

# Взлом компьютерных систем с помощью вирусов



# ОПРЕДЕЛЕНИЕ

*Компьютерный вирус — вид вредоносного программного обеспечения, способный создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а так же распространять свои копии по разнообразным каналам связи, с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведение в негодность аппаратных комплексов компьютера.*



# Классификация

Ныне существует немало разновидностей вирусов, разл по основному способу распространения и функциональности

Растёт и функциональность вирусов, которую они пере других видов программ.

В настоящее время не существует единой системы классификации и именования вирусов. Принято разделять вирусы:

- по поражаемым объектам (файловые вирусы, загрузочные вирусы, скриптовые вирусы, макровирусы, вирусы, поражающие исходный код);
- файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
- по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);
- по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, скриптовый язык);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты).



# Примеры компьютерных вирусов



- Penetrator (файловый вирус)
- Троянская программа (загрузочный)
- Macro.Word97.Thus (макровирус)
- Trojan.Winlock.6412 (загрузочный)



# Penetrator

*Компьютерный вирус, созданный российским студентом Дмитрием Уваровым. Вирус был написан на Visual Basic и предназначался для операционных систем Windows с процессором x86. Данный вирус внедряется в операционную систему и выполняет деструктивные действия над файлами .avi, .doc, .jpg, .jpeg, .mp3, .mpeg, .mpg, .pdf, .rar, .vob, .zip, в ночь на первое января.*

## **Характеристика:**

*Вирус распространяется с помощью файла flash.scr, тем самым маскируясь под программу — скринсейвер. Также были отмечены единичные случаи, когда вирус маскировался под файл mp3.*

*При запуске исполняемого файла вирус внедряется в папку «\Documents and Settings\All Users\Документы\», файлом Documents.scr, для операционной системы Windows XP, предварительно внедряясь в оперативную память и в раздел автозагрузки. Заражение файлов начинается лишь 1 января.*



WALLPAPERS

Файл Правка Вид Избранное Сервис Справка



Адрес:

abstract\_077..jpg

Acid\_Sun.jpg

AmberWaves1-0.jpg

Animorph.jpg

future\_mood\_2.jpg

g0\_smoke.jpg

Penetrator

Penetrator

Penetrator

Penetrator

Penetrator

Penetrator

Galactica1-0.jpg

GOLDIE.jpg

gravity\_well.jpg

IMG2.JPG

IMG78.JPG

Into-r.jpg

Penetrator

Penetrator

Penetrator

Penetrator

Penetrator

Penetrator

Light\_Sphere.jpg

LightWarp1-0.jpg

NeonDisaster1-0.jpg

Nissan Skilne GTR  
R35.jpg

Provenance1-0.jpg

фотка.jpg

Penetrator

Penetrator

Penetrator

Penetrator

Q2\_Image3.bmp

Q2\_Image4.bmp

time\_has\_no\_meaning...

фотка.jpg

Объектов: 70

4,32 МБ

Интернет

# Троянская программа

**Троянская программа** (также — **троя́н, троя́нец, троя́нский конь**) — вредоносная программа, распространяемая людьми, в отличие от вирусов и червей, которые распространяются самопроизвольно.

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

## **Распространение:**

Троянские программы распространяются людьми — как непосредственно загружаются в компьютерные системы злоумышленниками-инсайдерами, так и побуждают пользователей загружать и/или запускать их на своих системах.

Для достижения последнего, троянские программы помещаются злоумышленниками на открытые или индексируемые ресурсы (файл-серверы и системы файлообмена), носители информации, присылаются с помощью служб обмена сообщениями (например, электронной почтой), попадают на компьютер через бреши безопасности или загружаются самим пользователем с адресов полученных одним из перечисленных способов.

## **Целью троянской программы может быть:**

- ▣ *закачивание и скачивание файлов*
- ▣ *копирование ложных ссылок, ведущих на поддельные веб-сайты, чаты или другие сайты с регистрацией*
- ▣ *создание помех работе пользователя*
- ▣ *похищение данных, представляющих ценность или тайну, в том числе информации для аутентификации, для несанкционированного доступа к ресурсам, выуживание деталей касательно банковских счетов, которые могут быть использованы в преступных целях*
- ▣ *распространение других вредоносных программ*
- ▣ *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*
- ▣ *шпионство за пользователем и тайное сообщение третьим лицам сведений, таких как, например, привычка посещения сайтов*
- ▣ *дезактивация или создание помех работе антивирусных программ*



# Macro.Word97.Thus

Макро-вирус, содержит три процедуры

- Document\_Open
- Document\_Close
- Document\_New

Заражает область системных макросов при открытии зараженного документа. Остальные документы заражает при их открытии, закрытии и создании.

13-го декабря вирус ищет и удаляет все файлы в корневом каталоге и всех подкаталогах диска C:







