Вирусы и антивирусные программы

Компьютерный вирус – это специально написанная обычно небольшая по размерам программа, способная самопроизвольно присоединяться к другим программам (т. е. заражать их), создавать свои копии (не обязательно совпадающие с оригиналом) и внедрять их в файлы, системные области и другие объединенные компьютеры с целью создания различных помех.

I. Классификация вирусов в зависимости от среды обитания:

1. файловые;
2. загрузочные;
3. макровирусы;
4. сетевые.

1. Файловые вирусы.

К данной группе относятся вирусы, которые при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС.

Файловые вирусы могут внедряться практически во все исполняемые файлы всех популярных ОС.

Файловые вирусы заражают файлы различных типов:

• программные файлы с расширениями «.exe» или «.com»;
• командные файлы (расширение «.bat»);
• файлы документов, имеющих макрокоманды Microsoft Word, Microsoft Excel, баз данных Microsoft Access (расширение «.mdb») и Microsoft Power Point;
• самораззархивирующиеся файлы;
• файлы драйверов реального режима (расширение «.sys») и др

По способу заражения файлов

- overwriting,
- паразитические (parasitic),
- компаньон-вирусы (companion),
- link-вирусы,
- вирусы-черви,
- вирусы, заражающие объектные модули (OBJ), библиотеки компиляторов (LIB) и исходные тексты программ.

Overwriting-вирусы

Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.

Parasitic-вирусы

Вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.

- ✔Внедрение вируса в начало файла.
- ✔Внедрение вируса в конец файла.
- ✔Внедрение вируса в середину файла.
- ✔Вирусы без точки входа

Companion-вирусы

1 группа. Вирусы, не изменяющие заражаемых файлов.

2 группа. Вирусы, которые при заражении переименовывают файл, давая ему какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла.

3 группа. Вирусы, которые либо записывают свой код под именем заражаемого файла, но "выше" на один уровень.

Link-вирусы

Не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнит свой код.

Файловые черви

Не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем.

2. Загрузочные вирусы

- ✔в загрузочный сектор диска (Boot Record, BR) - сектор),
- ✔в сектор, содержащий системный загрузчик жесткого диска, системной дискеты или загрузочного компакт-диска.

3. Макровирусы

Вредительские программы, написанные на макроязыках, встроенных в текстовые редакторы, электронные таблицы и др. Наибольшее распространение получили макровирусы для MicrosoftWord, Excel и Office.

4. Сетевые вирусы

Для своего распространения активно используют протоколы и возможности локальных и глобальных сетей.

II. По деструктивным возможностям вирусы можно разделить на:

1. Безвредные.

Никак не влияют на работу компьютера (кроме уменьшения свободной памяти на диске при своем распространении).

Деструктивное воздействие:

- ✔вывод на экран монитора невинных текстов и картинок,
- ✔исполнение музыкальных фрагментов и т. п.

2. Опасные вирусы.

Могут привести к серьезным сбоям в работе компьютера.

Наносимый ущерб:

- занимающие память компьютера и каналы связи, но не блокирующие работу сети;
- вызывают необходимость повторного выполнения программ, перезагрузки операционной системы или повторной передачи данных по каналам связи и т. п.

3. Очень опасные.

Деструктивное воздействие:

- ✔потеря программ,
- ✔уничтожение данных,
- ✔нарушение конфиденциальности,
- ✔необратимую модификацию (в том числе и шифрование) информации,
- ✔стирание отдельных файлов, системных областей памяти,
- ✔форматирование дисков, и, шифруют данные и т. п.

III. По используемой ОС

Программы-вирусы создаются для компьютеров определенного типа, работающих с конкретными ОС.

- ✔распространенность ОС;
- ✔отсутствие встроенных антивирусных механизмов;
- ✔относительная простота;
- ✔продолжительность эксплуатации.

IV. По особенности алгоритма работы вирусов выделяются следующие:

1. Резидентные и нерезидентные.

Резидентные вирусы после их активизации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память компьютера.

Нерезидентные вирусы попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют деструктивную функцию и функцию заражения.

2. Использование "стелс"- алгоритмов.

