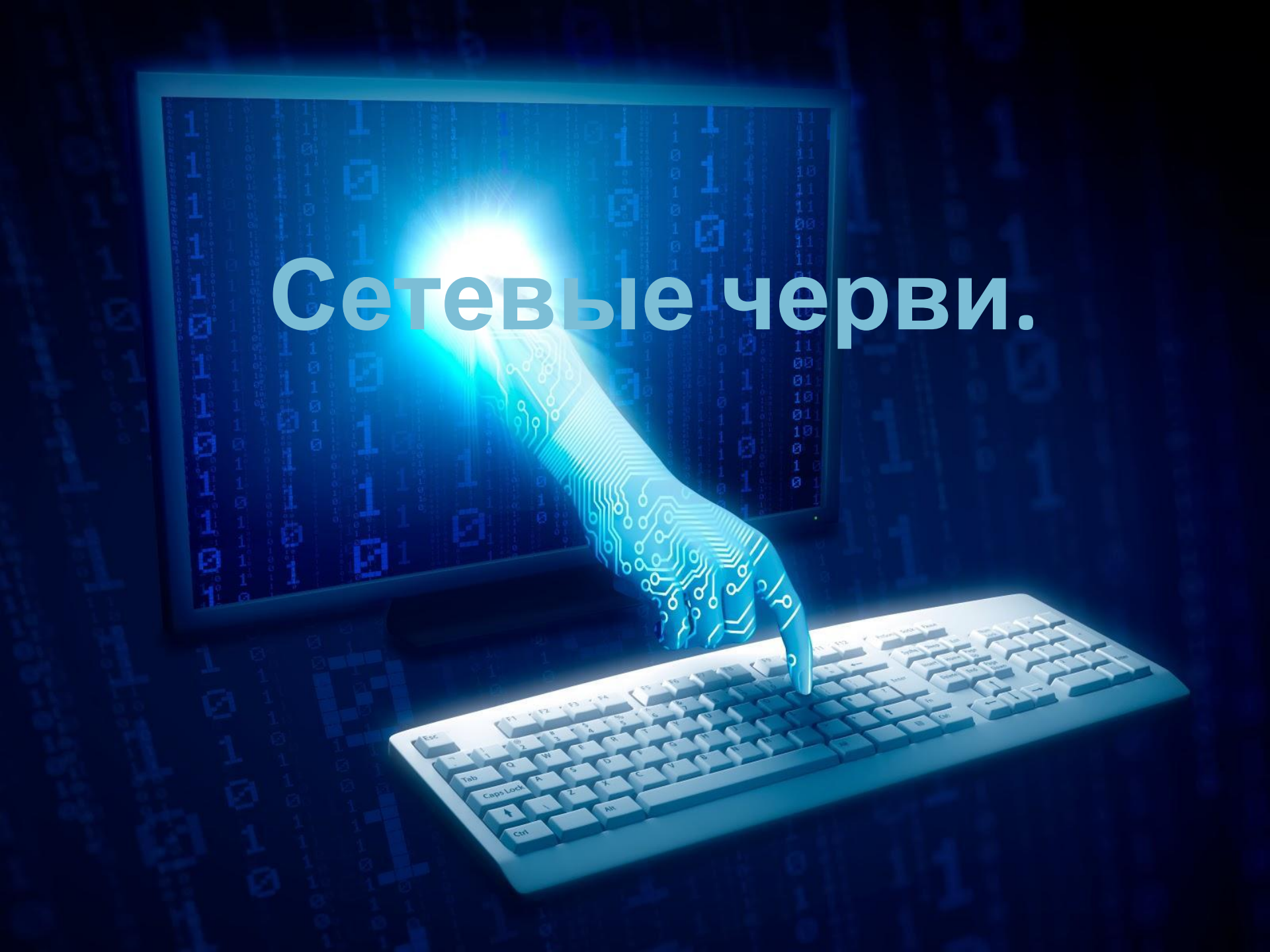

Сетевые черви.

