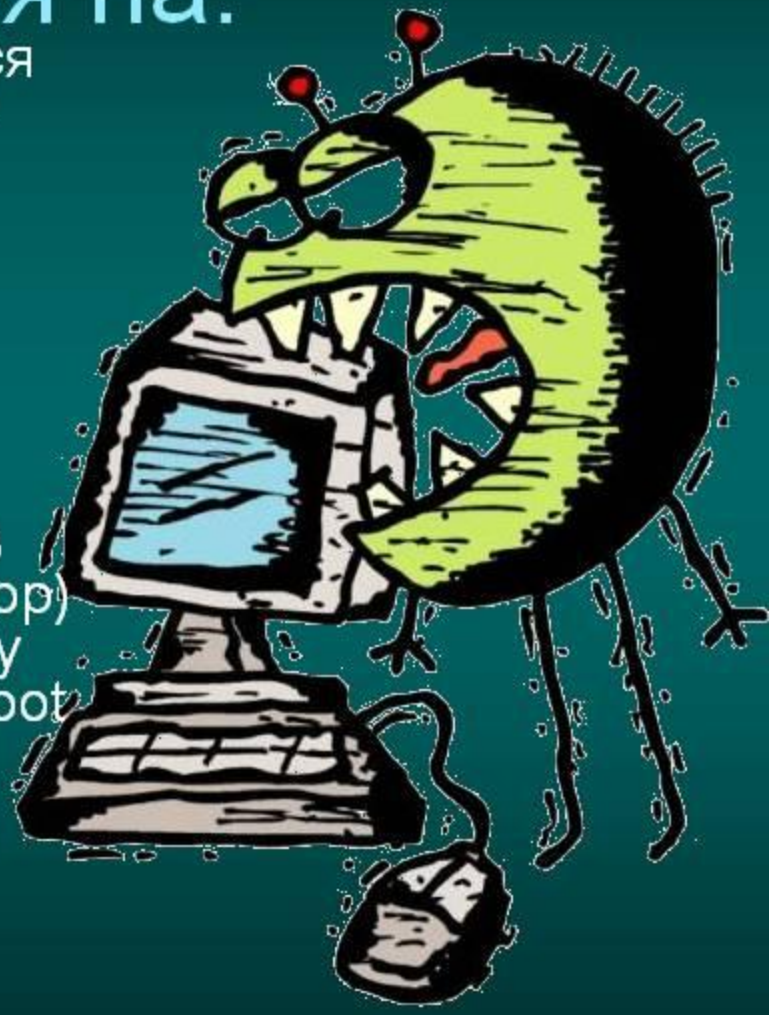
«КОМПЬЮТЕРНЫЕ ВИРУСЫ»


Virus

По среде обитания вирусы подразделяются на:

- ***Сетевые вирусы*** распространяются по различным компьютерным сетям.
- ***Файловые вирусы*** внедряются главным образом в исполняемые модули, т. е. В файлы, имеющие расширения COM и EXE.
- ***Загрузочные вирусы*** внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord**).**
- ***Файлово-загрузочные вирусы*** заражают как файлы, так и загрузочные сектора дисков**.**



- **Компью́терный ви́рус** — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

История


История компьютерного вируса
1974 год
Появление первого вируса «Кролик» Rabbit
13 мая 1988 год, пятница
Появился вирус “Jerusalem” – в этот день вирус уничтожал файлы при их запуске
Ноябрь 1988 г. Эпидемия вируса Морриса (заражено Более 6000 компьютерных Систем, включая NASA)
1995-1999 год- появление Windows-совместимых вирусов
Сегодняшний день: на сегодняшний день в Интернете ежедневно появляется порядка 5000 новых вирусов

Этимология названия

- Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения. По-видимому, впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом (Gregory Benford) в фантастическом рассказе «Человек в шрамах», опубликованном в журнале Venture в мае 1970 года.

- Термин «компьютерный вирус» впоследствии не раз «открывался» и переоткрывался. Так, переменная в подпрограмме PERVADE (1975), от значения которой зависело, будет ли программа ANIMAL распространяться по диску, называлась VIRUS. Также, вирусом назвал свои программы Джо Челленджер и, вероятно, это и было то, что впервые было правильно обозначено как вирус.

