Выражение «троянский конь» появилось из истории, и мы до сих пор его используем в разговоре. Выражение «троянский конь» подразумевает что-то, что на первый взгляд выглядит вполне обычно и невинно, но, на самом деле, может причинить вред. Троянский вирус (или ещё его называют Троян) - файл, который выглядит вполне безобидно, но, на самом деле, представляет угрозу. Хотя они и появились относительно недавно, они уже упрочнились в нашей жизни и своей репутацией затмили деревянного троянского коня из далёкого прошлого. Далее мы опишем некоторые из видов троянских вирусов, с которыми можно столкнуться.

Первый троянский вирус, который мы обсудим, входит в категорию «западня». Он также более известен под названием Spy Sheriff, и уже успел заразить миллионы компьютерных систем по всему миру. Этот троянский вирус классифицируется как malware (зловредное программное обеспечение). Он не влияет на компьютерную систему и не причиняет ей вреда, но он заставляет появляться всякие нудные всплывающие окна.

Большинство этих окон выглядят как системные сообщения, в которых содержатся предупреждения, заявляющие, что вы должны установить тот или иной тип программного обеспечения. Как только Spy Sheriff попадает на ваш компьютер, его очень трудно удалить. Если вы попробуете удалить его обычным способом, то он просто заново установиться с помощью скрытых файлов, которые он заразил на вашей системе. Большинство антивирусных и antispyware программ не смогут обнаружить этот вирус. Также его невозможно удалить, с помощью функции восстановления системы, поскольку он контролирует компоненты, которые управляют этой особенностью в Windows.

Иногда троянские вирусы могут содержаться в архивах, которые с виду кажутся безопасными. Некоторые Трояны используются злоумышленниками для удалённого управления чужим компьютером. Они также используются для атаки и взлома компьютерных систем. Один из самых известных случаев, связанных с Трояном произошёл с профессором, на компьютере которого обнаружились тысячи детских порнографических фотографий. Сначала его обвинили в том, что он сознательно их загрузил. Хотя, в конечном счёте, он был оправдан и выяснилось, что это действие Трояна, всё равно ситуация вышла пренеприятная.

Другой известный тип вирусной проблемы, который оказал след в истории - вирус Vundo. Этот вирус в различных интервалах использует память Windows и создаёт всплывающие окна, в которых указано, что потеряны важные системные файлы. Он также вызывает множество сообщений, в которых говорится, что вам следует установить несколько программных обеспечений безопасности, многие из которых в действительности являются вирусами. К счастью, этот вирус легко подаётся удалению, поскольку на рынке существует множество автоматических программ для этого процесса.

Троянский вирус может разными способами попасть в вашу компьютерную систему. Но одно вы должны помнить: они не смогут активизироваться, если вы сами не активизируете файл, в котором они скрыты. Именно поэтому настолько важно проверять неизвестные файлы и, по возможности, вообще их не открывать, ведь если в системе появиться Троян, это может привести к печальным последствиям

Троянец - это тип вируса-червя, который может послужить причиной серьезного повреждения Вашего компьютера. Червь - это программа, которая на первый взгляд может показаться безвредной и безопасной, но, на самом деле, она содержит кое-что весьма вредное для Вашего компьютера. Настолько вредное, что может разрушить Ваш компьютер посредством широкого повреждения, которое может оказаться необратимым.

Если Вы хорошо помните историю, то Вам не трудно будет вспомнить, как греки выиграли троянскую войну, скрываясь в большой полой деревянной лошади для того, чтобы войти в хорошо укрепленную Трою. В действительности, троянец также получает доступ к Вашему компьютеру. Троянцы попадают в Ваш компьютер при загрузке безопасных программ, таких, как игры, изображения, музыка или видео файлы, но как только эти программы выполняются, троянцы начинают свою работу. Троянцы могут сделать не только то, что Вас будет очень сильно раздражать; но также они могут серьезно повредить Ваш компьютер. Еще троянцы могут стереть Ваш диск, посылать номера Вашей кредитной карточки и пароли незнакомцам или позволить другим использовать Ваш компьютер в незаконных целях, таких, как отказ от сервисной защиты, тем самым, нанося вред сетям.

