**Реферат по информатике**

**на тему: “Троянский вирус”**

**Выполнил: Ученик 9 «А» класса**

**Школы № 50**

**Рыжков Максим**

**Троянские кони, утилиты скрытого администрирования, intended-вирусы, конструкторы вирусов и полиморфные генераторы.**

**История возникновения названия «троянский конь».**

В XII столетии до н.э. Греция объявила войну Трое. Греки начали 10-летнюю войну против этого города, но так и не смогли его взять. Тогда они пошли на хитрость. По совету Одиссея был сооружен огромный деревянный конь. Внутри этого коня спряталось несколько героев, а ахейское войско, погрузившись на корабли, отплыло к острову Тендос. Троянцы решили, что осада снята и, поверив словам лазутчика Синона о том, что конь оставлен ахейцами для того, чтобы умилостивить богиню Афину, и обладание им сделает Трою неприступной, перенесли его в город, разрушив при этом часть крепостной стены. Напрасно жрец Лаокоон убеждал троянцев, что этого не следует делать. Ночью из чрева коня вышли воины-ахейцы и открыли городские ворота вернувшемуся под покровом темноты войску. Троя была взята и разрушена.

Вот почему подобные программы называют "троянскими конями" — они работают незаметно для пользователя ПК, прикрываясь действиями других приложений.

**Что такое троянский конь?**

Троянский конь — это программа, которая предоставляет посторонним доступ к компьютеру для совершения каких-либо действий на месте назначения без предупреждения самого владельца компьютера либо высылает по определенному адресу собранную информацию. При этом она, как правило, выдает себя за что-нибудь мирное и чрезвычайно полезное. Часть троянских программ ограничивается тем, что отправляет ваши пароли по почте своему создателю или человеку, который сконфигурировал эту программу (е-mail trojan). Однако для пользователей Internet наиболее опасны программы, позволяющие получить удаленный доступ к их машине со стороны (BackDoor). Очень часто трояны попадают на компьютер вместе с полезными программами или популярными утилитами, маскируясь под них.

Особенностью этих программ, заставляющей классифицировать их как вредные, является отсутствие предупреждения об их инсталляции и запуске. При запуске троян устанавливает себя в систему и затем следит за ней, при этом пользователю не выдается никаких сообщений о его действиях. Более того, ссылка на троянца может отсутствовать в списке активных приложений или сливаться с ними. В результате пользователь компьютера может и не знать о его присутствии в системе, в то время как компьютер открыт для удаленного управления. Достаточно часто под понятием "троян" подразумевается вирус. На самом деле это далеко не так. В отличие от вирусов, трояны направлены на получение конфиденциальной информации и доступ к определенным ресурсам компьютера.

Возможны различные пути проникновения трояна в вашу систему. Чаще всего это происходит при запуске какой-либо полезной программы, в которую внедрен сервер трояна. В момент первого запуска сервер копирует себя в какую-нибудь директорию, прописывает себя на запуск в системном реестре, и даже если программа-носитель никогда больше не запустится, ваша система уже заражена трояном. Заразить машину можете вы сами, запустив зараженную программу. Обычно это происходит, если программы скачиваются не с официальных серверов, а с личных страничек. Внедрить трояна могут также посторонние люди при наличии доступа к вашей машине, просто запустив его с дискеты.

**Типы Троянов**

На данный момент наибольшее распространение получили трояны следующих типов:

**1. Утилиты скрытого (удаленного) администрирования (BackDoor — с англ. "задняя двеpь").**

Троянские кони этого класса по своей сути являются достаточно мощными утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые известными фирмами — производителями программных продуктов.

Единственная особенность этих программ заставляет классифицировать их как вредные троянские программы: отсутствие предупреждения об инсталляции и запуске.

При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянца в системе. Более того, ссылка на троянца может отсутствовать в списке активных приложений. В результате "пользователь" этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Современные утилиты скрытого администрирования (BackDoor) достаточно просты в использовании. Они обычно состоят главным образом из двух основных частей: сервера (исполнитель) и клиента (управляющий орган сервера).

