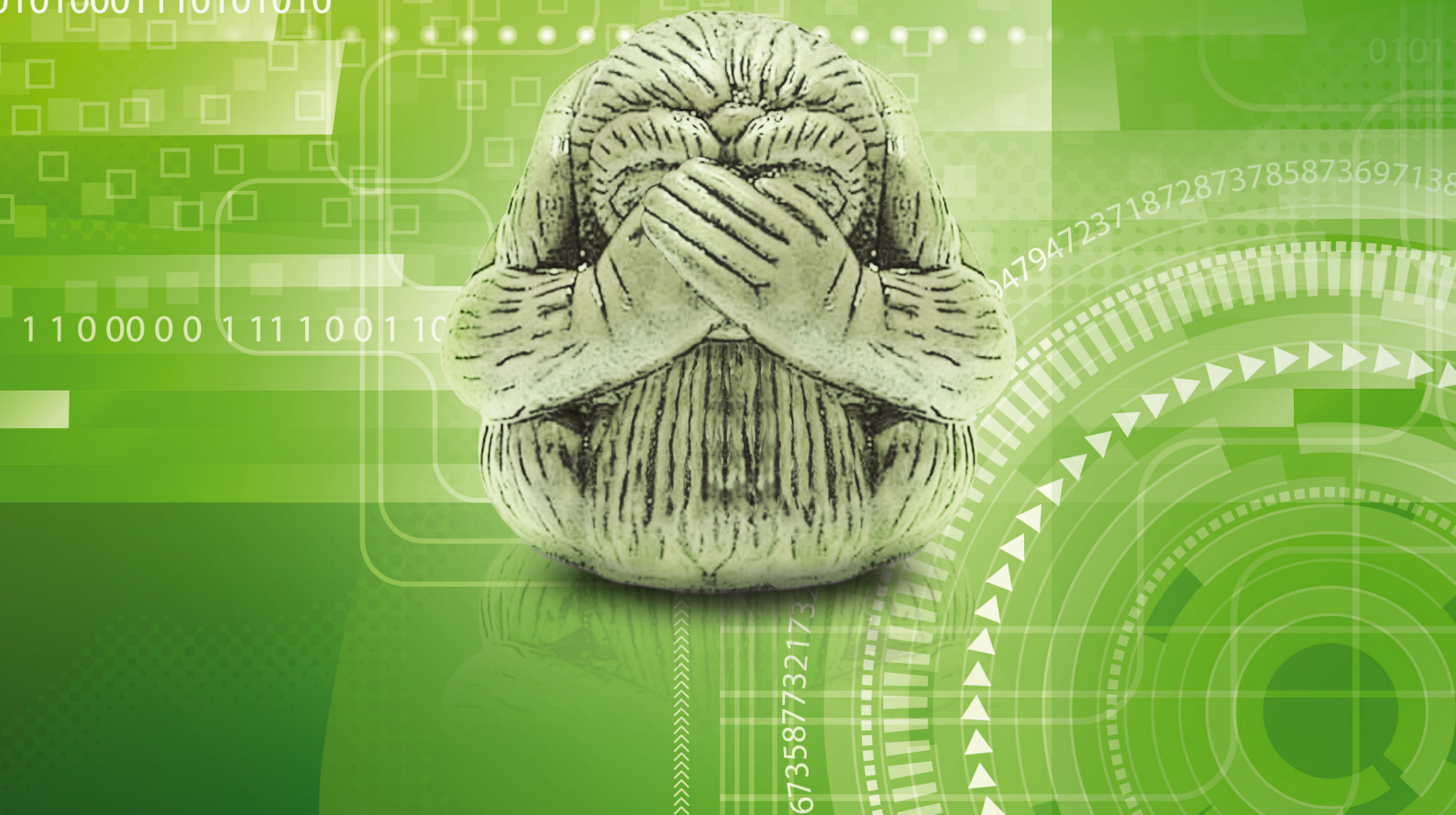
Dr.WEB®
с 1992 года

Защити созданное

Слепой не боится змеи

Внимание, угроза: банковские троянцы!



Один из сценариев заражения компьютера банковским троянцем

Реальный случай, который произошел в декабре 2012 года 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 все так же виснет, 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 эти дни совершены несколько мошеннических проводок 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, денежные средства с банковских счетов компаний любого масштаба;
- загружать другие вредоносные программы, в том числе свои дополнительные модули;
- по удаленной команде злоумышленника полностью парализовать работу компьютера.

Самый опасный из них на сегодняшний день — **Trojan.Carberp**.

У этого троянца имеются версии модулей для кражи денег из всех самых распространенных систем дистанционного банковского обслуживания (ДБО).