Ваша лучшая защита - это антивирусное программное обеспечение, которое автоматически обновляется и внимательно следит за тем, что Вы загружаете из Интернета. Благодаря антивирусному программному обеспечению, Вы загружаете с вебсайтов только то, что безопасно, и, тем самым, защищаете компьютер от вирусов. Антивирусное программное обеспечение - Ваша лучшая защита не только против троянских вирусов, но и от многого другого - защищает Вас от шпионского программного обеспечения, бесплатного программного продукта с размещенной в нем рекламой и других типов злонамеренных атак на Ваш компьютер. С хорошим антивирусным программным обеспечением Вам не придется волноваться о потере Ваших данных или пропаже личной информации

**Замаскированные вредоносные программы**

Какие бы меры для защиты ни принимались, никакую сеть невозможно оградить от одной серьезной опасности — человеческой доверчивости. Этим пользуются вредоносные программы, называемые «троянскими конями», зловредные коды которых прячутся внутри чего-нибудь совершенно безобидного. А ведь если программа была установлена по доброй воле, она может преодолеть любые брандмауэры, системы аутентификации и сканеры вирусов.

«Троянские кони» отличаются друг от друга тем, какие вредные действия они выполняют, оказавшись в компьютере. Это может быть как безобидная проделка, связанная с выводом на экран какой-нибудь непристойности или политического лозунга, так и настоящая информационная катастрофа, приводящая к уничтожению данных на диске и порче оборудования. Некоторые из «троянских коней», объединившись с вирусами, распространяются между системами по электронной почте.

Самые же изощренные действуют очень вероломно и не ограничиваются нанесением ущерба системе. Помимо хакерства «троянские кони» могут использоваться для шпионажа за людьми и действовать как настоящие преступники, хотя и виртуальные. Никто не может чувствовать себя в безопасности. Осенью 2000 г. корпорация Microsoft пострадала от получившего широкую огласку нападения хакеров, когда был украден и, возможно, видоизменен исходный код будущей операционной системы. Это стало результатом внедрения «троянского коня», скрывавшего в себе «червя» — программу, «ползающую» по сети и копирующую себя на другие компьютеры. Будучи установленной на одном из компьютеров Microsoft, программа начала распространяться по сети и делала это до тех пор, пока она не попала на компьютер, где содержалась важная секретная информация. После этого «троянский конь» подал хакеру сигнал о своем присутствии и открыл в сети «потайную дверь».

Итак, что же можно сделать, чтобы избежать участи Microsoft? Конечно, изгнать всех пользователей из сети вы не можете. Однако есть несколько способов минимизировать риск, и начать надо с бдительности и обучения. Регулярное резервное копирование является необходимой процедурой для восстановления информации после воздействия тех «троянских коней», вмешательство которых ограничивается уничтожением данных. Использование полного набора программных средств защиты, таких, как брандмауэры и сканеры вирусов, может помочь поймать некоторых наиболее известных нарушителей. Но важнее всего усвоить самому и объяснить пользователям сети, что такое «троянские кони», как они действуют и какого типа программы могут в себе скрывать. Кроме того, надо уяснить, как отличить «троянского» от настоящего «дареного коня», прежде чем он попадет в вашу сеть.

**Темные лошадки**

В большинстве «троянских коней» спрятаны вирусы или «черви». И те и другие паразиты существуют, главным образом, ради воспроизведения себе подобных, но могут и причинять серьезный ущерб (см. врезку «Виды программ-паразитов»). «Троянцы» приобрели особое значение для распространения вирусов, поскольку большинство из них сейчас посылается по электронной почте в виде вложенных файлов. Для активации вируса пользователь должен открыть такой вложенный файл, в то время как ранние вирусы, распространявшиеся на дискетах, активировались автоматически при загрузке ПК.

Не считая Bubbleboy, который встречался очень редко и проникал через уже устраненную «дыру» в системе безопасности Microsoft Outlook, вирус практически невозможно подхватить, просто читая сообщение электронной почты. Пользователя нужно обманным путем заставить запустить вложенный файл, и создатели вирусов не без оснований полагают, что сделать это не так уж сложно. Многие люди автоматически дважды щелкают мышью по любому файлу, приходящему по электронной почте, так что им нужно привить привычку поступать иначе.

