

# ВИДЫ КОМПЬЮТЕРНЫХ ВИРУСОВ

Милюкова Анастасия, г.Рязань, школа №60  
"Презентация подготовлена для конкурса  
"Интернешка" <http://interneshka.org/>".

**ВИРУС**- ЭТО САМОВОСПРОИЗВОДЯЩАЯСЯ  
ПРОГРАММА, СПОСОБНАЯ ВНЕДРЯТЬСЯ В  
ДРУГИЕ ПРОГРАММЫ



# Мотивы, движущие создателями вирусов:

- Озорство и одновременно недопонимание всех последствий распространения вируса;
- Стремление «насолить» кому-либо;
- Неестественная потребность в совершении преступлений;
- Желание самоутвердиться;
- Уверенность в полной безнаказанности;
- Невозможность использовать свои знания и умения в конструктивном русле.

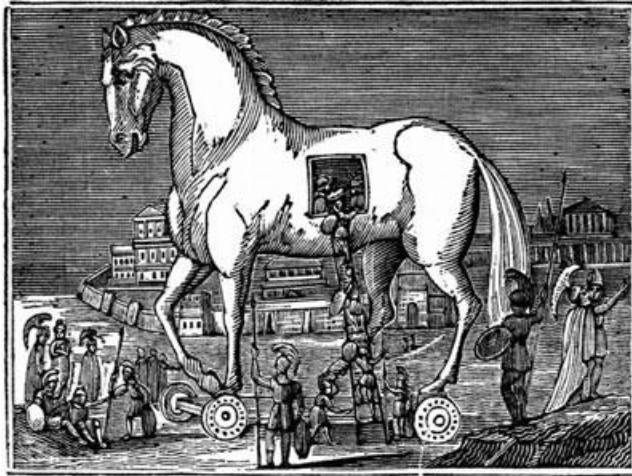


# ВИДЫ ВИРУСОВ

- ⦿ -Троянский конь
- ⦿ -Зомби
- ⦿ -Шпион
- ⦿ -Червь
- ⦿ -Руткиты
- ⦿ -Фишинг
- ⦿ -Фарминг

# ТРОЯНСКИЙ КОНЬ

- ◎ -это вредоносная программа, распространяемая людьми.
- ◎ «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. Примеры троянских программ: Back Orifice, Pinch, TDL-4, Trojan.Winlock.



*Trojans Deceived.*

ТРОЯНСКИЕ ПРОГРАММЫ РАСПРОСТРАНЯЮТСЯ ЛЮДЬМИ – КАК НЕПОСРЕДСТВЕННО ЗАГРУЖАЮТСЯ В КОМПЬЮТЕРНЫЕ СИСТЕМЫ ЗЛОУМЫШЛЕННИКАМИ-ИНСАЙДЕРАМИ, ТАК И ПОБУЖДАЮТ ПОЛЬЗОВАТЕЛЕЙ ЗАГРУЖАТЬ И/ИЛИ ЗАПУСКАТЬ ИХ НА СВОИХ СИСТЕМАХ.

ТРОЯНСКИЕ ПРОГРАММЫ ЧАЩЕ ВСЕГО РАЗРАБАТЫВАЮТСЯ ДЛЯ ВРЕДОНОСНЫХ ЦЕЛЕЙ. СУЩЕСТВУЕТ КЛАССИФИКАЦИЯ, ГДЕ ОНИ РАЗБИВАЮТСЯ НА КАТЕГОРИИ, ОСНОВАННЫЕ НА ТОМ, КАК ТРОЯНЫ ВНЕДРЯЮТСЯ В СИСТЕМУ И НАНОСЯТ ЕЙ ВРЕД.