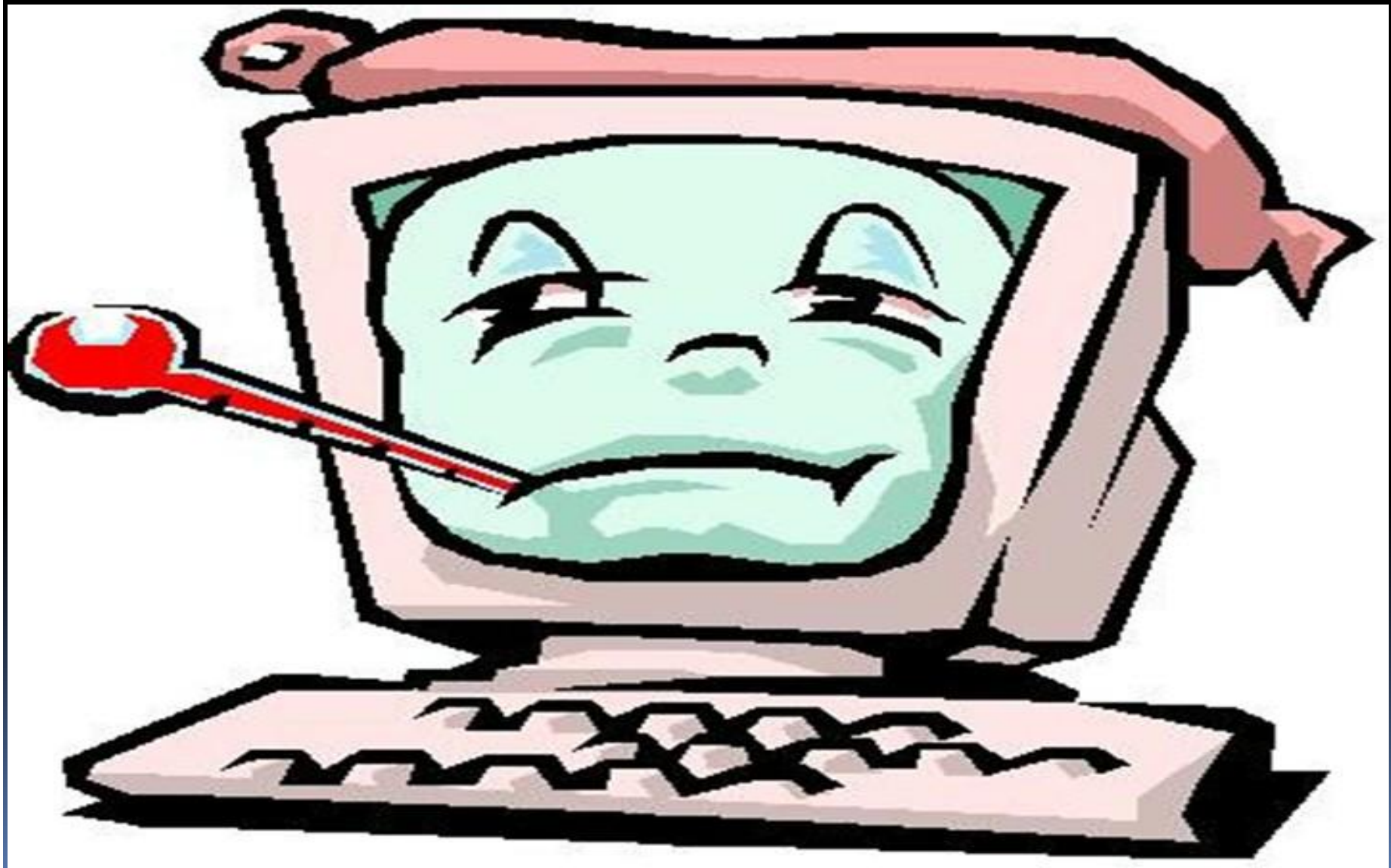
Противодействие обнаружению

- Во времена MS-DOS были распространены стелс-вирусы, перехватывающие прерывания для обращения к операционной системе. Вирус таким образом мог скрывать свои файлы из дерева каталогов или подставлять вместо зараженного файла исходную копию.

- С широким распространением антивирусных сканеров, проверяющих перед запуском любой код на наличие сигнатур или выполнение подозрительных действий, этой технологии стало недостаточно. Сокрытие вируса из списка процессов или дерева каталогов для того, чтобы не привлекать лишнее внимание пользователя, является базовым приемом, однако для борьбы с антивирусами требуются более изощренные методы. Для противодействия сканированию на наличие сигнатур применяется шифрование кода и полиморфизм. Эти техники часто применяются вместе, поскольку для расшифрования зашифрованной части вируса необходимо оставлять расшифровщик незашифрованным, что позволяет обнаруживать его по сигнатуре. Поэтому для изменения расшифровщика применяют полиморфизм — модификацию последовательности команд, не изменяющую выполняемых действий. Это возможно благодаря весьма разнообразной и гибкой системе команд процессоров Intel, в которой одно и то же элементарное действие, например, сложение двух чисел, может быть выполнено несколькими последовательностями команд.

- Также применяется перемешивание кода, когда отдельные команды случайным образом разупорядочиваются и соединяются безусловными переходами. Передовым фронтом вирусных технологий считается метаморфизм, который часто путают с полиморфизмом. Расшифровщик полиморфного вируса относительно прост, его функция — расшифровать основное тело вируса после внедрения, то есть после того, как его код будет проверен антивирусом и запущен. Он не содержит самого полиморфного движка, который находится в зашифрованной части вируса и генерирует расшифровщик. В отличие от этого, метаморфный вирус может вообще не применять шифрование, поскольку сам при каждой репликации переписывает весь свой код.

Профилактика и лечение



- В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.

- Отключать потенциально опасный функционал системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Отключать потенциально опасный функционал системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

Экономика

- Некоторые производители антивирусов утверждают, что сейчас создание вирусов превратилось из одиночного хулиганского занятия в серьёзный бизнес, имеющий тесные связи с бизнесом спама и другими видами противозаконной деятельности.