Компьютерные вирусы

И

АНТИВИРУСНЫЕ ПРОГРАММЫ.

Вирусы

- Компьютерный вирус — разновидность компьютерных программ, отличительной особенностью которых является способность к размножению (саморепликация). В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру. По этой причине вирусы относят к вредоносным программам.

- Неспециалисты ошибочно относят к компьютерным вирусам и другие виды вредоносных программ - программы-шпионы и даже спам. Известны десятки тысяч компьютерных вирусов, которые распространяются через Интернет по всему миру.

- Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному Кодексу РФ (глава 28, статья 273).

- Согласно доктрине информационной безопасности РФ, в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, и обеспечению информационной безопасности в сетях ЭВМ.

История

- О появлении первого компьютерного вируса много разных мнений. Доподлинно только известно, что на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, его не было, а на Univax 1108 и IBM 360/370, в середине 1970-х годов они уже были. Интересно, что идея компьютерных вирусов появилась намного раньше самих персональных компьютеров. Точкой отсчета можно считать труды известного ученого Джона фон Неймана по изучению самовоспроизводящихся математических автоматов, о которых стало известно в 1940-х годах. В 1951 году он предложил способ создания таких автоматов. А в 1959 году журнал Scientific American опубликовал статью Л. С. Пенроуза, посвященную самовоспроизводящимся механическим структурам. В ней была описана простейшая двумерная модель самовоспроизводящихся механических структур, способных к активации, размножению, мутациям, захвату. Позднее другой ученый Ф.Ж. Шталь реализовал данную модель на практике с помощью машинного кода на IBM 650.

Пути проникновения вирусов в компьютер и механизм распределения вирусов

- Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода А и перезагрузили компьютер, при этом дискета может быть и не системной. Заразить дискету гораздо проще. На нее вирус может попасть, даже если дискету просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление.
- Далее ⟶

- Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус прежде всего переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы.
- После заражения программы вирус может выполнить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания. И наконец, не забывает возвратить управление той программе, из которой был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом, заразится все программное обеспечение.

Признаки появления вирусов

- При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:
- 1.прекращение работы или неправильная работа ранее успешно функционировавших программ
- 2. медленная работа компьютера
- 3. невозможность загрузки операционной системы
- 4. исчезновение файлов и каталогов или искажение их содержимого
- 5. изменение даты и времени модификации файлов
- 6. изменение размеров файлов
- 7. неожиданное значительное увеличение количества файлов на диске
- 8. существенное уменьшение размера свободной оперативной памяти
- 9. вывод на экран непредусмотренных сообщений или изображений
- 10. подача непредусмотренных звуковых сигналов
- 11. частые зависания и сбои в работе компьютера
- Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

Методы защиты от вирусов

- **Сканирование**
- **Выявление изменений**
- **Эвристический анализ**
- **Верификация**
- **Обезвреживание вирусов**
- **Меры профилактики**
- **Как правильно лечить?**

Сканирование

- Если вирус известен и уже проанализирован, то можно разработать программу, выявляющую все файлы и загрузочные записи, инфицированные этим вирусом. Такая программа снабжена «медицинским» справочником, содержащим характерные образцы программного кода вируса. Программа ведет поиск комбинаций байтов, характерных для вируса, но нетипичных для обычных программ. Программы-детекторы, ведущие поиск подобных комбинаций байтов, называются полифагами, или сканерами.
- Для многих вирусов характерна простая комбинация, представляющая собой последовательность фиксированных байтов. Другие вирусы используют более сложные комбинации байтов. Необходимо удостовериться, что комбинация байтов не характерна для обычных программ, иначе программа-детектор сообщит о вирусе даже при его отсутствии.

Выявление изменений

- Для инфицирования программ или загрузочных записей вирусы должны их изменить. Существуют программы, которые специализируются на вылавливании таких изменений. Программу, регистрирующую изменение файлов и загрузочных записей, можно использовать даже для выявления ранее неизвестных вирусов. Однако изменение файлов и загрузочных записей может быть обусловлено целым рядом причин, которые не имеют никакого отношения к вирусам. Выявление изменений само по себе приносит не так много пользы, т.к. необходимо очень четко понимать, какие изменения действительно указывают на наличие вируса.

Эвристический анализ

- Эвристический анализ — это смутное подозрение антивирусной программы о том, что что-то не в порядке.
- При выявлении вирусов с помощью эвристическоrо анализа ведется поиск внешних проявлений или же действий, характерных для некоторых классов известных вирусов. Например, в файлах могут выявляться операции, применяемые вирусами, но редко используемые обычными программами, Могут так-же выявляться попытки записи на жесткие диски или дискеты с помощью нестандартных методов.
- Так же, как при использовании предыдущего метода, с помощью эвристического анализа можно выявить целые классы вирусов, однако необходимо удостовериться, что обычные программы не были приняты за инфицированные.