СУЩЕСТВУЕТ 5 ОСНОВНЫХ ТИПОВ:

- УДАЛЁННЫЙ ДОСТУП
- УНИЧТОЖЕНИЕ ДАННЫХ
- ЗАГРУЗЧИК
- СЕРВЕР
- ДЕЗАКТИВАТОР ПРОГРАММ БЕЗОПАСНОСТИ

ЗАДАЧИ, КОТОРЫЕ МОГУТ ВЫПОЛНЯТЬ ТРОЯНСКИЕ ПРОГРАММЫ, БЕСЧИСЛЕННЫ, НО В ОСНОВНОМ ОНИ ИДУТ ПО СЛЕДУЮЩИМ НАПРАВЛЕНИЯМ:

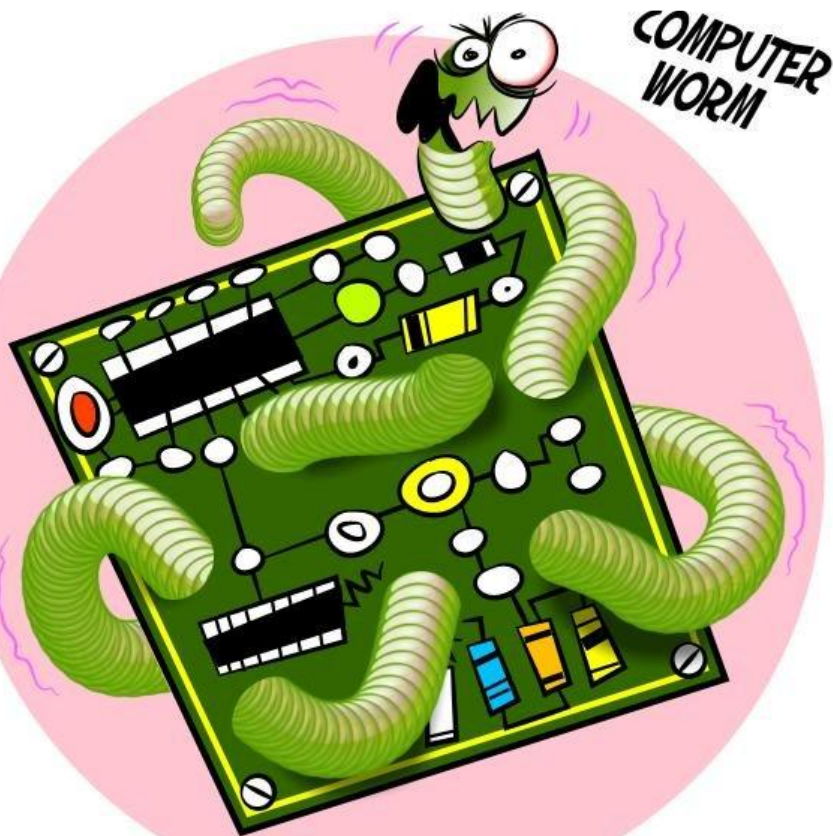
- НАРУШЕНИЕ РАБОТЫ ДРУГИХ ПРОГРАММ (ВПЛОТЬ ДО ПОВИСАНИЯ КОМПЬЮТЕРА, РЕШАЕМОГО ЛИШЬ ПЕРЕЗАГРУЗКОЙ, И НЕВОЗМОЖНОСТИ ИХ ЗАПУСКА);
- НАСТОЙЧИВОЕ, НЕЗАВИСИМОЕ ОТ ВЛАДЕЛЬЦА ПРЕДЛАГАНИЕ В КАЧЕСТВЕ СТАРТОВОЙ СТРАНИЦЫ СПАМ-ССЫЛОК, РЕКЛАМЫ;
- ПРЕВРАЩЕНИЕ ЯЗЫКА ТЕКСТОВЫХ ДОКУМЕНТОВ В БИНАРНЫЙ КОД;
- МОШЕННИЧЕСТВО (НАПРИМЕР, ПРИ ОТКРЫВАНИИ ОПРЕДЕЛЁННОГО САЙТА ПОЛЬЗОВАТЕЛЬ МОЖЕТ УВИДЕТЬ ОКНО, В КОТОРОМ ЕМУ ПРЕДЛАГАЮТ СДЕЛАТЬ ОПРЕДЕЛЁННОЕ ДЕЙСТВИЕ, ИНАЧЕ ПРОИЗОЙДЁТ ЧТО-ТО ТРУДНОПОПРАВИМОЕ – БЕССРОЧНАЯ БЛОКИРОВКА ПОЛЬЗОВАТЕЛЯ СО СТОРОНЫ САЙТА, ПОТЕРЯ БАНКОВСКОГО СЧЕТА И Т.П., ИНОГДА ЗА ДЕНЬГИ, ПОЛУЧЕНИЕ ДОСТУПА К УПРАВЛЕНИЮ КОМПЬЮТЕРОМ И УСТАНОВКИ ВРЕДОНОСНОГО ПО);

