ПРОГРАММЫ И ЗАЩИТА ОТ НИХ

Троянские программы

Троянской программой (троянцем, или троянским конем) называется:

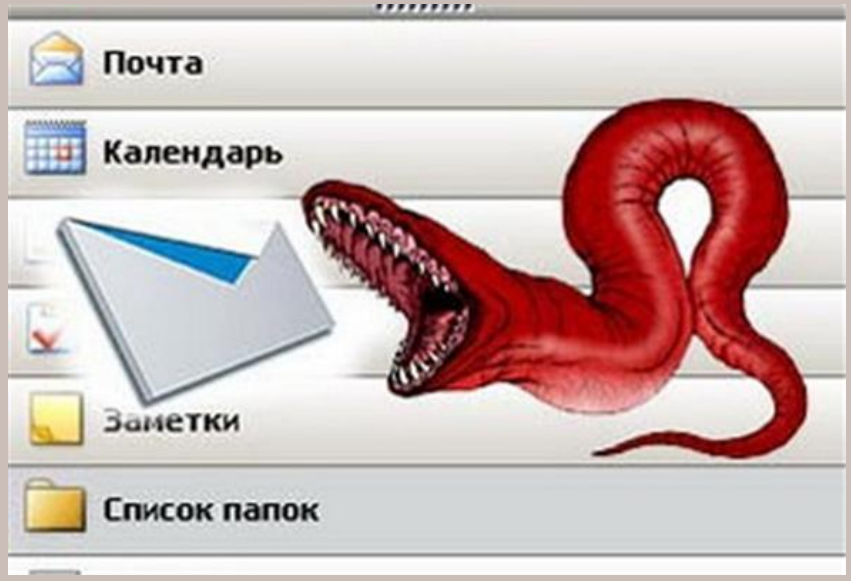
- программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба;
- программа с известными ее пользователю функциями, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие (разрушительные) действия.

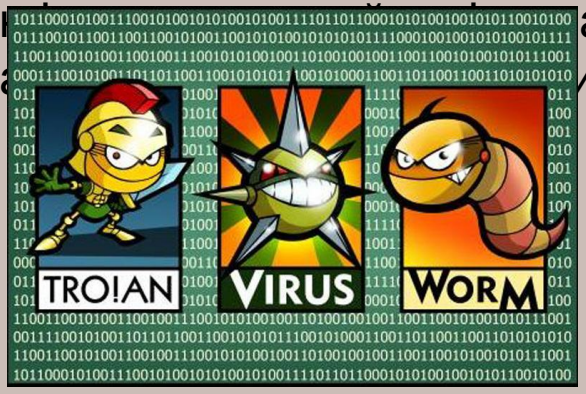
- Принципиальное различие троянских программ и вирусов состоит в том, что вирус представляет собой самостоятельно размножающуюся программу, тогда как троянец не имеет возможности самостоятельного распространения. Однако в настоящее время довольно

часто встречаются гибриды — вирусы (в основном e-mail и сетевые черви), вместе с которыми распространяются троянские программы.

Что будет делать подобная программа, внедрившись в компьютер, известно одному только ее создателю и зависит лишь от его фантазии и от стоящих перед ним целей. В то же время можно выделить ряд наиболее распространенных действий, имеющих явно вредоносную направленность:

Воровство паролей. Раньше, когда основным и фактически единственным способом массового доступа в Интернет было модемное соединение, большинство троянских программ создавались именно с целью кражи паролей для связи с Интернетом. Однако в последнее время все труднее найти пользователя, использующего dial-up, и сейчас крадут в основном пароли от почты, форумов, чатов, ICQ и других сервисов. Хотя обычно это не наносит прямого ущерба большинству пользователей, но последствия, связанные с получением злоумышленниками доступа к ко[illegible]ации, могут ока[illegible]и.