Верификация

- Рассмотренные выше методы могут свидетельствовать, что программа или загрузочная запись поражены вирусом, однако таким образом нельзя с уверенностью опознать поразивший их вирус и уничтожить его. Программы, с помощью которых можно идентифицировать вирус, называются верификаторами. Верификаторы можно разработать только для уже изученных вирусов после их тщательного анализа.

Обезвреживание вирусов

- Не исключено, что после выявления вируса его можно будет удалить и восстановить исходное состояние зараженных файлов и загрузочных записей, свойственное им до «болезни». Этот процесс называется обезвреживанием (дезинфекцией, лечением).
- Некоторые вирусы повреждают поражаемые ими файлы и загрузочные записи таким образом, что их успешная дезинфекция невозможна. Не исключено также, что детектор одинаково идентифицирует два различных вируса, поэтому дезинфицирующая программа будет эффективна для одного вируса, но бесполезна для другого.
- Дезинфицирующие программы изменяют ваши программы, поэтому они должны быть очень надежными

Меры профилактики

- Рассмотренные выше методы могут применяться с помощью различных способов. Одним из общепринятых методов является использование программ, которые тщательно обследуют диски, пытаясь обнаружить и обезвредить вирусы. Возможно также использование резидентных программ DOS, постоянно проверяющих вашу систему на вирусы. Резидентные программы имеют следующее преимущество: они проверяют все программы на вирусы при каждом их вышолнении. Резидентные программы должны быть очень тщательно разработаны, т.к. иначе они будут задерживать загрузку и выполнение программ.
- Нерезидентные программы эффективны при необходимости одновременного обследования всей системы на вирусы и их обезвреживания. Они представляют собой средство, дополняющее резидентные программы.
- Далее →

- Вы должны помнить о необходимости регулярного выполнения антивирусной программы. К сожалению, как показывает опыт, об этом часто забывают. Пренебрежение профилактическими проверками вашего компьютера увеличивает риск инфицирования не только вашей компьютерной системы, но и распространения вируса на другие компьютеры. И не только через дискеты, вирусы прекрасно распространяются и по локальным сетям.
- Чтобы впоследствии избежать головной боли, лучше всего обеспечить автоматическое выполнение антивирусной программы. В этом случае программа будет защищать ваш компьютер, не требуя от вас каких-либо явных действий. Для обеспечения такой защиты можно при запуске системы установить резидентные антивирусные программы, а также использовать нерезидентные программы, выполняемые при запуске или периодически в указанное время

Как правильно лечить?

- Прежде всего, перезагрузите компьютер, нажав кнопку **Reset**. Такая перезагрузка называется «холодной», в отличие от «теплой», вызываемой комбинацией клавиш **Ctrl-Alt-Del**. Существуют вирусы, которые спокойненько выживают при «теплой» перезагрузке.
- Загрузите компьютер с дискеты, защищенной от записи и с установленными антивирусными программами. Необходимость хранить антивирусный пакет на отдельной защищенной дискете вызвана не только опасностью заражения антивирусных программ вирусом. Частенько вирус специально ищет на жестком диске программу-антивирус и наносит ей повреждения.
- Далее

- Старайтесь почаще обновлять ваши антивирусные программы. Причем как отечественные, так и импортные. Отечественные— потому что у нас пишут вирусы все кому не лень и, чтобы быстро разработать антивирусную программу, надо жить здесь. Импортные — потому что все сильнее сливаются «на-ше» и «их» информационные пространства, все больше западных вирусов проникает к нам по глобальным компьютерным сетям.
- При обнаружении зараженного файла желательно скопировать его на дискету и лишь затем лечить антивирусом. Это делается для того, чтобы в случае некорректного лечения файла, что, к сожалению, случается, попытаться полечить файл другим антивирусом.
- Если вам понадобилась программа из ваших старых архивов или резервных копий, не поленитесь проверить ее. Не рискуйте. Лучше преувеличить опасность, чем недооценить ее.

Классификация вирусов по деструктивным возможностям

- По деструктивным возможностям вирусы можно разделить на следующие:
- Базовые, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения).
- Неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графически и пр. эффектами.
- Опасные вирусы, которые могут привести к серьезным ошибкам и сбоям в работе .
- Очень опасные, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти.
- Далее

- Безвредные вирусы, как правило, производят различные визуальные или звуковые эффекты. Диапазон проявления безвредных вирусов очень широк – от простейшего стирания содержимого экрана до сложных эффектов переворачивания изображения, создания иллюзии «вращения» или «опадания» (например, вирус Cascade-1701).