Как известно, файлы Windows с расширениями \*.com (command — командный), \*.exe (executable — выполняемый) и \*.dll (dynamic link library — динамически подключаемая библиотека) являются программами. Потенциально они способны сделать с системой практически все что угодно, поэтому с ними нужно обращаться с особой осторожностью, т. е. запускать их следует только в том случае, если источник, из которого вы их получили, заслуживает полного доверия, и вам точно известно, для чего предназначены данные программы. Тот факт, что программа была прислана по электронной почте вашим другом или коллегой, не является достаточным основанием, чтобы запускать ее. «Троянский конь» мог проникнуть в почтовую систему вашего приятеля и разослать себя по всем адресам из адресной книги.

Чтобы предотвратить заражение вирусами, многие организации вводят специальные правила, запрещающие пользователям устанавливать неразрешенное программное обеспечение. Однако соблюдение такого рода ограничений часто трудно проконтролировать, и, кроме того, это может помешать сотрудникам использовать для выполнения своей работы действительно лучшие программные средства, имеющиеся на рынке. Независимо от того, применяете вы подобные правила или нет, важно, чтобы пользователи были осведомлены о потенциальной опасности. Если сотрудникам разрешено загружать программы, то они должны знать, какие из них представляют наибольшую угрозу. Если же это им запрещено, то они больше будут обращать внимание на правила, понимая, чем они продиктованы.

Наиболее серьезную опасность представляют пиратские программы, поскольку источник, из которого они поступают, по определению не заслуживает доверия. Серьезные программисты давно точат зуб на пиратов, распространяющих «троянских коней» под видом нелегальных программ. Под эту категорию подпадает первая известная атака на платформу Palm, предпринятая с помощью программы, представленной как эмулятор популярной программы GameBoy под названием Liberty. Вместо обещанной эмуляции она удаляет все файлы и приложения.

Список расширений имен файлов, используемых программами, постоянно пополняется, что затрудняет задачу их отслеживания с помощью сканеров вирусов. Большинство антивирусных программ проверяет около 30 различных видов файлов, но они все же «споткнулись» на файлах с расширением \*.vbs (Visual Basic Script), которыми в 2000 г. воспользовался вирус Love Bug. Если ваша антивирусная программа старее, чем этот вирус, то вам следует либо обновить ее, либо вручную настроить на проверку всех типов файлов. Автоматические обновления, распространяемые через Internet, обычно содержат только новые списки вирусов и исправления, а не новые типы файлов, в которых те могут скрываться.

Наиболее опасным типом файлов являются системные файлы-фрагменты, предназначение которых состоит в передаче частей документов между приложениями и рабочим столом (shell scrap object) — они как будто специально созданы для использования в качестве «троянского коня». И хотя они должны были бы иметь расширение \*.shs или \*.shb, они остаются скрытыми в среде Windows 98/Me, маскируясь под любой другой тип файла. Первой программой, где была использована подобная уязвимость, был появившийся в июне 1998 г. вирус Stages. Прикидываясь безобидным текстовым файлом, он на самом деле был сценарием Visual Basic и рассылал себя по электронной почте всем, кто был указан в адресной книге пользователя.

Файлы-фрагменты настолько опасны, что антивирусный исследовательский центр компании Symantec рекомендует вообще отказаться от их использования. Поскольку с этими файлами имеет дело очень мало легальных приложений, многие пользователи вполне могли бы вообще обойтись без них, удалив файл schscrap.dll из каталога Windows/system на своем ПК. В качестве менее радикальной меры можно запретить системе скрывать такие файлы, удалив элемент реестра HKEY\_ CLASSES\_ROOT\ShellScrap.

**Натягивая поводья**

Какую бы серьезную угрозу ни несли в себе вирусы и «черви», они все же являются не самой опасной начинкой, которая может быть спрятана в «троянских конях». Многие из них предназначены для получения доступа к вашей сети и прячут небольшие серверные программы, работающие практически незаметно. С помощью этих программ хакер может выведать ваши секреты или даже получить контроль над вашим ПК.