ЛЮБОПЫТНЫЙ ФАКТ:  
ПО СООБЩЕНИЮ DAILY MAIL, ПЕРЕХОДНИКИ ДЛЯ  
МОБИЛЬНЫХ ТЕЛЕФОНОВ И USB-НАКОПИТЕЛИ,  
ВРУЧЕННЫЕ СОТРУДНИКАМ ДЭВИДА КЭМЕРОНА, А  
ТАКЖЕ ДРУГИМ ИНОСТРАННЫМ ДЕЛЕГАТАМ НА ВСТРЕЧЕ  
G20 В РОССИИ, ОКАЗАЛИСЬ ЗАРАЖЕННЫМИ  
«ТРОЯНАМИ», СПОСОБНЫМИ ПЕРЕДАВАТЬ ДАННЫЕ ДЛЯ  
РОССИЙСКОЙ РАЗВЕДКИ.





## 2012 ГОД



Flame — компьютерный червь. Его обнаружил Роэл Шоэннберг, старший научный сотрудник по компьютерной безопасности «Лаборатории Касперского». Основной особенностью червя является наличие в нём множества (по крайней мере, несколько десятков) компонентов, способных выполнять разнообразные вредоносные действия: размножаться в сетях различных типов с использованием различных протоколов, похищать и уничтожать конфиденциальную информацию, взаимодействовать с вредоносными программами других типов и т. п. Всё это делает Flame удобным средством для промышленного и политического шпионажа и диверсий.

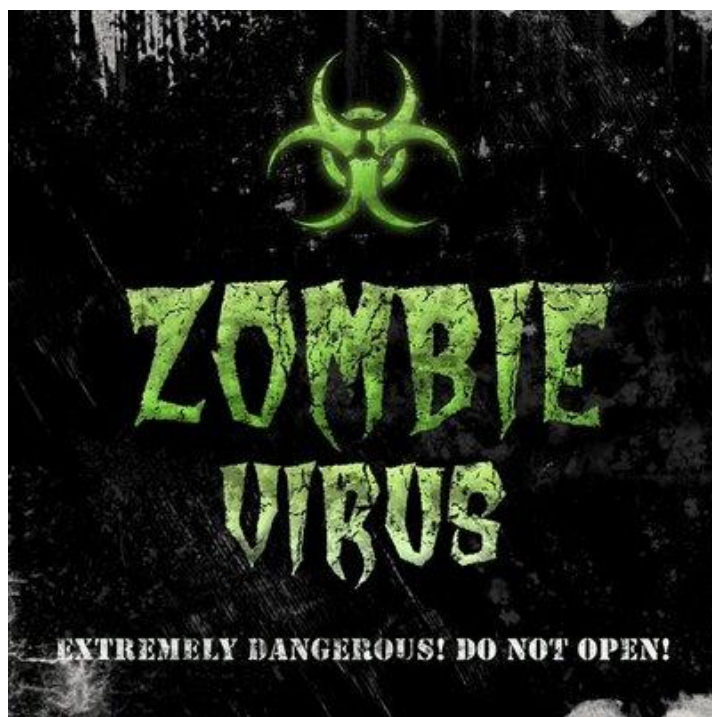
## Руткиты

Руткит- это программа для скрытия присутствия злоумышленника или вредоносного кода в оперативной памяти. Главная задача руткитов- не допустить обнаружения действий вирусов хозяином компьютера, скрыть от пользователя присутствия хакера и изменений в системе.