Выполняемые вредными вирусами деструктивные функции тоже чрезвычайно разнообразны. В процессе своего распространения некоторые вирусы повреждают или искажают некоторые выполняемые программы, дописывая в начало уничтожаемой программы некий код без сохранения исходной последовательности байт. Некоторые вирусы при определенных условиях выполняют форматирование диска, точнее его нулевой дорожки, тем самым уничтожая важную информацию о хранящихся на диске файлах. Другие через определенные (как правило, случайные) промежутки времени перезагружают компьютер, приводя к потере несохраненных данных. В последнее время появилось огромное количество вирусов, направленных на борьбу с антивирусными программами. Некоторые из них при просмотре каталогов ищут программы, в именах которых имеются фрагменты, характерные для антивирусных программ (ANTI, AIDS, SCAN), и при обнаружении таковых пытаются нанести им какой-либо вред: стереть с диска, изменить код в теле программы и др.

Антивирусные программы

- Способы противодействия компьютерным вирусам можно разделить на несколько групп: профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения; методика использования антивирусных программ, в том числе обезвреживание и удаление известного вируса; способы обнаружения и удаления неизвестного вируса.
- С давних времен известно, что к любому яду рано или поздно можно найти противоядие. Таким противоядием в компьютерном мире стали программы, называемые антивирусными. Данные программы можно классифицировать по пяти основным группам: фильтры, детекторы, ревизоры, доктора и вакцинаторы.
- Антивирусы-фильтры - это резидентные программы, которые оповещают пользователя о всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях (например о попытках изменить установки CMOS). При этом выводится запрос о разрешении или запрещении данного действия. Принцип работы этих программ основан на перехвате соответствующих векторов прерываний. К преимуществу программ этого класса по сравнению с программами-детекторами можно отнести универсальность по отношению как к известным, так и неизвестным вирусам, тогда как детекторы пишутся под конкретные, известные на данный момент программисту виды. Это особенно актуально сейчас, когда появилось множество вирусов-мутантов, не имеющих постоянного кода. Однако, программы-фильтры не могут отслеживать вирусы, обращающиеся непосредственно к BIOS, а также BOOT-вирусы, активизирующиеся ещс до запуска антивируса, в начальной стадии загрузки DOS, К недостаткам также можно отнести частую выдачу запросов на осуществление какой-либо операции: ответы на вопросы отнимают у пользователя много времени и действуют ему на нервы. При установке некоторых антивирусов-фильтров могут возникать конфликты с другими резидентными программами, использующими те же прерывания, которые просто перестают работать.
- Далее

- Наибольшее распространение в нашей стране получили программы-детекторы,а вернее программы, объединяющие в себе детектор и доктор. Наиболее известные представители этого класса - Aidstest, Doctor Web,MicroSoft AntiVirus. Антивирусы-детекторы расчитаны на конкретные вирусы и основаны на сравнении последовательности кодов содержащихся в теле вируса с кодами проверяемых программ.Такие программы нужно регулярно обновлять, так как они быстро устаревают и не могут обнаруживать новые виды вирусов.
- Ревизоры - программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов данных ревизора. При этом проверяется состояние BOOT-сектора, таблицы FAT, а также длина файлов, их время создания, атрибуты, контрольная сумма. Анализируя сообщения программы-ревизора, пользователь может решить, чем вызваны изменения: вирусом или нет. При выдаче такого рода сообщений не следует предаваться панике, так как причиной изменений, например, длины программы может быть вовсе и не вирус.
- К последней группе относятся самые неэффективные антивирусы вакцинаторы. Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной.

Типы антивирусных программ.

- Блокираторы
- Сканеры
- Мониторы
- Ревизоры изменений
- Иммунизаторы

Блокираторы

- Сегодня выделяются 5 основных типов антивирусных программ: сканеры, мониторы, ревизоры изменений, иммунизаторы и поведенческие блокираторы. Некоторые из них практически вышли из употребления в связи с низкой эффективностью, другие еще не используются достаточно широко.

Сканеры

- Антивирусные сканеры – пионеры антивирусного движения, впервые появившиеся на свет практически одновременно с самими компьютерными вирусами. Принцип их работы заключается в поиске в файлах, памяти, и загрузочных секторах вирусных масок, т.е. уникального программного кода вируса. Вирусные маски (описания) известных вирусов содержатся в антивирусной базе данных и если сканер встречает программный код, совпадающий с одним из этих описаний, то он выдает сообщение об обнаружении соответствующего вируса.

- Здесь возникает первая проблема, потому что малейшие модификации вируса могут сделать его невидимым для сканера: программный код не будет полностью совпадать с описанием в базе данных. К примеру, существует много вариантов вируса "Чернобыль", и почти для каждого из них антивирусным кампаниям приходилось выпускать отдельное обновление антивирусной базы данных. Другим аспектом данной проблемы являются т.н. полиморфные вирусы, т.е. вирусы, не имеющие постоянного программного кода: заражая очередной файл, они при помощи шифрования самостоятельно изменяют свой вид, при этом сохраняя свою функциональность.
- Далее→