно даже через фотоаппарат или MP3-плеер.

Троянцы специально рассчитаны на распространение самими пользователями, так как в отличие от вирусов не имеют механизмов саморазмножения. Жертвы сами переносят троянцев с компьютера на компьютер на флешках. Именно так происходит заражение — даже изолированных от Интернета или отключенных от локальной сети ПК.

Еще один путь распространения банковских троянцев — электронная почта и массовые почтовые рассылки. Если вы получили сообщение от неизвестного отправителя с темой «Сверка счетов», «Акт приемки-сдачи», «Срочная оплата» или тому подобной, вполне возможно, что во вложении скрывается опасная вредоносная программа.

Вредоносная программа (или небольшой скрипт, предназначенный для ее загрузки и запуска), может быть прикреплена к электронному письму, отправленному якобы налоговой инспекцией, судебными органами или фирмами-контрагентами. Достаточно одной попытки открыть такое вложение, и опасный троянец в считанные секунды проникнет на компьютер.

Банковские троянцы для мобильных устройств

Мишенями преступных киберсообществ давно перестали быть только офисные ПК — атакам подвергаются и личные устройства сотрудников, включая мобильные.

Все чаще люди пользуются услугами мобильного банкинга и совершают операции с картами и счетами при помощи Android-смартфонов и планшетов. Поскольку установить сторонние приложения на такие устройства очень легко, с каждым днем число банковских троянцев для Android увеличивается.

Попадая на мобильные устройства, эти вредоносные приложения могут:

- проверять баланс банковской карты и автоматически переводить деньги на счета киберпреступников;
- перехватывать СМС с одноразовыми проверочными кодами, помогая вирусописателям покупать товары за ваш счет;
- заставлять пользователя ввести в поддельную форму логин пароль от учетной записи сервиса мобильного банкинга;
- пополнять баланс мобильных телефонов злоумышленников;
- незаметно отправлять СМС-сообщения.

Заполучить банковского троянца на свое устройство очень просто. Чаще всего жертве приходит СМС, в котором предлагается перейти по ссылке и прочитать некое MMS-сообщение или ознакомиться с ответом покупателя на то или иное объявление. Достаточно открыть в веб-браузере указанную ссылку – вредоносная программа загрузится с мошеннического сайта автоматически. Чаще всего эти банкеры распространяются под видом новых версий известных программ (например, Adobe Flash Player, Google Play) или обновлений операционной системы.

Жертвы сами устанавливают и запускают троянцев, не видя никакой опасности.

Сегодня существуют сотни модификаций банковских троянцев для ОС Android, наиболее известные среди них относятся к семействам Android.Banker, Android.BankBot, Android.ZBot, Android.SmsBot, Android.Obad, Android.SpyEye и Android.Panda. С каждым годом число этих вредоносных приложений и атак с их участием растет. Например, только в 2015 году на мобильных устройствах различные банкеры были обнаружены антивирусами Dr.Web более **880 000 раз**.

Троянцы незаметны?

До сих пор бытует опаснейшее заблуждение, что действие вредоносной программы на компьютере всегда заметно, и, если компьютер окажется заражен, это станет понятно сразу.
Это совершенно не так!

- Современные вирусописатели стремятся создавать вредоносное ПО, которое должно как можно дольше оставаться в системе необнаруженным – как со стороны пользователя, так и со стороны антивирусов.
- Например, Trojan.Carberp, запускаясь на инфицированной машине, предпринимает целый ряд действий, чтобы обмануть средства контроля и наблюдения. После успешного запуска троянец внедряется в другие работающие приложения.

Почему это происходит?

