



# Троянская программа

Название «тройанская программа» происходит от названия «тройанский конь» — деревянный конь, по легенде, подаренный древними греками жителям Трои, внутри которого прятались воины, впоследствии открывшие завоевателям ворота города. Такое название, прежде всего, отражает скрытность и потенциальную коварность истинных замыслов разработчика программы.

Выполнила: Брянцева Ольга 10 Б

Учитель: Мухатдинова Г.Н.

# Троянская программа

(троян, троянец, троянский конь) — вредоносная программа, используемая злоумышленником для сбора информации, её разрушения или модификации, нарушения работоспособности компьютера или использования

его ресурсов в  
неблаговидных целях.



Вредоносные и маскировочные функции используются компьютерными вирусами, но в отличие от них, троянские программы не умеют распространяться самостоятельно. Вместе с тем, она может быть модулем вируса

Троянская программа запускается пользователем вручную или автоматически — программой или частью операционной системы, выполняемой на компьютере-жертве (как модуль или служебная программа). Для этого файл программы называют служебным именем, маскируют под другую программу файл другого типа или просто дают привлекательное для запуска название и иконку



Простым примером трояна может являться программа `waterfalls.scr`, чей автор утверждает, что это бесплатная экранная заставка. При запуске она загружает скрытые программы, команды и скрипты без согласия и ведома пользователя. Троянские программы часто используются для обмана систем защиты, в результате чего система становится уязвимой, позволяя таким образом неавторизованный доступ к компьютеру пользователя.



# Распространение

Троянские программы помещаются злоумышленником на открытые ресурсы (файл-серверы) носители информации или присылаются с помощью служб обмена сообщениями (например, электронной почтой) из расчета на их запуск на конкретном, входящем в определенный круг или произвольном «целевом» компьютере.

Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определенные компьютеры,  
сети или ресурсы



# Типы тел троянских программ

Тела троянских программ почти всегда разработаны для различных вредоносных целей, но могут быть также безвредными. Они разбиваются на категории, основанные на том, как трояны внедряются в систему и наносят ей вред. Существует 6 главных типов:

1. удалённый доступ;

2. уничтожение данных;

3. загрузчик;

4. сервер;

5. дезактиватор программ безопасности;

6. DoS-атаки.

# Цели

## □ Целью троянской программы может быть:

- \* закичивание и скачивание файлов;
- \* копирование ложных ссылок, ведущих на поддельные вебсайты, чаты или другие сайты с регистрацией;
- \* создание помех работе пользователя (в шутку или для достижения других целей);
- \* выуживание деталей касательно банковских счетов, которые могут быть использованы в преступных целях,
- \* похищение данных, представляющих ценность или тайну, в том числе информации для аутентификации, для несанкционированного доступа к ресурсам
- \* шифрование файлов при кодовirusной атаке;
- \* вандализм: уничтожение данных (стирание или переписывание данных на диске, труднозамечаемые повреждения файлов) и оборудования, выведения из строя или отказа обслуживания компьютерных систем, сетей и т.д

# *Симптомы заражения тroyном*

- \* появление в реестре автозапуска новых приложений;
- \* показ фальшивой загрузки видеопрограмм, игр, которые вы не закатывали и не посещали;
- \* создание снимков экрана;
- \* открывание и закрывание консоли CD-ROM;
- \* проигрывание звуков и/или изображений, демонстрация фотоснимков;
- \* перезапуск компьютера во время старта инфицированной программы;
- \* случайное и/или беспорядочное отключение компьютера.



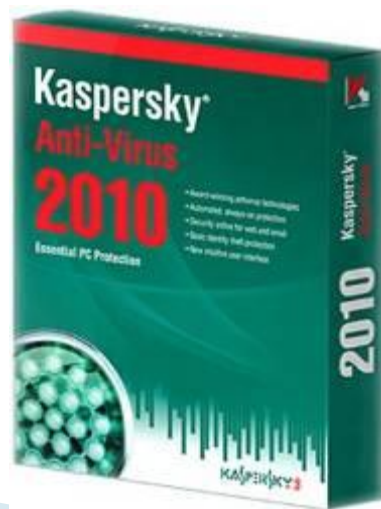
# Маскировка

Многие трояны могут находиться на компьютере пользователя без его ведома. Иногда трояны прописываются в Реестре, что приводит к их автоматическому запуску при старте Windows. Также они могут комбинироваться с легитимными файлами. Когда пользователь открывает такой файл или запускает приложение, троян запускается также.



# Методы удаления

Поскольку трояны обладают множеством видов и форм, не существует единого метода их удаления. Наиболее простое решение заключается в очистке папки Temporary Internet Files или нахождении вредоносного файла и удаление его вручную (рекомендуется Безопасный Режим). В принципе, антивирусные программы способны обнаруживать и удалять трояны автоматически. Чрезвычайно важно для обеспечения бóльшей точности обнаружения регулярное обновление антивирусной базы данных.



**СПАСИБО ЗА ВНИМАНИЕ !**

