"Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/".

ВИРУСЫ

Выполнили ученики
Лицея №11 им.Т.И.Александровой:
Крылов Никита, Чернова Анастасия,
Смирнова Дарья

г.Йошкар-Ола, 2016г.

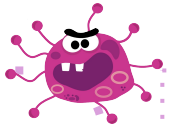
СОДЕРЖАНИЕ

КОМПЬЮТЕРНЫЙ ВИРУС

– вид вредоносного программного обеспечения, способный:

- **удалять** файлы
- **создавать** копии самого себя
- **блокировать** работы пользователей
- **приводить в негодность** компьютер
- **внедряться** в код других программ, с целью нарушения работы программно-аппаратных комплексов

СТАДИИ ФУНКЦИОНИРОВАНИЯ

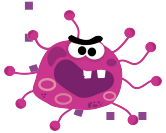


Латентная стадия

– вирус в системе, но никаких **действий не предпринимает**

Инкубационная стадия

– вирус активируется и начинает создавать свои копии, **загрузка** информации из Интернета может замедляться



Активная стадия

– вирус продолжает размножаться доступными ему способами, начинает разрушительные **действия** на которые ориентирован

КЛАССИФИКАЦИЯ ВИРУСОВ ПО СРЕДЕ ОБИТАНИЯ

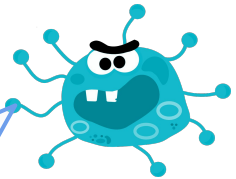
1. Загрузочные вирусы

2. Файловые вирусы

3. Файлово–загрузочные вирусы

4. Сетевые вирусы

5. Документные вирусы



На сегодняшний день существует много компьютерных вирусов. Ежедневно появляется тысячи новых. Однако все это множество поддается классификации!

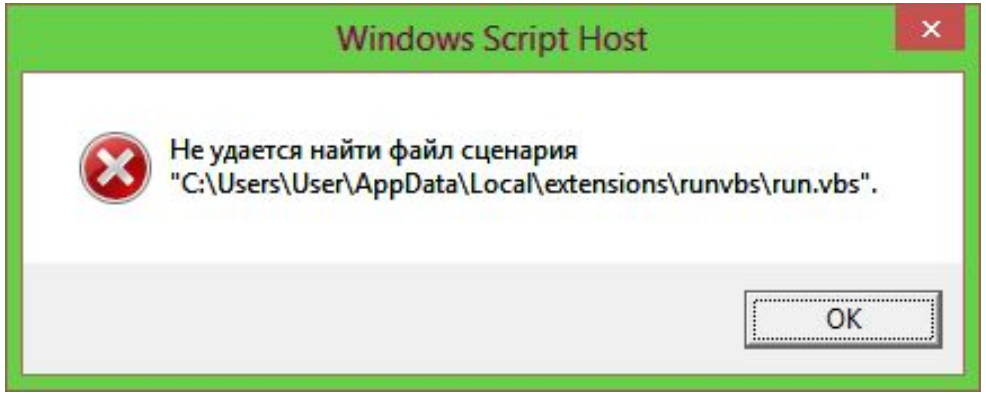
ЗАГРУЗОЧНЫЙ ВИРУС

Проникает в загрузочные сектора устройств хранения данных (жесткие диски, дискеты, переносные запоминающие устройства). При загрузке операционной системы с зараженного диска происходит активация вируса.

Его действия могут состоять в нарушении работы загрузчика операционной системы, что приводит к невозможности ее работы, либо изменении файловой таблицы, что делает недоступным определенные файлы.

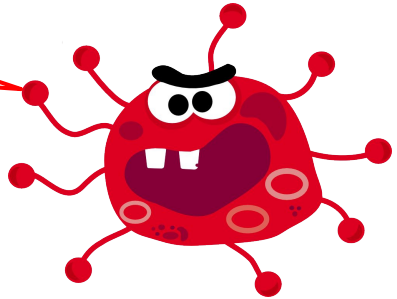
Файловый вирус

Эти вирусы чаще всего внедряются в исполнительные модули программ , что позволяет им активироваться в момент запуска программы, влияя на ее функциональность. Реже файловые вирусы могут внедрятся в библиотеки операционной системы или прикладного ПО, исполнительные пакетные файлы, файлы реестра Windows, файлы сценариев, файлы драйверов. Внедрение может проводиться либо изменением кода атакуемого файла, либо созданием его модифицированной копии.

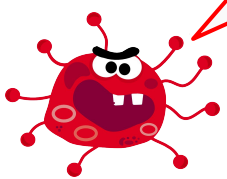


ФАЙЛОВО-ЗАГРУЗОЧНЫЕ ВИРУСЫ

Таким образом, вирус, находясь в файле, активируется при доступе к этому файлу, инициируемому пользователем или самой ОС. Файловые вирусы – наиболее распространенный вид компьютерных вирусов.