**ПРИЗНАКИ НАЛИЧИЯ РУТКИТОВ:**  
-КОМПЬЮТЕР ВЕДЕТ СЕБЯ КАК-ТО НЕ ТАК. В АВТОЗАГРУЗКЕ ЧИСТО, ПРОЦЕССЫ В ПОРЯДКЕ, АНТИВИРУС НИЧЕГО НЕ НАХОДИТ, НО ЕСТЬ ПОДОЗРЕНИЯ, ЧТО КОМПЬЮТЕР НЕ В ПОРЯДКЕ.  
-НЕЗАМЕТНАЯ ПОЛЬЗОВАТЕЛЮ РАССЫЛКА СПАМОВ, КРАЖА ПАРОЛЕЙ ОТ САЙТОВ И ПОЧТЫ.

**ЗОМБИ** (ZOMBIE) - ЭТО ПРОГРАММА-ВИРУС, КОТОРАЯ ПОСЛЕ ПРОНИКНОВЕНИЯ В КОМПЬЮТЕР, ПОДКЛЮЧЕННЫЙ К СЕТИ ИНТЕРНЕТ УПРАВЛЯЕТСЯ ИЗВНЕ И ИСПОЛЬЗУЕТСЯ ЗЛОУМЫШЛЕННИКАМИ ДЛЯ ОРГАНИЗАЦИИ АТАК НА ДРУГИЕ КОМПЬЮТЕРЫ. ЗАРАЖЕННЫЕ ТАКИМ ОБРАЗОМ КОМПЬЮТЕРЫ-ЗОМБИ МОГУТ ОБЪЕДИНЯТЬСЯ В СЕТИ, ЧЕРЕЗ КОТОРЫЕ РАССЫЛАЕТСЯ ОГРОМНОЕ КОЛИЧЕСТВО НЕЖЕЛАТЕЛЬНЫХ СООБЩЕНИЙ ЭЛЕКТРОННОЙ ПОЧТЫ, А ТАКЖЕ РАСПРОСТРАНЯЮТСЯ ВИРУСЫ И ДРУГИЕ ВРЕДОНОСНЫЕ ПРОГРАММЫ.



**Шпионская программа** (Spyware) - это программный продукт, установленный или проникший на компьютер без согласия его владельца, с целью получения практически полного доступа к компьютеру, сбора и отслеживания личной или конфиденциальной информации.

Эти программы, как правило, проникают на компьютер при помощи сетевых червей, троянских программ или под видом рекламы. Одной из разновидностей шпионских программ являются фишинг рассылки.





**Фишинг** (Phishing) - это почтовая рассылка имеющая своей целью получение конфиденциальной финансовой информации. Такое письмо, как правило, содержит ссылку на сайт, являющейся точной копией интернет-банка или другого финансового учреждения. Пользователь, обычно, не догадывается, что находится на фальшивом сайте и спокойно выдает злоумышленникам информацию о своих счетах, кредитных карточках, паролях и т. д.

**Фарминг** - это замаскированная форма фишинга, заключающаяся в том, что при попытке зайти на официальный сайт интернет банка или коммерческой организации, пользователь автоматически перенаправляется на ложный сайт, который очень трудно отличить от официального сайта.

Как и в случае фишинга основной целью злоумышленников, использующих фарминг, является завладение личной финансовой информацией пользователя. Отличие заключается только в том, что вместо электронной почты мошенники используют более изощренные методы направления пользователя на фальшивый сайт.