Сервер — это исполняемый файл, который определенным образом внедряется на вашу машину, загружается в память одновременно с запуском Windows и выполняет получаемые от удаленного клиента команды. Сервер отправляется жертве, и в дальнейшем вся работа ведется через клиента на компьютере хакера, т.е. через клиента посылаются команды, а сервер их выполняет. Внешне его присутствие никак не обнаруживается. После запуска серверной части трояна на компьютере пользователя резервируется определенный порт, отвечающий за связь с Интернетом.

После этих действий злоумышленник запускает клиентскую часть программы, подключается к этому компьютеру через открытый в онлайне порт и может выполнять на вашей машине практически любые действия (это ограничивается лишь возможностями используемой программы). После подключения к серверу управлять удаленным компьютером можно практически как своим: перезагружать, выключать, открывать CD-ROM, удалять, записывать, менять файлы, выводить сообщения и т.д. На некоторых троянах можно изменять открытый порт в процессе работы и даже устанавливать пароль доступа для "хозяина" данного трояна. Существуют также трояны, которые позволяют использовать "затрояненную" машину в качестве прокси-сервера (протоколы HTTP или Socks) для сокрытия реального IP-адреса хакера.

В архиве такого трояна обычно находится 5 следующих файлов: клиент, редактор для сервера (конфигуратор), сервер трояна, упаковщик (склейщик) файлов, файлы документации. У него достаточно много функций, среди которых можно выделить следующие:  
1) сбор информации об операционной системе;

2) определение кэшированных и dial-up-паролей, а также паролей популярных программ дозвона;

3) нахождение новых паролей и отправка другой информации на е-mail;

4) скачивание и запуск файлов по указанному пути;

5) закрывание окон известных антивирусов и файрволлов при обнаружении;

6) выполнение стандартных операций по работе с файлами: просмотра, копирования, удаления, изменения, скачивания, закачивания, запуска и воспроизведения;

7) автоматическое удаление сервера трояна из системы через указанное количество дней;

8) управление CD-ROM, включение/отключение сочетания клавиш Ctrl+Alt+Del, просмотр и изменение содержимого буфера обмена, сокрытие и показ таскбара, трея, часов, рабочего стола и окон;

9) установление чата с жертвой, в т.ч. для всех пользователей, подключенных к данному серверу;

10) отображение на экране клиента всех нажатых кнопок, т.е. имеются функции клавиатурного шпиона;

11) выполнение снимков экрана разного качества и размера, просмотр определенной области экрана удаленного компьютера, изменение текущего разрешения монитора.

Трояны скрытого администрирования и сейчас наиболее популярны. Каждому хочется стать обладателем такого трояна, поскольку он может предоставить исключительные возможности для управления и выполнения различных действий на удаленном компьютере, которые могут напугать большинство пользователей и доставить уйму веселья хозяину трояна. Очень многие используют трояны для того, чтобы просто поиздеваться над кем-нибудь, выглядеть в глазах окружающих "суперхакером", а также для получения конфиденциальной информации.

**2. Почтовые (е-mail trojan).**

Трояны, позволяющие "вытаскивать" пароли и другую информацию из файлов вашего компьютера и отправлять их по электронной почте хозяину. Это могут быть логины и Internet-пароли провайдера, пароль от почтового ящика, пароли ICQ и IRC и др.  
Чтобы отправить письмо владельцу по почте, троян связывается с почтовым сервером сайта по протоколу SMTP (например, на smtp.mail.ru). После сбора необходимых данных троян проверит, отсылались ли эти данные. Если нет — данные отсылаются и сохраняются в регистре. Если уже отсылались, то из регистра извлекается предыдущее письмо, и происходит его сравнение с текущим. Если в информации произошли какие-либо изменения (появились новые данные), то письмо отсылается, и в регистре записываются свежие данные о паролях. Одним словом, этот вид троянов просто занимается сбором информации, и жертва может даже и не догадываться, что ее пароли уже кому-то известны.  
В архиве такого трояна обычно находится 4 файла: редактор сервера (конфигуратор), сервер трояна, упаковщик (склейщик) файлов, руководство для использования.

В результате работы могут определяться следующие данные:

1) IP-адрес компьютера жертвы;

2) подробнейшие сведения о системе (имя компьютера и пользователя, версия Windows, модем и т.д.);

3) все кэшированные пароли;

4) все настройки телефонных соединений включая телефонные номера, логины и пароли;  
5) пароли от ICQ;

6) N последних посещенных сайтов.