Самым бессовестным хакерским инструментом считается Back Orifice 2000, часто называемый просто BO2K, созданный командой хакеров «Культ дохлой коровы». Авторы определяют свою программу как «средство дистанционного администрирования», позволяющее управлять компьютером без ведома и согласия пользователя. Она может практически незаметно работать под любой версией Windows, обеспечивая постороннему пользователю практически полный доступ к системе. Кроме копирования и изменения содержимого файлов хакеры, имеющие на вооружении BO2K, могут записывать каждое действие пользователя и даже в реальном времени получать поток видеоинформации с его экрана.

По иронии судьбы, команда «Культ дохлой коровы» сама стала жертвой «троянского коня». Первые компакт-диски с Back Orifice 2000, предназначавшиеся для распространения, были заражены страшным вирусом Chernobyl («Чернобыль»), способным нанести необратимый ущерб оборудованию. Честолюбивые хакеры, участвовавшие в 1999 г. в конференции DefCon, обнаружили, что вместо того, чтобы получить контроль на компьютерами других людей, они потеряли контроль над своими собственными, так как их жесткие диски оказались перезаписаны, а микросхемы BIOS стерты.

В нападении на Microsoft осенью 2000 г. использовался «троянский конь» под названием QAZ, который маскировался под утилиту Notepad, размещаясь в файле notepdad.exe. Исходная программа Notepad была по-прежнему доступна, но переименована в note.exe, так что пользователи не замечали изменений. Администратор, зная, что этот файл не входит в стандартную установку Windows, мог удалить его, в результате чего программа Notepad переставала работать, а «троянский конь» оставался нетронутым.

Даже если злоумышленники не заинтересованы в вашей информации, получение ими контроля над компьютерами по-прежнему представляет серьезную опасность. Атаки по типу распределенный отказ в обслуживании (Distributed Denial of Service, DDoS), в результате которых в начале 2000 г. оказались недоступны некоторые популярные Web-сайты, были произведены с помощью «троянских коней». Принцип действия подобных программ основывается на использовании тысяч компьютеров, работающих вместе, и поэтому они не могут быть просто запущены на каком-то одном из них. Однако атака становится возможной, когда один из компьютеров получает контроль над тысячами других.

Последствия вашего участия в атаках наподобие DdoS не исчерпывается тем, что вы получаете неодобрение как член сетевого сообщества, а ваша организация подвергается риску судебного разбирательства. К примеру, в результате атак на Yahoo! и eBay пострадали не только эти серверы, но и тысячи домашних и офисных пользователей, чьи компьютеры были задействованы в данных атаках. Если ваш почтовый сервер занят в атаке, то он не сможет выполнять своего основного назначения.

Любой ПК, подключенный к телефонной линии, является потенциальной мишенью для нападения по финансовым мотивам, поскольку его модем может быть перепрограммирован на звонки по дорогостоящим телефонным номерам. Известны «троянские кони», заменяющие в параметрах настройки коммутируемого доступа пользователя обычный телефонный номер на международный, звонки по которому могут стоить несколько долларов в минуту. И если этот номер действительно подключен к провайдеру Internet, жертва может ничего не заметить до тех пор, пока не получит счета за телефонные разговоры.

Этот вид «троянских коней» впервые появился в 1998 г., когда тысячи пользователей в Европе, загружавшие порнографическое слайд-шоу, обнаружили, что их модемы звонят по очень дорогому номеру в Республике Гана. Данная атака была занесена под №3 в список наиболее опасных случаев мошенничества в Internet, составленный Федеральной торговой комиссией (Federal Trade Commission), и считается более опасным явлением, чем телефонное пиратство и финансовые пирамиды.

