Компьютерные вирусы

Выполнила: Коконова Елена
Проверила: Струневских Алена Васильевна

Содержание

Введение

Чтобы эффективно бороться с вирусами, необходимо иметь представление о “привычках” вирусов и ориентироваться в методах противодействия вирусам. **Вирусом называется специально созданная программа, способная самостоятельно распространяться в компьютерной среде**. Если вирус попал в компьютер вместе с одной из программ или с файлом документа, то через некоторое время другие программы или файлы на этом компьютере будут заражены. Если компьютер подключен к локальной или глобальной сети, то вирус может распространиться и дальше, на другие компьютеры. **Авторы вирусных программ создают их из разных побуждений, однако результаты работы вирусов оказываются, как правило, схожими: инфекции портят программы и документы, находящиеся на компьютере, что часто приводит к их утрате**. Некоторые вирусы способны уничтожать вообще всю информацию на дисках компьютеров, стоимость которой может в десятки и сотни раз превышать стоимость самого компьютера.

Внешние проявления деятельности вирусов весьма разнообразны. Одни вирусы относительно **безопасны для данных и действуют только на нервы пользователю**. Они могут, например, *вызывать осыпание символов на экране, выводить на экран посторонние надписи, воспроизводить посторонние звуки через динамик компьютера*. **Другие** *- немного изменяют данные на диске компьютера. Этот случай наиболее опасен. Если пользователь вовремя не обнаружит вирус, и тот незаметно изменит файлы документов или баз данных, ошибка проявится позже в виде неправильных расчетов или искаженного баланса*. **Встречается вирус, выполняющий компрессию заражаемых файлов**. *Он сжимает файлы без разрешения пользователя*.

Защита информации зависит от того, в какой стадии она находится: создание, хранение, передача по локальным сетям, передача по глобальной сети Интернет и т.д., поэтому это очень сложный и объемный вопрос, требующий отдельного изучения.

Существует несколько основных методов поиска вирусов, которые применяются антивирусными программами: **сканирование; эвристический анализ; обнаружение изменений; резидентные мониторы**. Антивирусы могут реализовывать все перечисленные выше методики, либо только некоторые из них.

Даже, если угрозы вирусов как будто бы нет, необходимо заранее провести мероприятия антивирусной защиты, в том числе организационного характера.

Для успешной борьбы с вирусами можно воспользоваться различными **программными продуктами** отечественного производства, некоторые из которых признаются лучшими в мире.

История возникновения

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.

Виды вирусов

- **файловые вирусы;**
- **загрузочные вирусы;**
- **комбинированные файлово-загрузочные вирусы.**

Кроме того, вирусы бывают: **макрокомандные, резидентные и нерезидентные, полиморфные и маскирующиеся (стелс-вирусы).**

Файловые вирусы

Они записывают свой код в тело исполняемого файла. При запуске зараженной программы вирус первым получает управление, ищет очередную жертву и записывает в нее свой код, а затем передает управление самой программе, так что пользователь ничего не замечает. Метод распространения файловых вирусов довольно прост. Обычно для заражения выбирается что-нибудь интересное: новая игра, самораскрывающийся архив с привлекательным названием или новая версия популярной программы. Однако, даже если не пользоваться программами сомнительного происхождения, можно заразиться через средства **доступа к Internet** или им подобным или получить относительно новую разновидность файлового вируса - **макрокомандный вирус**, *распространяющийся с документами офисных приложений*, таких как Word for Windows или Excel. Документы офисных приложений содержат в себе не только текст и графические изображения, но и макрокоманды. Вирус может изменять существующие макрокоманды и добавлять новые, внедряя свое тело в файл документа. **Для профилактики макрокомандных вирусов нужны антивирусные программы, способных искать подобные инфекции.**

Загрузочные вирусы

Они активизируются и распространяются в момент загрузки операционной системы, еще до того как пользователь успел запустить какую-либо антивирусную программу. Загрузка компьютера обычно производится с жесткого диска - винчестера, а в аварийных случаях - с системной дискеты. Порядок загрузки зависит от выбора, сделанного в программе BIOS Setup. Пользователь может указать, что компьютер должен загружаться либо только с жесткого диска, либо с дискеты с устройства A, а если такой дискеты нет, то с жесткого диска. Возможны и другие варианты, зависящие от конкретной реализации BIOS (например, загрузка с компакт-диска CD-ROM).