**3. Клавиатурные (Keylog-gers).**

Эти трояны записывают все, что было набрано на клавиатуре (включая пароли) в файл, который впоследствии отправляется на определенный е-mail или пpосматpивается чеpез FTP (File Transfer Protocol). Keylogger'ы обычно занимают мало места и могут маскироваться под другие полезные программы, из-за чего их бывает трудно обнаружить. Еще одной причиной трудности обнаружения такого трояна является то, что его файлы называются как системные. Некоторые трояны этого типа могут выделять и расшифровывать пароли, найденные в специальных полях для ввода паролей.

Такие программы требуют ручной настройки и маскировки. Keylogger'ы можно использовать не только в хулиганских целях. Например, их очень удобно поставить на своем рабочем месте или дома на время отъезда.

**4. Программы-шутки (Joke programs).**

Эти программы безвредны по своей сути. Они не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, может быть причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. Программы-шутки запугивают пользователя сообщениями о форматировании жесткого диска, определяют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т.д. — это зависит от чувства юмора создателя такой программы. Конечно же, тут нет никаких причин для волнения, если за этим компьютером не работают другие неопытные пользователи, которых подобные сообщения могут сильно напугать.

**5.** К "троянским коням" также можно отнести зараженные файлы, код которых определенным образом подправлен или изменен криптографическим методом. Например, файл шифруется специальной программой и (или) упаковывается неизвестным архиватором. В итоге даже последние версии антивирусов не могут определить наличие в файле трояна, так как носитель кода отсутствует в их антивирусной базе.

**Защита от троянов (платформа Windows)**

Обнаружить работу современной троянской программы на своем компьютере достаточно сложно. Однако можно выделить следующие рекомендации для обнаружения и удаления троянских программ:

1. Используйте антивирусную программу.

Обязательно используйте антивирусную программу для проверки файлов и дисков, регулярно обновляя при этом ее антивирусную базу через Интернет. Если база не обновляется, результат работы антивируса сводится к нулю, поскольку новые трояны появляются с не меньшей регулярностью, чем обновления антивирусных баз.  
Поэтому этот метод нельзя признать абсолютно надежным. Иногда, как показывает практика, если сервер трояна внедрен в исполняемый файл, антивирусы во многих случаях не могут его обнаружить. На сегодняшний момент с наилучшей стороны в этом плане зарекомендовали себя антивирусы Kaspersky Anti-Virus и Dr. Web.

Наряду с антивирусами существуют специализированные программы (антигены), которые могут найти, определить и уничтожить большую часть троянов, однако бороться с ними становится все сложнее и сложнее. В качестве такой программы, предназначенной для поиска и уничтожения троянов на вашем компьютере, можно порекомендовать Trojan Hunter.

2. Установите персональный брандмауэр (файрволл) и внимательно разберитесь в его настройках. Основным признаком работы трояна являются лишние открытые порты. При запуске сервера троянской программы файрволл изнутри заблокирует ее порт, лишив тем самым связи с Интернетом. Файрволл дает дополнительную защиту, однако, с другой стороны, пользователю просто надоедает постоянно отвечать на запросы программы по поводу работы определенного сервиса и прохождения данных через определенный порт. Иногда бывают крайние случаи, когда даже файрволл и антивирус бессильны что-либо предпринять, так как закрываются трояном. Это также является сигналом пользователю о том, что в системе присутствует троян.

Для контроля открытых портов можно также воспользоваться сканерами портов или программами, которые показывают открытые в настоящий момент порты и возможное подключение к ним посторонних пользователей.

Из файрволлов достаточно качественным продуктом является Agnitum Outpost Firewall Pro, позволяющий настроить работу приложений и необходимый пользовательский уровень.

3. Ограничьте число посторонних, имеющих доступ к вашему компьютеру, поскольку достаточно большое число троянов и вирусов переносится на внешних носителях (дискетах и дисках). Также рекомендуется периодически менять пароли на особо важные аккаунты.

4. Не скачивайте файлы и фотографии с сомнительных сайтов (домашние странички с фото и т.д.). Достаточно часто фотография и сервер трояна скреплены ("склеены") вместе для усыпления бдительности пользователя, и этот фактор не вызывает сомнений. Здесь троян маскируется под картинку. При этом иконка действительно будет от картинки, но вот расширение останется \*.ехе. После двухкратного нажатия на фотографию троян запускается и делает свое черное дело.