Сетевые черви

- **Сетевые черви** (другое название – компьютерные черви) – это программы, которые созданы с внутренним механизмом распространения по локальным и глобальным компьютерным сетям с некоторыми целями. Данными целями являются:
- *проникновение на удаленные компьютеры с частичным или полным перехватом управления ими (скрытым от пользователя – хозяина этого компьютера разумеется);*
- *запуск своей копии на компьютере;*
- *дальнейшее распространение по всем доступным сетям, как локальным, так и глобальным.*

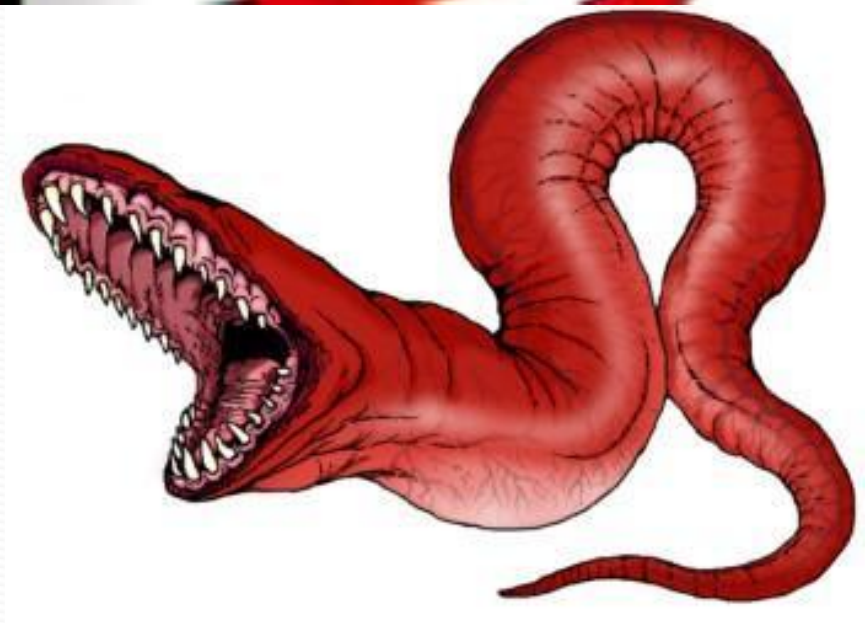
Виды сетей, по которым передаются сетевые черви.

- Это, в первую очередь, конечно, электронная почта, различные интернет-мессенджеры, файлообменные и торрент-сети, локальные сети, сети обмена между мобильными устройствами.

В основном компьютерные черви распространяются в виде файлов.

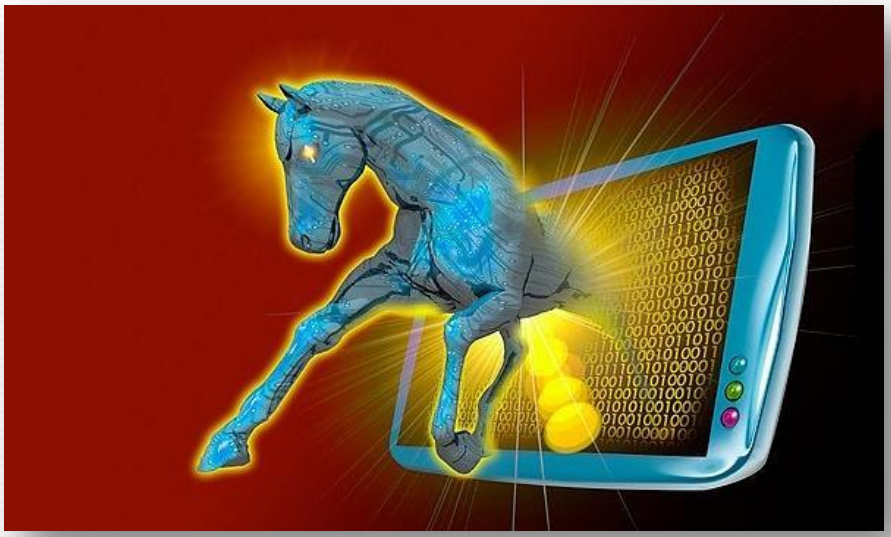
- Их прикрепляют в качестве вложений к электронным письмам и сообщениям, либо же различными способами пользователю предлагается пройти по определенной ссылке, закачать и запустить у себя на локальном компьютере некую крайне нужную и бесплатную программу, фотографию и т.д. (вариантов маскировки сетевых вирусов существует бесконечно много). Нужно сказать, что электронная почта стала практически идеальной почвой для распространения сетевых червей. И скорость их (сетевых червей) распространения по всему Интернету зачастую просто потрясает воображение.

- Но существуют и так называемые «бесфайловые, пакетные» сетевые вирусы, которые распространяются в виде сетевых пакетов и проникают на компьютер при помощи различных брешей и уязвимостей в операционной системе или установленном программном обеспечении.



- Для проникновения на удаленный компьютер используются самые различные методы, начиная от методов социальной инженерии (когда Вам приходит некое заманчивое письмо с ссылкой или вложенным файлом, призывающее либо открыть данный вложенный файл либо пройти по указанной ссылке), либо же, как уже писалось выше, это проникновение с помощью уязвимостей и back-door в используемом программном обеспечении. Также проникновение возможно при существующих недочетах в планировании и обслуживании локальной сети (примером может служить какой-либо полностью незащищенный локальный диск).