Загрузка компьютера производится следующим образом. Сразу после включения электропитания начинает работать программа инициализации, записанная в ПЗУ базовой системы ввода/вывода BIOS. Она проверяет оперативную память и другие устройства компьютера, а затем передает управление программе начальной загрузки, которая также находится в ПЗУ BIOS. Последняя считывает в оперативную память содержимое самого первого сектора нулевой дорожки жесткого диска, в котором находится главная загрузочная запись Master Boot Record (MBR), либо содержимое самого первого сектора нулевой дорожки дискеты, вставленной в дисковод A. Этот сектор содержит загрузочную запись Boot Record (BR). При загрузке с жесткого диска в память по фиксированному адресу считывается содержимое главной загрузочной записи (MBR) - программа загрузки операционной системы с логического диска. Загрузчик просматривает таблицу разделов диска Partition Table, ищет раздел, отмеченный как активный и считывает в оперативную память самый первый сектор этого раздела, сектор загрузочной записи BR. В этом секторе остается еще один загрузчик. Задачей загрузчика BR является считывание в оперативную память стартовых модулей операционной системы и передача им управления. При загрузке с дискеты этот процесс намного проще, так как формат дискеты в точности соответствует формату логического диска.

Самый первый сектор нулевой дорожки дискеты содержит загрузочную запись BR, после считывания в оперативную память ей передается управление. При чем, если дискета - несистемная, в первый сектор ее нулевой дорожки все равно записана программа, единственное назначение которой - вывод сообщения о необходимости вставить в дисковод системную дискету. И данное обстоятельство - присутствие загрузочной записи на несистемной дискете - играет важную роль при распространении загрузочных вирусов.

Таким образом, загрузка операционной системы является многоступенчатым процессом, ход которого зависит от разных обстоятельств. Важно то, что в этом процессе задействовано три программы, которые служат объектом нападения загрузочных вирусов:

- главная загрузочная запись;

- загрузочная запись на логическом диске,

- загрузочная запись на дискете.

Вирусы могут заменять некоторые или все перечисленные объекты, встраивая в них свое тело и сохраняя содержимое оригинального загрузочного сектора в каком-либо другом, более или менее подходящем для этого месте на диске. При последующем включении компьютера *программа загрузки заносит в память вирусный код и передает ему управление. Загрузка операционной системы продолжается под контролем вируса, что затрудняет, а в некоторых случаях и исключает его обнаружение антивирусными программами.*

Загрузочные вирусы распространяются главным образом *при перезапуске* (или включении) компьютера с забытой в дисководе зараженной дискетой, именно тогда (при загрузке) вирус проникает в главную загрузочную запись жесткого диска компьютера. Поэтому можно полностью перекрыть доступ к компьютеру для загрузочных вирусов, отключив в BIOS Setup возможность загрузки с устройства a. Кроме того, не следует без крайней необходимости снимать с дискет защиту от записи. Особенно это относится к дистрибутивным дискетам, с которых выполняется установка ПО, и системным дискетам.

Комбинированные файлово-загрузочное вирусы

Эти самые совершенные и наиболее опасные инфекции используют методы распространения, характерные **и для файловых, и для загрузочных вирусов** - они записывают свое тело в файлы и загрузочные записи дискет и дисков. Вы можете получить такой вирус, либо, загрузив компьютер с зараженной дискеты, либо, запустив зараженный файл, в любом случае результат будет **одинаково печальным**.

Простые и полиморфные вирусы

Многие вирусы легко обнаруживаются по их коду, который они записывают в заражаемый файл или системную область диска в процессе проникновенна. Автору антивирусной программы достаточно выделить из этого кода сигнатуру - уникальную последовательность байтов, характерную только для данного вируса, - после чего антивирусная программа уже в автоматическом режиме просмотрит все файлы и системные области дисков на предмет нахождения “знакомых” сигнатур. Поэтому **проблем с обнаружением таких вирусов нет.**

Однако очень скоро авторы вирусов стали применять **алгоритмы шифрования**, затрудняющие выделение сигнатур. Такие вирусы, получившие название шифрующихся, при заражении новых файлов и системных областей диска шифруют собственный код, раскрывая его только при получении управления. **Сложность обнаружения таких вирусов состоит в том, что при каждом новом заражении они случайным образом изменяют свои коды**. Правда, так как процедура шифрования вируса все же неизменна, то сигнатура в конечном итоге **вычисляется** даже простой антивирусной программой. И поэтому вслед за шифрующимися вирусами **появилась вирусы-мутанты**. Более строгое их название - **полиморфные вирусы**. От простых шифрующихся они отличаются тем, что **полностью изменяют процедуру расшифровки при создании каждой новой особи вируса, поэтому выделить на них сигнатуру невозможно.**