5. Не следует использовать сомнительные программы, якобы ускоряющие работу компьютера в Интернете в N раз (ускоряющие работу CD-ROM, мыши, коврика для мыши и т.п.). При этом внимание необходимо обратить на иконку программы, особенно если вы ни с кем заранее не договаривались. В этом случае можно задать вопрос отправителю, и, если положительного ответа не последовало, удалять такую программу.

6. При получении письма от неизвестного адресата следует обратить особое внимание на расширение вложенного файла. Возможна маскировка названия завирусованного расширения файла \*.exe, \*.jpg, \*.bat, \*.com, \*.scr, \*.vbs двойным окончанием (\*.doc .exe), причем буквы .exe могут быть разделены большим количеством пробелов или перенесены на следующую строку.

При получении письма с прикрепленным архивом (файл с расширениями \*.rar, \*.zip, \*.arj) не следует сразу его открывать и просматривать файлы. По возможности его надо сохранить на диск, после чего проверить антивирусной программой и только после этого открыть. Если в архиве обнаружен вирус, необходимо немедленно удалить весь архив, не пытаясь его сохранять или, тем более, открывать файлы.

7. Если вы пользуетесь системой Windows XP, то при риске открыть зараженный файл создайте точку восстановления. Для Windows 98 рекомендуется установить аналогичную программу, позволяющую произвести откат системы назад (например, Second Chance или другую подобного типа).

8. При использовании стандартного почтового клиента Windows (Microsoft Outlook Express) следует отключить автоматическое получение почты, которое может запустить закодированного трояна, находящегося в теле (внутри) письма. Вместо программы Outlook Express вы также можете использовать более безопасный и быстрый почтовый клиент The Bat!, являющийся одним из лучших.

9. Осуществляйте контроль задач и сервисов, запускаемых в системе. Практика показывает, что 99% троянов прописываются на запуск в системном реестре. Для эффективного удаления трояна из системы нужно сначала удалить запись в реестре или строку, его запускающую, затем перезагрузить компьютер, а уж затем спокойно удалять этот файл.

10. Если ПК ведет себя подозрительно, а продолжать работу необходимо, вводите вручную свой логин и пароль в окнах, минуя сохранение их в браузере или в почтовом клиенте.

11. Желательно делать копии важных файлов, сохраняя их на дискете или CD-диске. Это поможет быстро восстановить утраченные данные при возможном крахе системы и последующем форматировании жестких дисков.

**Intended-вирусы**

К таким вирусам относятся программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножаться по причине ошибок.

Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (что в подавляющем большинстве случаев завешивает компьютер) и т.д.

К категории "intended" также относятся вирусы, которые по приведенным выше причинам размножаются только один раз - из "авторской" копии. Заразив какой-либо файл, они теряют способность к дальнейшему размножению.

Появляются intended-вирусы чаще всего при неумелой перекомпиляции какого-либо уже существующего вируса, либо по причине недостаточного знания языка программирования, либо по причине незнания технических тонкостей операционной системы.

**Конструкторы вирусов**

Конструктор вирусов - это утилита, предназначенная для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS, Windows и макро-вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули, и/или непосредственно зараженные файлы.

Некоторые конструктороы (VLC, NRLG) снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты (COM и/или EXE), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса и т.п. Прочие конструкторы (PS-MPC, G2) не имеют интерфейса и считывают информацию о типе вируса из конфигурационного файла.

**Полиморфные генераторы**

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т.е. открытия, закрытия и записи в файлы, чтения и записи секторов и т.д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

Обычно полиморфные генераторы распространяются их авторами без ограничений в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор. Во всех встречавшихся генераторах этот модуль содержит внешнюю (external) функцию - вызов программы генератора.

Таким образом автору вируса, если он желает создать настоящий полиморфик-вирус, не приходится корпеть над кодами собственного за/расшифровщика. При желании он может подключить к своему вирусу любой известный полиморфик-генератор и вызывать его из кодов вируса. Физически это достигается следующим образом: объектный файл вируса линкуется с объектным файлом генератора, а в исходный текст вируса перед командами его записи в файл вставляется вызов полиморфик-генератора, который создает коды расшифровщика и шифрует тело вируса.