- В дополнение к своим основным функциям **сетевые черви** довольно часто содержат и функции другого вредоносного программного обеспечения – вирусов, троянских программ и т.д.
- Как показывает статистика антивирусных лабораторий, более 80% всех проблем, связанных с проникновением вредоносного программного обеспечения (сетевых червей, троянов и вирусов) на локальные компьютеры пользователей, связано с элементарной безграмотностью и отсутствием необходимых навыков работы в сети Интернет у самих пользователей.

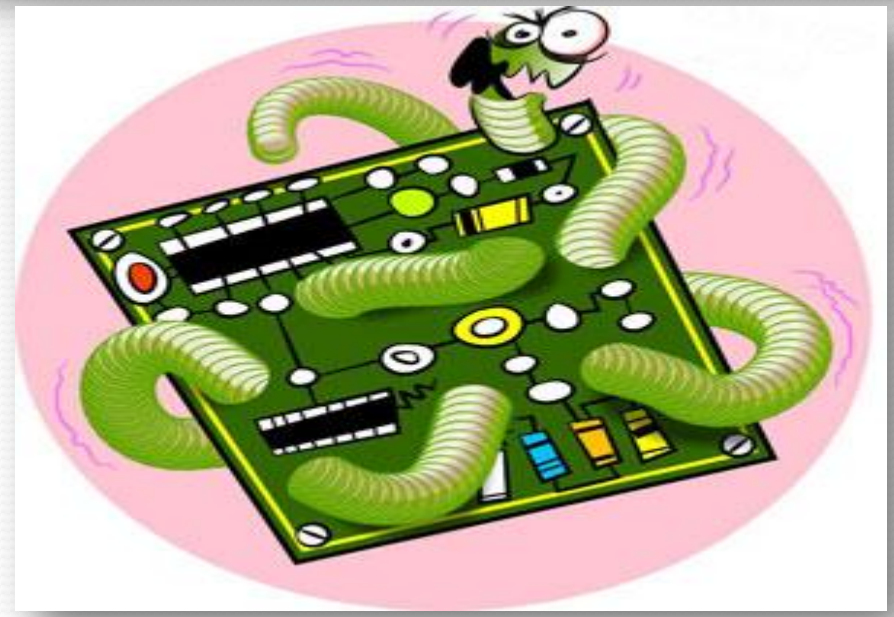


Как возникли сетевые черви?

- Первые эксперименты, в ходе которых были использованы первые прототипы компьютерных червей, были проведены в 1978 году в научно-исследовательском центре *Xerox* в Пало Альто. Инициаторами данных работ были Джон Шоч и Йон Хупп. Сам термин «сетевой червь» возник под влиянием научно-фантастической литературы (в частности, это романы Д.Геррольда *«Когда Харли исполнился год»* и Д. Браннера *«На ударной волне»).*
- Наверное, самым известным сетевым червем является так называемый *«Червь Морриса»,* который был написан в 1988 году студентом Корнельского университета Р. Моррисом-младшим. Вирус попал в сеть 2 ноября 1988 года, и стремительно распространился на большое количество компьютеров, имеющих подключение к Интернет.

Виды сетевых червей.

- Существуют различные виды сетевых червей. В первую очередь следует упомянуть ОЗУ-резидентных червей, которые располагаются в оперативной памяти компьютера, не затрагивая файлов на жестком диске. Избавиться от таких компьютерных червей достаточно просто – достаточно просто перезапустить операционную систему, при этом произойдет сброс данных, находящихся в ОЗУ, соответственно, сотрется и червь. ОЗУ-резидентные вирусы состоят из двух частей: эксплойта (или шелл-кода), с помощью которого они проникают на компьютер, и самого тела червя.



- Также существуют вирусы, которые при успешном проникновении на компьютер проводят некоторые действия с локальными дисками: прописывают там некий программный код (примером может служить модификация ключей в реестре *Windows* или прописывание файла вируса в Автозагрузке). Также *червь* при успешном проникновении на компьютер может самостоятельно догрузить какие-либо дополнительные файлы по сети (вирусы, троянские программы, другие сетевые черви) и превратить ваш компьютер в рассадник всякой компьютерной заразы.

Обнаружить и, соответственно, обезвредить данных сетевых червей довольно сложно. В этом Вам помогут антивирусные программы с обновленными базами вирусных сигнатур.