Объединяют в себе возможности двух предыдущих групп, что позволяет им представлять серьезную угрозу работе компьютера.



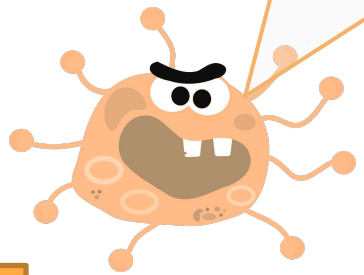
СЕТЕВЫЕ ВИРУСЫ

Распространяются посредством сетевых служб и протоколов. Таких как рассылка почты, доступ к файлам по FTP, доступ файлам через службы локальных сетей.

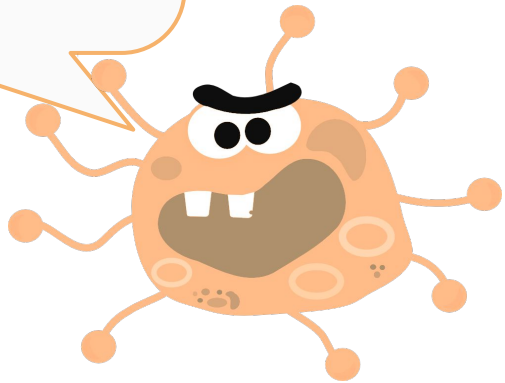
Что делает их очень опасными, так как заражение не остается в пределах одного компьютера или даже одной локальной сети, а начинает распространятся по разнообразным каналам связи.

ДОКУМЕНТНЫЕ ВИРУСЫ

Заражают файлы офисных систем (Microsoft Office, Open Office…) через использование в этих системах макросов



Макрос – микропрограмма, встроенная в документ для модификации этого документа или других функций. Именно макрос и является целью макровирусов.



КЛАССИФИКАЦИЯ ВИРУСОВ ПО МЕТОДУ СУЩЕСТВОВАНИЯ

Резидентный вирус

- если вызван запуском зараженной программы, остается в памяти после ее завершения. Может заражать другие запущенные программы, искажая их функциональность. Может “наблюдать” за действиями пользователя, сохраняя информацию о его действиях

Нерезидентный вирус

- является неотъемлемой частью зараженной программы и может функционировать только во время ее работы.

ПРИНЦИП ФУНКЦИОНИРОВАНИЯ

1. **Вирусы-паразиты (Parasitic)**
– вирусы, частично выводящие программы их из строя. Часто файл-носитель остается не пригодным.

2. **Вирусы- репликаторы (Worm)**
– размножаются по всем возможным местам хранения данных. Являются транспортом для других видов вредоносного кода.

3. **Трояны (Trojan)**
– получили свое название в честь “Троянского коня”. Маскирует свои модули под модули используемых программ, создавая файлы со схожими именами и параметрами, меняя ссылки рабочих модулей программ на свои. Итог - уничтожение данных пользователя, рассылка СПАМа и слежка. Выявляются достаточно сложно, так как простого сканирования файловой системы не достаточно.

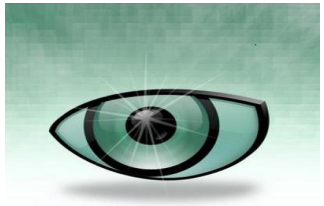
ПРИНЦИП ФУНКЦИОНИРОВАНИЯ

4. **"Отдыхающие" вирусы**
– являются очень опасными, так как могут очень продолжительное время находится в состоянии покоя, распространяясь по компьютерным сетям. Активация вируса происходит при определенном условии, зачастую по определенной дате, что может вызвать огромные масштабы одновременного заражения. Примером такого вируса является вирус CHIH или Чернобыль, который активировался в день годовщины аварии на ЧАЭС, вызвав выход из строя тысячи компьютеров.

Задание 1:

ПРОВЕРЬ СЕБЯ

Какие это антивирусные программы?



Задание 2:

Установите соответствие:

– вирус продолжает размножаться доступными ему способами, начинает разрушительные **действия** на которые ориентирован

вирус в системе, но никаких **действий не предпринимает**

– вирус активируется и начинает создавать свои копии, **загрузка** информации из Интернета может замедляться

активная стадия

инкубационная стадия

латентная стадия

Задание 3:

Действия какого вируса могут состоять в нарушении работы загрузчика операционной системы или изменение файловой таблицы

- Файловый вирус
- Троянский конь
- Загрузочный вирус

Задание 4:

Какие вирусы относятся к файловым вирусам

- Вирусы, заражающие программы
- Макровирусы
- Вирусы-невидимки
- Вирусы-черви

Результаты

Тестовое задание *1:* Касперский, Nod 32, Avast

Тестовое задание *2:* активная стадия, латентная стадия, инкубационная стадия

Тестовое задание *3:* загрузочный вирус

Тестовое задание *4:* вирусы, заражающие программы, макровирусы