**Плотно закрывайте дверь**

Большинство «троянских коней» посылает хакеру сигнал о своем присутствии через заданный порт TCP, поэтому правильно настроенный брандмауэр может обнаружить и заблокировать их. Списки портов, используемых популярными «троянскими конями», публикуются на специальных Web-сайтах (см. врезку «Ресурсы Internet»), некоторые из них могут даже выполнять сканирование. Однако последние версии многих вредительских программ могут менять заданный порт, усложняя их обнаружение. Антивирусное ПО также может обнаруживать «троянских коней», хотя это и связано с определенным риском. Поскольку такое ПО необходимо регулярно обновлять, компания, производящая антивирусные программы, получает доступ к вашей сети. В ноябре 2000 г. обновление ПО McAfee VirusScan компании Network Associates привело к сбою некоторых систем и потере несохраненных данных. Это произошло из- за ошибки в ПО, а не в результате умышленных действий, однако для уже скомпрометированных компаний, таких, как Microsoft, выходящих на рынок антивирусного ПО, существует риск, что отдельные «троянские кони» могут использовать данный метод нападения.

Правительство Германии считает, что Windows 2000 возможно уже является убежищем для «троянского коня». Оно дошло до того, что грозится наложить запрет на распространение данного ПО, пока Microsoft не удалит из него утилиту Disk Defragmenter (программу дефрагментации диска), в которой якобы скрывается этот опасный код. Microsoft отказалась это делать, но опубликовала на своем немецком сайте технической поддержки подробные инструкции, объясняющие пользователям, как удалить утилиту самостоятельно. Те менеджеры, которых беспокоит этот факт, должны иметь в виду, что до сих пор нет доказательств того, что упомянутый «троянский конь» вообще существует. Действительно, правительство США настолько уверено в безопасности Windows 2000, что использует это ПО во многих своих организациях, включая военные.

**Виды программ-паразитов**

Хотя пресса и некоторые пользователи часто называют любую вредную программу вирусом, специалисты по безопасности знают, что это не так. Вот краткое описание трех наиболее распространенных видов зловредных программ, каждая из которых может скрываться внутри «троянского коня».

Вирус (virus) представляет собой самовоспроизводящийся код, присоединяющийся к другому файлу точно так же, как настоящие вирусы прикрепляются к живым клеткам. Изначально вирусы поражали программные файлы, имеющие расширения \*.com или \*.exe, однако распространение языков сценариев позволило им заражать офисные документы и даже сообщения электронной почты.

«Червь» (worm) — это автономная программа, обычно воспроизводящаяся путем копирования себя на другие компьютеры в сети. Иногда их называют бактериями, поскольку они не зависят от других программ. Наибольшее распространение получила программа happy99.exe, парализовавшая множество компьютеров два года назад и все еще изредка появляющаяся — особенно под Новый год.

«Логическая бомба» (logic bomb) не воспроизводится, но может принести серьезный ущерб. Обычно это простые программы, выполняющие вредные функции, такие, как удаление пользовательских файлов при выполнении. Современный Интернет — это не только крайне полезная информационная среда, но и потенциальный источник различных опасностей, угрожающих как компьютерам простых пользователей, так и серверам. И если верить статистике, то самой серьезной из этих угроз являются вирусы, особенно так называемые *троянские* кони. Происхождение этого термина известно всем еще из школьного курса истории. Он определяет подарок, который таит в себе какую-то угрозу для его получателя. В принципе это очень точно описывает данный класс зловредных программ. Эти «подарочки» **могут** нанести интернетчикам серьезный ущерб. Ну а для того чтобы не быть голословными, давайте мы с вами, уважаемые читатели, рассмотрим действие троянских коней поподробнее.

*Троянские* кони — это одна из самых опасных для компьютера и его владельца угроз в Интернете

Итак, как мы уже говорили, **троянские** **кони** — это одна из самых опасных для компьютера и его владельца угроз в Интернете. Причем эти зловредные программы могут быть чрезвычайно разнообразными. По сути, даже большинство современных интернет-червей можно отнести к троянским коням. Описать их, как-то классифицировать — задача явно не простая. Однако есть один параметр, по которому всех **троянских** коней можно очень легко распределить по разным группам. Речь идет об их предназначении, то есть фактически о том действии, которое они оказывают на компьютер-жертву. Если подойти к данному вопросу внимательно, то можно выделить целых шесть классов зловредных программ, оказывающих различное деструктивное влияние на систему жертвы.

