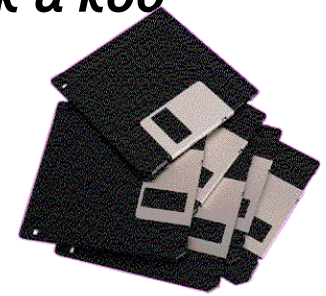
Вирусы

Вирус

Под ***компьютерным вирусом*** принято понимать программы или элементы программ, несанкционированно проникшие в компьютер с целью нанесения вреда, отличительной особенностью которых является способность самотиражирования.

Все вирусы можно объединить в следующие основные группы:

- **Загрузочные вирусы (boot – вирусы)** — инфицируют загрузочные секторы жестких дисков и дискет, помещая в нем команды запуска на исполнение самого вируса, который находится где-то в другом месте компьютера.
- **Файловые вирусы** — заражают исполняемые файлы (с расширением .com, .exe, .sys), путем дописывания своей основной части («тела») в конец заражаемой программы, «головы» - в его начало. Вирус, находящийся в памяти, заражает все любой запущенный после этого исполняемый файл.
- **Загрузочно-файловые вирусы** способны поражать как код загрузочных секторов, так и код файлов.
- **Сетевые вирусы.**



Загрузочные вирусы (boot – вирусы)

- ***Макро-вирусы.***

Заражает файлы документов, например текстовые документы. После загрузки заражённого документа постоянно находится в оперативной памяти до закрытия документа.

- ***«Червь».***

это программа, которая тиражируется на жестком диске, в памяти компьютера и распространяется по сети.

- Особенностью червей, отличающих их от других вирусов, является то, что они не несут в себе ни какой вредоносной нагрузки, кроме саморазмножения, целью которого является замусоривание памяти, и как следствие, затормаживание работы операционной системы.

СЕТЕВЫЕ ЧЕРВИ

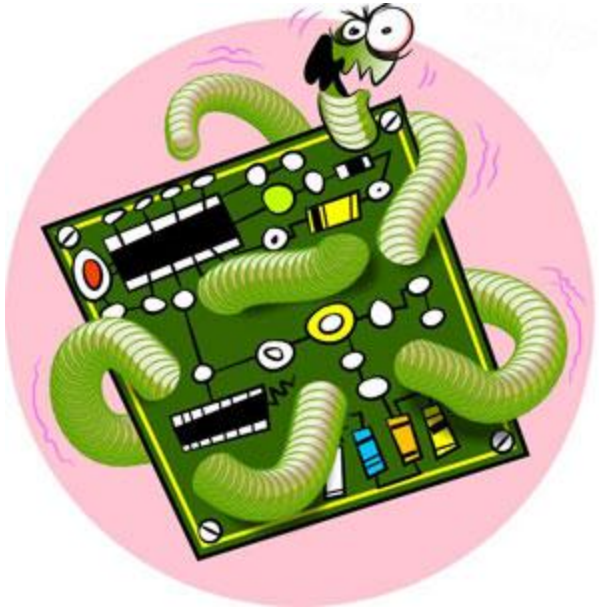
К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

1. ***проникновения на удаленные компьютеры;***
2. ***запуска своей копии на удаленном компьютере;***
3. ***дальнейшего распространения на другие компьютеры в сети.***

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях, файл в каталоге обмена P2P и т. д.

Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.



В дополнение к этой классификации отметим еще несколько отличительных особенностей, характеризующих некоторые файлово - загрузочные вирусы.

Полиморфизм.

Большинство вирусов, созданных в прежние годы, при саморазмножении никак не изменяются, так что «потомки» являются абсолютно точной копией «прародителя», что и позволяет легко их обнаруживать по характерной для каждого последовательности байтов

«Стелс» - технология.

Этот термин появился по аналогии с названием технологии разработки американского бомбардировщика, невидимого на экране радара. Стелс-вирус, находясь в памяти компьютера, перехватывает почти все векторы прерываний . В результате при попытке контроля длины зараженного файла ДОС выдает старую, «правильную» длину вместо истинной, а при просмотре коды вируса исключаются им из рассмотрения.