Поэтому для выявления полиморфных вирусов разработаны антивирусные программы нового поколения. В качестве примеров можно привести DoctorWeb, FindVirus из комплекта Dr. Solomon's AntiVirus ToolKit и Norton Antivirus для Windows 95. Эвристический анализатор Doctor Web “выполняет” под своим управлением проверяемые программы и обнаруживает действия, характерные для вирусов. Благодаря этому он находит полиморфные вирусы, даже ранее не известные, так же легко, как и обычные, не использующие механизма маскировки.

Стелс-вирусы

В ходе проверки компьютера антивирусные программы считывают данные - файлы и системные области - с жестких дисков и дискет, пользуясь средствами операционном системы и BIOS. **Стелс-вирусы, или вирусы-невидимки, после запуска оставляют в оперативной памяти компьютера специальные модули, перехватывающие обращение программ к дисковой подсистеме компьютера**. Если такой модуль обнаруживает, что программа пользователя пытается прочитать зараженный файл или системную область диска, он на ходу **подменяет читаемые данные и таким образом остается незамеченным, обманывая антивирусные программы**.

Есть простой способ отключить механизм маскировки стелс-вирусов. **Достаточно загрузить компьютер с незараженной системной дискеты и проверить компьютер антивирусной программой, не запуская программ с диска компьютера** (они могут оказаться зараженными). В этом случае вирус не сможет получить управление и установить в оперативной памяти резидентный модуль, реализующий стелс-алгоритм, антивирус прочитает информацию, действительно записанную на диске, и легко обнаружит “бациллу”.

Антивирусные программы

Существует несколько основных методов поиска вирусов, которые применяются антивирусными программами: сканирование; эвристический анализ; обнаружение изменений; резидентные мониторы. Антивирусы могут реализовывать все перечисленные выше методики, либо только некоторые из них.

Сканирование. Это наиболее традиционный метод поиска вирусов. Он заключается в поиске сигнатур, выделенных из рануей обнаруженных вирусов. Антивирусные программы-сканеры, способные удалить обнаруженные вирусы, обычно называются полифагами. Сканеры могут обнаружить только уже известные и предварительно изученные вирусы, для которых была определена сигнатура. Поэтому программы-сканеры не защитят компьютер от проникновения новых вирусов, число которых постоянно увеличивается. Простые сканеры неспособны обнаружить и полиморфные вирусы, полностью меняющие свой код. Для этой цели необходимо использовать более сложные алгоритмы поиска, включающие эвристический анализ проверяемых программ.

Эвристический анализ. Этот метод нередко используется совместно со сканированием для поиска шифрующихся и полиморфных вирусов. Очень часто эвристический анализ позволяет обнаруживать ранее неизвестные инфекции, хотя лечение в этих случаях обычно оказывается невозможным. Если эвристический анализатор сообщает, что файл или загрузочный сектор, возможно, заражен вирусом, пользователю необходимо провести дополнительную проверку с помощью самых последних версий антивирусных программ - сканеров.

Обнаружение изменений. Заражая компьютер, вирус делает изменения на жестком диске: дописывает свой код в заражаемый файл, изменяет системные области диска и т.д. Антивирусные программы-ревизоры находят такие изменения: они запоминают характеристики всех областей диска, которые могут подвергаться нападению вируса, а затем периодически проверяют их и в случае обнаружения изменений выдают сообщение о подозрении на вирус. Следует учитывать, что не все изменения вызываются вторжением вирусов. Загрузочная запись может измениться при обновлении версии операционной системы, а некоторые программы записывают данные внутри своего исполняемого файла.

Резидентные мониторы. Антивирусные программы, постоянно находящиеся в оперативной памяти компьютера и отслеживающие все подозрительные действия, выполняемые другими программами, носят название резидентных мониторов, или сторожей. К сожалению, они имеют очень много недостатков: занимают много оперативной памяти и раздражают пользователей большим количеством сообщений, по большей части не имеющим отношения к проникновению вирусов.

Даже, если угрозы вирусов как будто бы нет, необходимо заранее провести мероприятия антивирусной защиты, в том числе организационного характера.