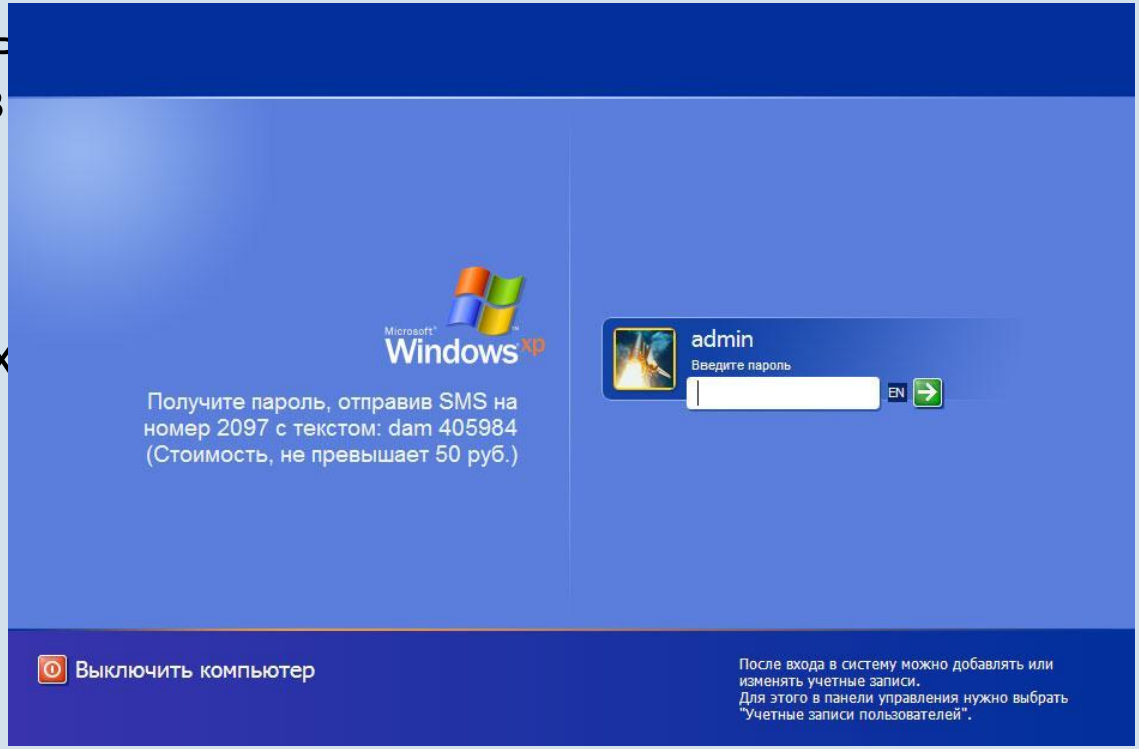




Программы DDoS-атаки. Зараженные такой троянской программой компьютеры участвуют в DDoS-атаках, вызывая перегрузку атакуемого сервера. И опять с точки зрения атакуемого все выглядит так, словно один из нападавших — это компьютер жертвы.

Удаленное администрирование. Программы этого класса аналогичны профессиональным утилитам удаленного администрирования, однако устанавливаются без согласия пользователя и позволяют злоумышленнику держать компьютер под полным контролем. При этом иногда с помощью такой утилиты злоумышленник имеет возможность совершать на компьютере-жертве даже больше действий, чем сам владелец, не применяющий специальных средств. Нередко данные программы внедряются друзьями или знакомыми пользователя — для организации дружеских розыгрышей (которые, впрочем, далеко не всегда оказываются безобидными).

Рассылка спама. Такой троянец после установки на компьютер пользователя начинает рассылать спам по заранее заданным адресам либо собирать адреса электронной почты, имеющиеся на компьютере пользователя и на тех сайтах, где тот бывает, и организует массовую рассылку по ним. Другой вариант использования компьютера-жертвы для рассылки спама — установка на нем SMTP-сервера, самостоятельно задействуемого злоумышленником для рассылки спама. Хотя от такого поведения троянца страдает больше не сам пользователь, а миллионы получателей нежелатель пользователя последств могут быть весьма неприятные (например, блокировка IP-адреса в большинстве почтовых систем).



