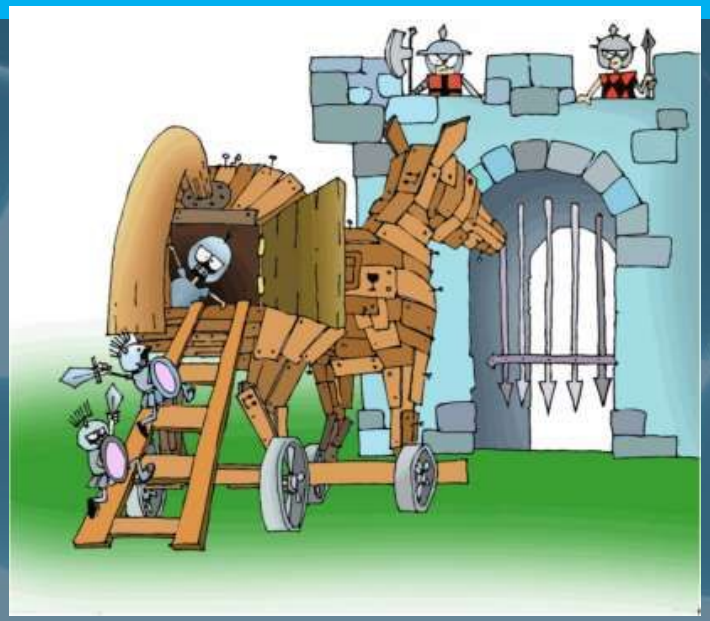
Троя́нская программа (также — **троя́н**, **троя́нец**, **троя́нский конь**) — вредоносная программа, распространяемая людьми.
В отличие от вирусов и червей, которые распространяются самопроизвольно.
Название «троянская» восходит к легенде о «Троянском коне» — дарёном деревянном коне, послужившим причиной падения Трои.

Троянская программа

В коне, подаренном в знак лже-перемирия, прятались греческие воины, ночью открывшие ворота армии завоевателя. Больша́я часть троянских программ действует подобным образом — маскируется под безвредные или полезные программы, чтобы пользователь запустил их на своем компьютере.



Троянская программа

.

Трояны — самый простой вид вредоносных программ, сложность которых зависит исключительно от сложности истинной задачи и средств маскировки. Самые примитивные экземпляры (например, стирающие содержимое диска при запуске) могут иметь исходный код в несколько строк.

Вредоносное действие

Как и любая вредоносная программа, троян может делать практически все, что угодно, например:

- мешать работе пользователя
- воровать или уничтожать данные и регистрационную информацию (пароли, кредитные карты)
- вымогать деньги (за возможность работы или сохранность данных)
- шпионить за пользователем
- использовать ресурсы компьютера (в том числе сетевые соединения), в том числе для противозаконной деятельности

и т.д. и т.п.

Маскировка

Троянская программа может имитировать имя и иконку существующей, несуществующей, или просто привлекательной программы, компонента, или файла данных (например картинки), как для запуска пользователем, так и для маскировки в системе своего присутсвия.

Троянская программа может в той или иной мере имитировать или даже полноценно выполнять задачу, под которую она маскируется (в последнем случае вредоносный код встраивается злоумышленником в существующую программу).

Методы удаления

В целом, троянские программы обнаруживаются и удаляются антивирусаным и антишпионским ПО точно так же как и остальные вредоностные программы.

Троянские программы хуже обнаруживаются контекстными методами антивирусов (основанных на поиске известных программ), потому что их распространение лучше контролируется, и экземпляры программ попадают к специалистам антивирусной индустрии с бóльшей задержкой, нежели самопроизвольно распространяемые вредоносные программы. Однако эвристические (поиск алгоритмов) и проативные (слежение) методы для них столь же эффективны.

Типы троянов

На данный момент наибольшее распространение получили трояны следующих типов:

1. Утилиты скрытого (удаленного) администрирования (BackDoor — с англ. "задняя дверь").
Троянские кони этого класса по своей сути являются достаточно мощными утилитами удаленного администрирования компьютеров в сети.

Типы троянов

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 e-mail;

Типы троянов

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;

Типы троянов

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.

Типы троянов

2. Почтовые (e-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.

Типы троянов

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.

Типы троянов

3. Клавиатурные (Keylog-gers).
Эти трояны записывают все, что было набрано на клавиатуре (включая пароли) в файл, который впоследствии отправляется на определенный e-mail или просматривается через 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.

Типы троянов

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.

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.

Защита от троянов (платформа Windows)

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.

Защита от троянов (платформа Windows)

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 *.exe. После двухкратного нажатия на фотографию троян запускается и делает свое черное дело.

Защита от троянов (платформа Windows)

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.

Защита от троянов (платформа Windows)

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.

Защита от троянов (платформа Windows)

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.