«Логические бомбы».

кая программа добавляется к какой-либо полезной программе и «дремлет» в ней до определенного часа. Когда же показания системного счетчика времени данного компьютера станут равными установленному программистом значению часов, минут и секунд (или превысят их), производится какое-либо разрушающее действие, например, форматирование винчестера. Это один из распространенных вариантов мести обиженных программистов своему руководству.

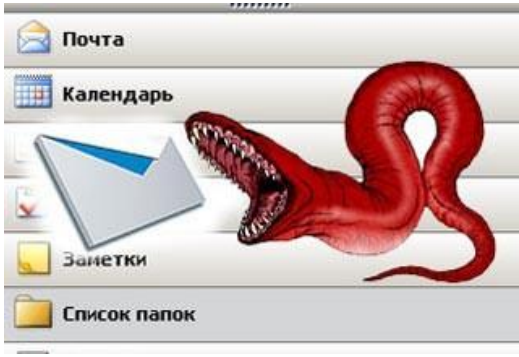
Программы-вандалы.

Самый простой способ напакостить всем и вся. Пишется программа-разрушитель (например, все тот же форматировщик винчестера), ей дается название, такое же, как у другой, полезной программы, и она размещается в качестве «обновленной версии». Ничего не подозревающий пользователь обрадовано «скачивает» ее на свой компьютер и запускает, а в результате - лишается всей информации на жестком диске.

Сетевые вирусы.

- **«Логические бомбы» - скрипты и апплеты**.

И хотя основные функции доступа к содержимому вашего диска здесь отключены, некоторые мелкие неприятности это может доставить. Кстати, в последнее время создатели некоторых сайтов (как правило, из разряда «только для взрослых») освоили любопытный вариант скриптов (на базе JavaScript), способных при открытии такой Web-страницы не только «прописать» адрес данного сайта в качестве «домашнего» (естественно, не спрашивая у посетителя разрешения), но и внести его непосредственно в системный реестр Windows в качестве «базового».



- **«Троянские кони».**

Это модули, присоединяемые к каким-либо нормальным программам, распространяемым по сети, или «забрасываемые» в ваш компьютер несанкционированным способом.

Цель «троянского коня» - воровать ценную информацию (пароли доступа, номера кредитных карточек и т. п.) и передавать ее тому, кто этого «коня» запустил.

- **Почтовые вирусы**.

Чаще всего заражение начинается с получения неизвестно от кого письма, содержащего исполняемую программу-«зародыш» . Когда ничего не подозревающий пользователь запустит такую программу на исполнение, содержащийся в ней вирус «прописывается» в системе и, обращаясь к содержимому адресной книги, начинает тайком от вас рассылать всем абонентам свои копии-зародыши в качестве вложений.

Вирусы делятся также на резидентные и нерезидентные

— первые при получении управления загружаются в память и могут действовать, в отличие от нерезидентных, не только во время работы зараженного файла.

Дополнительные типы вирусов

- ***Зомби***

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.

Шпионские 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 (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.

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.

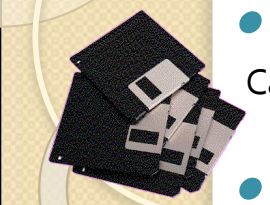
основной целью злоумышленников, использующих Фарминг, является завладение личной финансовой информацией пользователя. Отличие заключается только в том, что вместо электронной почты мошенники используют более изощренные методы направления пользователя на фальшивый сайт.

Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Каналы распространения



- ***Дискеты***

Самый распространённый канал заражения в 1980-90 годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов.

- ***Флеш-накопители (флешки)***

В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны. Использование этого канала преимущественно обусловлено возможностью создания на накопителе специального файла ***autorun.inf,*** в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. Флешки — основной источник заражения для компьютеров, не подключённых к сети Интернет.

- ***Электронная почта***

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты.

- ***Системы обмена мгновенными сообщениями***

Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

- ***Веб-страницы***

Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов

- ***Интернет и локальные сети (черви)***

Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.