

Российский Университет Дружбы Народов имени Патриса Лулумбы

**Факультет физико-математических и естественных наук**

**Основы информационной безопасности**

**Доклад на тему  
«Вредоносные программы. Троянские программы.»**

Докладчик:  
Лушин Артём Андреевич  
НКАбд-01-22

Преподаватель:  
Кулябов Дмитрий Сергеевич

Москва, 2024г.

## **Содержание:**

1) Введение:	стр 3
2) Происхождение	стр 3
3) Цели и распространение	стр 3-4
4) Защита	стр 4-5
5) Литература	стр 6

## **Введение:**

Троянская вирусная программа (также — троян) — разновидность вредоносные программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации о банковских картах, передача этой информации злоумышленнику, а также использование, удаление или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в целях майнинга, использование IP для нелегальной торговли. Также троянские программы могут всецело оставаться на компьютере, даже после полной переустановки Windows.

## **Происхождение:**

Свое общее название троянские программы получили за сходство механизма проникновения в компьютер пользователя с описанным в эпизоде Илиады, рассказывающем о «Троянском коне» — дарёном деревянном коне, использованном для проникновения в Трою, что и стало причиной падения Трои. В Коне, подаренном в знак лже-перемирия, спрятались воины Одиссея, ночью выбравшиеся из Коня и открывшие ворота основным силам объединённой греческой армии. Большая часть троянских программ действуют подобным образом — маскируется под безвредные или полезные программы, чтобы пользователь запустил их на своем компьютере. Считается, что первым этот термин в контексте компьютерной безопасности употребил в своём отчёте «Computer Security Technology Planning Study» Дэниэл Эдвардс.

## **Цели и распространение:**

Целью троянской программы может быть:

закачивание и скачивание файлов;

копирование и подача пользователю ПК ложных ссылок, ведущих на поддельные веб-сайты, чаты или другие сайты с регистрацией;

создание помех работе пользователя;

кража данных, представляющих ценность или тайну, в том числе информации для аутентификация, для не санкционируемого доступа к ресурсам, выуживание деталей касательно банковских счетов, которые могут быть использованы в преступных целях;

распространение других вредоносных программ, чаще всего таких, как вирусы или черви;

уничтожение данных (стирание или переписывание данных на диске, трудно замечаемые повреждения файлов) и оборудования, выведения из строя или отказа обслуживания компьютерных систем, сетей;

сбор адресов электронной почты и использование их для рассылки спама;

слежка за пользователем и тайное сообщение злоумышленникам о посещении конкретных сайтов;

регистрация нажатий клавиш с целью кражи информации такого рода как пароли и номера кредитных карточек;

дезактивация или создание помех работе антивирусных программ и файервола;

для самоутверждения вирусодела, из мести или просто «повеселиться».

Троянские программы распространяются как злоумышленниками-инсайдерами (непосредственно загружаются в компьютерные системы), так и пользователями (побуждают загружать или запускать их на своих системах).

Для достижения последнего троянские программы помещаются злоумышленниками на открытые или индексируемые ресурсы (системы файлообмена), присылаются с помощью служб обмена сообщениями, попадают на компьютер через брешы безопасности или загружаются самим пользователем с адресов, полученных одним из перечисленных способов.

Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определённые компьютеры, сети или ресурсы (в том числе, третьи).

## **Защита**

Два главных совета — быть внимательным и понять, как трояны попадают на компьютер или смартфон. Разберём основные способы защиты, снижающие риск заражения.

Своевременно загружайте обновления системы. Они закрывают дыры в безопасности, добавляют новые функции и обновляют базы данных встроенного антивируса.

Не ведитесь на фишинг. Не скачивайте и не открывайте вложения в электронных письмах, полученных от неизвестного человека, и помните,

что злоумышленники любят маскировать опасные письма под рассылку от любимого магазина.

Скачивайте проверенное программное обеспечение и только с официальных сайтов. Если скачивать программы с торрентов или неофициальных сайтов, то есть риск получить зловреда на свой компьютер.

Если вы пользователь Windows, не устанавливайте системы собранные сторонними командами разработчиков. Чаще всего это усечённые образы Windows, где вырезана часть стандартных приложений, таких как «Защитник Windows», «Брандмауэр», и отключены автоматические обновления, а также контроль учётных записей. Такие системы — идеальная цель для троянов.

## Литература:

Основная информация взята с источника 1. Дополнительная информация с источника 2.

- 1) [Троянская программа — Википедия \(wikipedia.org\)](#)
- 2) [Троян: что это, чем опасен, как защитить компьютер от троянских программ / Skillbox Media](#)