**Удаленное администрирование**

Трояны, реализующие удаленное администрирование, позволяют хакеру управлять компьютером-жертвой

Сегодня можно найти немало программ, позволяющих осуществлять удаленное администрирование как отдельных компьютеров, так и целых компьютерных систем. Это очень удобные утилиты, существенно облегчающие задачу администраторов локальной сети и позволяющие экономить их время (а значит, и деньги компаний). Принцип работы таких программ прост. На удаленный ПК устанавливается специальный агент. После этого администратор может в любой момент запустить на своей машине основной модуль, подключиться к другому компьютеру и получить возможность полностью им управлять.

А теперь представьте, что пользователь персонального компьютера не знает об установленном в его системе агенте. А последний связывается не с соседней по локальной сети машиной, а с удаленным за тысячи километров ПК, за которым сидит хакер. В этом случае злоумышленник может сделать все что угодно: получить пароли, скопировать личные документы, установить любое программное обеспечение, просто перегрузить или выключить компьютер... Именно поэтому **троянские** *кони* (фактически это агенты утилит удаленного администрирования) рассмотренного класса считаются самыми опасными. Они предоставляют злоумышленнику практически неограниченные возможности по управлению машиной жертвы.

**Кража данных**

Некоторые трояны *могут* воровать пароли пользователей

К другой крайне опасной группе *троянских* коней относятся те из них, которые нацелены на воровство информации у пользователей. Особенно серьезную угрозу они представляют для владельцев домашних ПК. Казалось бы, все должно быть совсем наоборот. Ну какие могут быть секретные данные у простых пользователей? Гораздо интересней хакерам должны быть компании, у каждой из которых полно коммерческих тайн, а их всегда можно попытаться продать конкурентам. Однако здесь есть одна проблема. Ведь **троянский** конь не может самостоятельно найти файлы с секретной документацией. Кроме того, незаметно передать через Интернет сколько-нибудь существенные объемы данных довольно сложно. А вот с компьютеров домашних пользователей (зачастую менее защищенных) можно легко украсть, например, пароли для доступа в операционную систему или в Интернет.

Причем наибольшую популярность получил именно последний вариант. С помощью троянских коней, ворующих пароли для доступа к Сети, злоумышленники, которые подключены у того же провайдера, что и жертва, *могут* легко переложить свои затраты на Интернет на других людей, просто пользуясь их авторизационными данными. Кроме того, иногда встречаются зловредные программы с достаточно сложным алгоритмом, которые **могут** попытаться вытащить сохраненные в браузере пароли от различных веб-сервисов, FTP-серверов и т. п.

**Шпионаж**

Трояны-шпионы позволяют хакеру получить подробную информацию о пользователе вплоть до его паролей к разным сервисам

Сегодня злоумышленники все чаще и чаще используют шпионаж. Суть его заключается в следующем. На компьютере жертвы устанавливается специальный агент, который, работая незаметно для пользователя, собирает определенную информацию о нем и через Интернет отправляет ее хакеру. Для такого ПО придумали даже специальный термин — spyware. Современные программы-шпионы умеют делать очень многое: вести лог нажатых человеком клавиш на клавиатуре, периодически делать скриншоты всего экрана и активного окна, записывать названия запущенных программ, открытых документов и адреса посещенных веб-страниц.

Все это позволяет злоумышленникам получить весьма подробные данные о своей жертве вплоть до паролей, необходимых для выхода в Сеть и использования различных сервисов.

Впрочем, справедливости ради стоит отметить, что подавляющее большинство **троянских** коней, осуществляющих шпионаж, записывают только последовательность нажатых клавиш. Во-первых, это — самая критичная информация. Именно так можно узнать пароли пользователя, например, к различным онлайновым сервисам: электронной почте, интернет-магазинам и т. п. А получив их, злоумышленник сможет в будущем спокойно пользоваться этими ресурсами от имени жертвы. Во-вторых, список нажатых клавиш занимает относительно малый объем. А чем меньше данных, тем проще незаметно передать их на компьютер хакера.