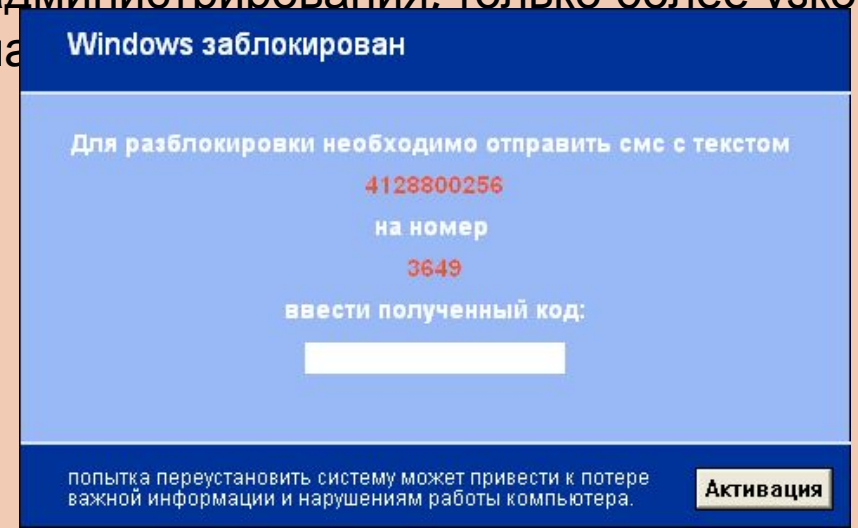
Proxy-серверы. Троянская программа устанавливает на компьютер один или несколько видов прокси-серверов (Socks, HTTP и пр.), с помощью которых злоумышленник может совершать любые действия в Интернете, не опасаясь обнаружения истинного IP-адреса, поскольку вместо него подставляется адрес жертвы.

Шпионские программы. Программы этого класса собирают сведения с зараженного компьютера (это может быть вся переписка, все нажимаемые клавиши, посещаемые страницы, установленные программы и многое другое) и пересылают их по адресу, прописанному в троянце.

Программы распределенных вычислений. Эти программы можно назвать одним из самых «интеллигентных» классов троянцев. Цели таких программ могут быть различным, в том числе — установка модулей открытых проектов распределенных вычислений (distributed.net), где, например, отыскиваются алгоритмы взлома систем шифрования, а тот, на чьем компьютере получен искомый результат, может претендовать на денежное вознаграждение. Злоумышленник, стремясь получить вознаграждение, конфигурирует официальный модуль системы распределенных вычислений с внесенными в него своими идентификационными данными и встраивает его в троянскую программу, которая незаметно его устанавливает и запускает. Наука наукой, но в любом случае человек, участвующий в проекте, должен делать это добровольно. Распределенные вычисления могут использоваться и для менее благовидных дел: для поиска сервисов в Интернете (например, прокси-серверов), а также для подбора паролей. В этой ситуации автору для достижения результата не потребуется так много времени, как если бы он работал на своем компьютере.

Рекламные модули и модули накрутки рекламы. Троянские программы могут демонстрировать пользователю зараженного компьютера рекламную информацию разного рода, например всплывающие окна, баннеры, которые встраиваются в системные панели, просматриваемые страницы. Другой вариант применения зараженного компьютера в рекламных целях — накрутка баннерных систем путем имитации заходов пользователя на ресурс, где размещена реклама.

Троянцы, устанавливающие дополнительные модули либо ждущие команды от своего автора. Такие программы загружают на зараженный компьютер файлы с запрограммированного адреса или ждут получения команды от автора (каналом связи может быть получение электронного письма, появление сообщения на форуме или на сайте и т. д.) на совершение каких-либо действий (как перечисленных выше, так и любых других). В некотором смысле это может считаться вариантом удаленного администрирования, только более узко на



- Таким образом, троянская программа — это особая разновидность программной закладки. Она дополнительно наделена функциями, о существовании которых пользователь даже не подозревает. Когда троянская программа выполняет эти функции, компьютерной системе наносится определенный ущерб. Однако то, что при одних обстоятельствах причиняет непоправимый вред, при других— может оказаться вполне полезным. К примеру, программу, которая форматирует жесткий диск, нельзя назван. троянской, если она как раз и предназначена для его форматирования (как это делает команда format операционной системы DOS). Но если пользователь, выполняя некоторую программу, совершенно не ждет, что она отформатирует его винчестер, — это и есть самый настоящий троянец.