1. Все технологически сложные и опасные вредоносные программы, разработанные с целью кражи денег, тестируются вирусописателями на необнаружение всеми антивирусами. Именно поэтому до поступления образцов вредоносных программ в вирусную лабораторию некоторые из них антивирус не «видит».
2. Троянцы, созданные для кражи средств у конкретных компаний, могут достаточно долго не обнаруживаться антивирусом, если мошенники точно знают, какой антивирус установлен на компьютерах организации.
3. Проникновение троянца на компьютер часто происходит с использованием нескольких уязвимостей в программах, установленных на ПК.
4. Сами пользователи — не знающие основ компьютерной безопасности, просто уставшие или невнимательные — неумышленно или по халатности нарушая политики безопасности, способствуют проникновению вирусов в сеть компании (используют USB-устройства, не проверяя их на вирусы, автоматически открывают почту от неизвестных отправителей, бесконтрольно путешествуют по Интернету в рабочее время и пр.).

Для борьбы с ИТ-безграмотностью компания «Доктор Веб» создает обучающие курсы, рассчитанные на широкий круг пользователей ПК, предлагает бесплатные онлайн-тестирования на знание основ компьютерной безопасности и постоянно обращает внимание пользователей на актуальные проблемы в сфере ИБ. Приобретаемые в ходе изучения курсов знания помогают лучше справляться с компьютерными угрозами и не попадаться на уловки злоумышленников.

Образовательный проект ВебIQметр:
http://www.drweb.ru/web-iq

Информационный проект «Антивирусная правДА»:
https://www.drweb.ru/pravda

Портал системы обучения «Доктор Веб»:
https://training.drweb.ru

Что делать?

Почти всегда о фактах хищения денег жертвы узнают, когда все уже произошло. Но это не значит, что не надо действовать! В этот момент исключительно важной становится правильная реакция на инцидент.

Внимание!

- Не пытайтесь обновить антивирус или запустить сканирование — так вы уничтожите следы деятельности злоумышленников в системе!
- Не пытайтесь переустановить операционную систему!
- Не пытайтесь удалить с диска какие-либо файлы или программы!
- Не пользуйтесь компьютером, с которого предположительно произошла утечка средств аутентификации к системе ДБО, — даже если в этом есть острая (производственная) необходимость!

Часто пострадавшие даже не обращаются в правоохранительные органы, считая, что средства вернуть невозможно. Жертвы не знают, с чего начать действовать в кризисной ситуации, им не знакома процедура инициирования расследования по возврату средств, они теряют драгоценное время.

Кража средств с помощью вредоносного ПО является противоправным действием, при совершении которого могут присутствовать признаки преступлений, предусмотренных статьями 159, 159.6, 165, 272 и 273 УК РФ.

Для возбуждения в отношении злоумышленников уголовного дела правоохранительным органам необходим процессуальный повод — ваше заявление о преступлении. Помните, что вы можете быть далеко не единственным пострадавшим, но первым, обратившим внимание на деятельность преступников, и ваше своевременное обращение в полицию поможет прекратить деятельность злоумышленников.

Каждый преступник оставляет за собой следы. После компьютерных преступлений тоже остаются следы — т. е. с этим злом можно и нужно бороться.

Компания «Доктор Веб» оказывает услуги по **экспертизе вирусозависимых компьютерных инцидентов**, а также проводит психологическую экспертизу личностей (персонала) с целью выявления фактов причастности к совершению / пособничеству / укрывательству / поощрению противоправных действий в отношении заказчика, фактов бездействия или халатного отношения к служебным обязанностям.

http://antifraud.drweb.com/expertise/

На сайте «Доктор Веб» в разделе «Правовой уголок» http://legal.drweb.com/ размещены образцы заявлений в правоохранительные органы и другие инстанции, а также рекомендации по действиям после обнаружения хищения. Пользуйтесь этой информацией!

Помните: компьютер для работы с денежными средствами (системами дистанционного банковского обслуживания) не должен использоваться для работы с критически важными данными, и наоборот. Никакие другие операции на таком выделенном компьютере производиться не должны.

Внимание!

Антивирус — это единственная на сегодняшний день программа, способная избавить систему от вредоносного ПО.

125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Телефон: +7 (495) 789-45-87 (многоканальный)
Факс: +7 (495) 789-45-97

www.drweb.ru | estore.drweb.ru | www.curenet.drweb.ru | www.av-desk.com | www.freedrweb.ru