**Переходы на страницы**

Некоторые трояны заставляют пользователя открывать определенные веб-сайты

Сегодня в Интернете существует немало партнерских программ. Суть их заключается в следующем. Человек привлекает на сайт спонсора посетителей, за каждого из которых получает небольшое вознаграждение. В принципе партнерские программы — явление абсолютно нормальное. Но только до тех пор, пока обе стороны соблюдают правила и придерживаются общепринятых норм. Между тем многие ресурсы с контентом «только для взрослых» смотрят на действия партнеров сквозь пальцы, в результате чего происходит следующее.

Некоторые люди для получения максимального заработка используют **троянских** коней. То есть они заражают компьютеры интернетчиков такими зловредными программами, которые постоянно изменяют домашнюю страницу в браузере на адрес сайта партнера, при переходе на который тут же открываются еще несколько всплывающих окон с веб-проектами спонсоров. Кроме того, такие **троянские** **кони** способны самостоятельно инициировать открытие заданного им адреса при наступлении некоторых событий (подключение к Интернету, открытие нового окна браузера и т. п.).

**Проведение атак**

Троянские **кони** используются для проведения DDoS-атак

|  |
| --- |
|  |

Наиболее распространенным типом удаленных атак на сегодняшний день являются распределенные атаки, направленные на отказ сервера в обслуживании (DDoS-атаки). Суть их заключается в следующем. Злоумышленники обрушивают на сервер-жертву огромное множество специально созданных сетевых пакетов. В результате компьютер просто-напросто не справляется с этим потоком и перестает обрабатывать информацию, то есть становится недоступным для простых посетителей. Однако создать с одного компьютера настолько большое число потоков, чтобы полностью загрузить сервер, невозможно. Да и для хакеров это опасно.

Поэтому чаще всего злоумышленники действуют по следующей схеме. Сначала они заражают специальным троянским конем как можно большее число машин обычных интернетчиков. Эта зловредная программа до поры до времени живет на ПК, ничем себя не выдавая и не совершая никаких деструктивных действий. Однако при получении специальной команды от управляющего центра троян активизируется и начинает отправку на указанную жертву требуемых для атаки пакетов. А поскольку таких компьютеров может быть сотни и тысячи, то нет ничего удивительного в том, что сервер «падает». В принципе для самого пользователя **троянские** **кони** этого класса практически не опасны. За исключением того момента, что во время их работы достаточно серьезно загружается его канал. Кроме того, мало кому из интернетчиков доставит удовольствие тот факт, что он фактически стал соучастником преступления.

**Загрузка и инсталляция другого ПО**

**Троянские** **кони** могут использоваться для загрузки другого зловредного ПО на компьютер пользователя и его инсталляции

В последнее время требования к зловредному ПО изменились. Если раньше все вирусы были очень маленькими, то современные **троянские** кони **могут** иметь достаточно большой размер. Это обусловлено большой их функциональностью (например, программы-шпионы и утилиты удаленного администрирования) и используемыми технологиями. Между тем далеко не всегда удается незаметно загрузить на компьютер пользователя такие объемы информации. Поэтому хакеры стали использовать следующий прием. Сначала ПК заражается довольно маленькой утилитой, которая устанавливает связь с определенным сервером, скачивает оттуда другое зловредное ПО, инсталлирует и запускает его. Особенно опасны в этом плане универсальные загрузчики. Они позволяет злоумышленнику устанавливать на ПК жертвы разные **троянские** *кони* или даже целый их букет. Все зависит от того, что в данный момент лежит на указанном сервере.

**Подводим итоги**

Итак, как мы с вами, уважаемые читатели, убедились, современные **троянские** кони действительно представляют собой серьезную угрозу безопасности любого компьютера, подключенного к Глобальной сети. Причем необходимо учитывать, что сегодня существуют программы, относящиеся сразу к двум, трем, а то и к большему количеству классов. Такие трояны могут, например, следить за пользователем, тайно загружать и устанавливать на его компьютере другое ПО и участвовать в атаках. Между тем защититься от этой угрозы в общем-то несложно. Регулярно обновляемой антивирусной программы, правильно настроенного файрвола и периодического обновления операционной системы и используемого ПО для этого вполне достаточно.