Защита компьютера

Для защиты компьютера через интернет, на компьютере должен быть установлен антивирус с защитой от ненадежных сайтов. На сегодняшние дни существует не малое количество антивирусов, из них являются надежными отечественные антивирусы, такие как компания Лаборатория Касперского и Dr.Web. Существуют троянские программы, которые могут отключить защиту компьютера, тем самым распространяться по файлам, но благодаря этим надежным антивирусам, вирус не сможет отключить его.

В паре с антивирусом могут работать брандмауэры или фрайрволлы. Их задача отслеживать открываемые несанкционированно открытые порты, в случае, если сервер троянской программы откроет его. Брандмауэр работает по принципу разрешения открытия порта той или иной программе, каждый раз при этом спрашивая. Существуют вирусы, которые отключают брандмауэр, по этому признаку

Наилучшим средством для снижения риска заражения компьютера являются:

- не работать в системе с правами администратора. Желательно работать с ограниченными правами, а для запуска программ, требующих больших прав, использовать пункт «Запустить от имени» в контекстном меню;
- не загружать программ из непроверенных источников — прежде всего это относится к сайтам, распространяющим взломанное, нелицензионное программное обеспечение и хакерские утилиты;
- по возможности не допускать к своему компьютеру посторонних;
- регулярно делать снимки для восстановления системы и резервные копии важной информации и файлов;
- пользоваться малораспространенными программами для работы в сети или хотя бы не теми, что установлены по умолчанию (например, браузером Opera, Mozilla, почтовым клиентом Thunderbird, The Bat! и т.д.). Этот подход, несомненно, имеет массу недостатков, но на уровне частных пользователей нередко оказывается самым действенным;
- пользоваться нестандартными брандмауэрами, пусть даже не самыми лучшими по результатам тестирований, поскольку злоумышленник, как правило, не будет встраивать средства для обхода всех существующих брандмауэров, ограничившись несколькими самыми популярными;
- переименовывать исполняемые файлы антивирусов и брандмауэров, а также сервисы, используемые ими, а при наличии соответствующих навыков — изменять заголовки их окон;
- пользоваться мониторами реестра, в которых необходимо включить слежение за указанными в данной статье разделами;
- сделать снимок файлов в системных директориях и при появлении новых попытаться определить, что это за файл и откуда он взялся, либо применять специальные программы — ревизоры диска, которые позволяют выявить новые подозрительные файлы, а также изменение размера существующих;
- не запускать программ, полученных от неизвестных лиц;
- включать на компьютере отображение всех расширений файлов и внимательно следить за полным именем файла. Троянская программа может скрываться в файле, имеющем двойное расширение (первое — безопасное, служащие для маскировки, например картинки gif, а второе — реальное расширение исполняемого файла);
- регулярно устанавливать заплатки для операционной системы и используемых программ;
- не разрешать браузеру запоминать пароли и не хранить их в слабо защищенных программах хранения паролей. В том случае, если вам удобнее не запоминать пароли, а хранить их на компьютере, стоит подумать над установкой программы, которая сохраняет вводимые в нее записи в стойко зашифрованном виде.

Большинство троянских программ не афиширует своего присутствия на компьютере пользователя, однако предположить, что компьютер заражен, можно по ряду косвенных признаков:

- отказ работы одной либо нескольких программ, особенно антивируса и брандмауэра;
- появление всплывающих окон, содержащих рекламу;
- периодическое появление окна dial-up-соединения с попытками соединиться с провайдером либо вообще с неизвестным номером (часто зарубежным);
- при отсутствии вашей активности на подключенном к Интернету компьютере (вы ничего не скачиваете, программы общений неактивны и т.д.) индикаторы подключения к сети продолжают показывать обмен информацией;
- стартовая страница браузера постоянно меняется, а страница, указанная вами в роли стартовой, не сохраняется;
- при попытке посетить сайты, куда вы раньше легко заходили (например, в поисковые системы), компьютер переадресовывает вас на незнакомый сайт, часто содержащий порнографическую либо рекламную информацию.