Использование "стелс"-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе.

3. Самошифрование и полиморфичность.

Цель самошифрования и полиморфичности: максимально усложнить процедуру обнаружения вируса.

Особенность полиморфик-вирусов: трудно поддаются обнаружению; они не имеют сигнатур, т. е. не содержат ни одного постоянного участка кода.

Вредоносные программы

1. Троянские программы.

Троянский конь – это программы, полученные путем явного изменения или добавления команд в программы пользователя и способные вмешиваться в процесс обработки информации.

2. Логические бомбы.

Представляют собой программы или их части, резидентно находящиеся в ситеме и запускаемые всякий раз, когда выполняются определенные условия.

3. **Intended-вирусы.**

К таким вирусам относятся программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножаться по причине ошибок.

4. **Конструкторы вирусов** – это утилита, предназначенная для изготовления новых компьютерных вирусов.

5. **Полиморфные генераторы.**

Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

Защита от компьютерных вирусов

Источники "компьютерных вирусов"

1.Глобальные сети — электронная почта

2.Персональные компьютеры общего пользования

3.Пиратское программное обеспечение

4.Локальные сети

5.Электронные конференции, файл-серверы ftp и BBS

6.Ремонтные службы

Задачи антивирусных программ:

1. Обнаружение вирусов в КС.
2. Блокирование работы программ-вирусов.
3. Устранение последствий воздействия вирусов.

Методы обнаружения вирусов

1. Метод сравнения с эталоном (сканирование).

Суть: для поиска известных вирусов используется маска, т.е программа ищет опознавательную часть вируса – сигнатуру.

Вирусная сигнатура (маска) – некоторая постоянная последовательность кода, специфичная для конкретного вируса и выдающая присутствие вируса в системе.

2. Эвристический анализ.

Эвристический анализатор содержит список подозрительных действий и проверяет программы и загрузочные секторы дисков, пытаясь обнаружить в них код, характерный для вирусов.

3. Антивирусный мониторинг.

Используется резидентными программам-сторожами.

Суть: антивирусная программа постоянно находится в памяти компьютера, выполняя мониторинг подозрительных действий.

4. Метод обнаружения изменений. Используется в программах-ревизорах.

Суть: Антивирусные программы, называемые ревизорами диска, запоминают предварительные характеристики всех областей диска, в которых обычно размещаются вирусы, а затем периодически проверяют их.

5. Программно-аппаратная защита (встраивание антивирусов в BIOS) компьютера.

В системные платы встраиваются простейшие средства защиты от вирусов – специальные контроллера и их программное обеспечение.

Типы антивирусов

1. Программы-детекторы (сканеры).

Принцип работы: выполняют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение.

Достоинства: универсальность.

Недостаток:

- могут находить только те вирусы, которые известны разработчикам,
- размеры антивирусных баз, которые сканерам приходится «таскать за собой»,
- относительно небольшая скорость поиска вирусов.

2. Программы-ревизоры (CRC-сканеры)

Принцип работы: основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов.

Недостатки:

- CRC-сканеры не способны поймать вирус в момент его появления в системе,
- CRC-сканеры не могут детектировать вирус в новых файлах, поскольку в их базах данных отсутствует информация об этих файлах.

3. Программы-доктора или фаги не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы вируса.

Программы фаги также делятся на

- **резидентные** – выполняют сканирование «на лету»,
- **нерезидентные** – обеспечивают проверку оп запросу.

Достоинства: универсальность.

Недостатки: относительно небольшая скорость поиска вирусов, большие размеры антивирусных баз.

4. Антивирусные мониторы – это резидентные программы, перехватывающие вирусоопасные ситуации и сообщающие об этом пользователю.

Достоинства: способность обнаруживать и блокировать вирус на самой ранней стадии его размножения.

Недостатки:

- существование путей обхода защиты монитора,
- большое количество ложных срабатываний.

5. Вакцины или иммунизаторы – это резидентные программы, предоставляющие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, лечащие» этот вирус.

Типы иммунизаторов:

1. Иммунизаторы, сообщающие о заражении.
2. Иммунизаторы, блокирующие заражение каким-либо типом вируса.