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

Что крадет банковский троянец?

Деньги.

Другое его владельцев не интересует.

Прежде чем приступить к хищениям, владельцы троянца собирают информацию о жертве: они знают состояние баланса компании до копейки в любой момент времени, суммы и формулировки оснований перечислений (эти же формулировки потом используются в мошеннических платежках), мгновенно получают информацию обо ВСЕХ совершаемых бухгалтером компании платежах — за жертвой ведется круглосуточное наблюдение перед тем как будет опустошен счет. Мошенники получают такие 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
- Скомпрометированная система ДБО (название)
- WWW-адрес системы ДБО
- IP-адрес компьютера жертвы
- Используемый браузер

Если скомпрометирована банковская карта

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

Кому это нужно?

Современные вредоносные программы разрабатываются вирусописателями-профессионалами, и это — хорошо организованный криминальный бизнес, вовлекающий в свою деятельность высококвалифицированных системных и прикладных разработчиков ПО.

Разработкой и «продвижением» банковских троянцев занимаются организованные преступные группы: 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, — в нескольких странах.

Программы постоянно совершенствуются их авторами, процесс выпуска новых версий троянцев поставлен на поток. Ежедневно в вирусные базы Dr.Web добавляется несколько десятков разновидностей **Trojan.Carberp!!!!! А ведь это только один троянец...**

Факты

- Ежесуточно в вирусную лабораторию «Доктор Веб» поступает в среднем не менее 60 000 образцов вредоносных программ.
- 28 ноября 2012 года был поставлен своеобразный «рекорд» — на анализ поступило более 300 000 образцов. А уже в начале декабря рекорд был перекрыт вдвое! И это далеко не все, что создается вредоносного за сутки!

Вирусные аналитики — не волшебники, и мгновенно обработать многие тысячи ежедневно поступающих подозрительных файлов не могут. Поэтому риск заражения еще неизвестным антивирусу вирусом есть всегда.

Троянец подкрался незаметно?

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

Троянцы семейства **Trojan.Carberp** проникают на компьютеры пользователей **во время просмотра взломанных сайтов**. Не нужно предпринимать вообще никаких действий для того, чтобы «получить троянца», — **заражение происходит автоматически**.

Сайты, 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 флеш-карты, 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 умышленно 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 компьютеров — даже изолированных от Интернета или отключенных от локальной сети.

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

Уже существует банковский троянец для платформы Android — Android.SpyEye.1.

Троянцы незаметны?

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

- Задачей современных вирусописателей является создание вредоносного ПО, которое должно как можно дольше оставаться в системе необнаруженным — как со стороны пользователя системы, так и со стороны специальных программ (антивирусов).
- Например, Trojan.Carberp, запускаясь на инфицированной машине, предпринимает целый ряд действий для того, 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 денежных средств, тестируются вирусописателями на обнаружение всеми антивирусами. Именно поэтому до поступления образцов вредоносных программ в вирусную лабораторию некоторые из них не обнаруживаются антивирусом.
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 бухгалтера произошло благодаря эксплуатации троянцем нескольких уязвимостей в программах, установленных на ПК. Нажатие на кнопку во всплывающем окошке послужило спусковым крючком для приведения троянца в действие. После этого троянцу не составляло труда похищать любую информацию с компьютера жертвы.
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, и предлагает бесплатные онлайн-тестирования на знание основ компьютерной безопасности. Приобретаемые в ходе изучения курсов знания помогают лучше справляться с компьютерными угрозами и не попадаться на уловки злоумышленников.

Образовательный проект ВебIQметр:
http://www.drweb.com/web-iq/
Портал системы обучения «Доктор Веб»:
http://training.drweb.com

Внимание!

Антивирус — это единственное на сегодняшний день программное обеспечение, которое способно избавить систему от вредоносного ПО.

Что делать?

Почти всегда о фактах хищения 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 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 нем есть острая (производственная) необходимость!

В России не существует единой статистики фактов хищений средств через системы дистанционного банковского обслуживания с помощью вредоносных программ. 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 по ст. ст. 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.

Дополнительная информация

Ознакомление с этими информационными материалами позволит вам минимизировать возможные финансовые потери при работе с системами дистанционного банковского обслуживания. В них также содержатся полезные советы о том, как правильно организовать защищенную работу с системами ДБО, что для этого необходимо предпринять и чего делать категорически не следует.

- Брошюра «Слепой змеи не боится» (Распечатать в PDF | Читать в SWF).
- Видео «Слепой змеи не боится».
- Информационный раздел на сайте «Доктор Веб» о банковских троянцах.
- Учебный курс DWCERT 070-3 «Антивирусная система защиты предприятия».

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