Для успешной борьбы с вирусами можно воспользоваться различными программными продуктами отечественного производства, некоторые из которых признаются лучшими в мире.

Антивирусные программы. Существует несколько основных методов поиска вирусов, которые применяются антивирусными программами: сканирование; эвристический анализ; обнаружение изменений; резидентные мониторы. Антивирусы могут реализовывать все перечисленные выше методики, либо только некоторые из них. Антивирусная программа Aidstest (зарегистрированная торговая марка АО ДиалогНаука (DialogueScience), автор Лозинский Д. Н). Программа Aidstest предназначена для обнаружения и исправления программ, зараженных определенными типами вирусов, а именно типами, известными в настоящее время автору. В комплект поставки входит несколько файлов. Перечень опознаваемых вирусов дается в файле aidsread. me, а их краткое описание - в файле aidsvir. txt, также поставляемом в комплекте с антивирусной программой. Этот набор вирусов постоянно пополняется по мере появления у автора новых вирусов. В процессе исправления программные файлы, которые исправить невозможно, стираются.

Антивирусная программа Aidstest (зарегистрированная торговая марка АО ДиалогНаука (DialogueScience), автор Лозинский Д. Н). Программа Aidstest предназначена для обнаружения и исправления программ, зараженных определенными типами вирусов, а именно типами, известными в настоящее время автору. В комплект поставки входит несколько файлов. Перечень опознаваемых вирусов дается в файле aidsread. me, а их краткое описание - в файле aidsvir. txt, также поставляемом в комплекте с антивирусной программой. Этот набор вирусов постоянно пополняется по мере появления у автора новых вирусов. В процессе исправления программные файлы, которые исправить невозможно, стираются.

Антивирусные программы. Существует несколько основных методов поиска вирусов, которые применяются антивирусными программами: сканирование; эвристический анализ; обнаружение изменений; резидентные мониторы. Антивирусы могут реализовывать все перечисленные выше методики, либо только некоторые из них. Антивирусная программа Aidstest (зарегистрированная торговая марка АО ДиалогНаука (DialogueScience), автор Лозинский Д. Н). Программа Aidstest предназначена для обнаружения и исправления программ, зараженных определенными типами вирусов, а именно типами, известными в настоящее время автору. В комплект поставки входит несколько файлов. Перечень опознаваемых вирусов дается в файле aidsread. me, а их краткое описание - в файле aidsvir. txt, также поставляемом в комплекте с антивирусной программой. Этот набор вирусов постоянно пополняется по мере появления у автора новых вирусов. В процессе исправления программные файлы, которые исправить невозможно, стираются.

Антивирусная программа Aidstest (зарегистрированная торговая марка АО ДиалогНаука (DialogueScience), автор Лозинский Д. Н). Программа Aidstest предназначена для обнаружения и исправления программ, зараженных определенными типами вирусов, а именно типами, известными в настоящее время автору. В комплект поставки входит несколько файлов. Перечень опознаваемых вирусов дается в файле aidsread. me, а их краткое описание - в файле aidsvir. txt, также поставляемом в комплекте с антивирусной программой. Этот набор вирусов постоянно пополняется по мере появления у автора новых вирусов. В процессе исправления программные файлы, которые исправить невозможно, стираются.

В момент запуска Aidstest в памяти не должно быть резидентных антивирусных программ, которые блокируют запись в программные файлы. Основной протокол Aidstest достаточно прост и понятен. Про каждый вирус, обнаруженный в файле, сообщается его имя, номинальная длина (в скобках после имени), а в случае успешного лечения через косую черту величина изменения длины файла (бывает и нулевой, если вирус при заражении не изменил длину файла). Программа обнаруживает и обезвреживает все известные ей типы вирусов и в памяти машины. В этом случае в конце работы на экран выдается предложение автоматически перезагрузить систему. Следует учитывать, что обезвреживание вирусов в памяти призвано, в первую очередь обеспечить возможность успешного завершения лечения. Некоторые функции системы при этом могут восстанавливаться неполноценно. Кроме того, свойства вирусов, не связанные с размножением, не убираются, т.е. может продолжаться осыпание букв, появление черного квадрата, исполнение мелодии и т.п.

Aidstest довольно надежно контролирует собственное здоровье относительно большинства типов вирусов. При обнаружении собственного заражения новым типом вируса Aidstest выдает соответствующее сообщение и прекращает работу.

Антивирусная программа Adinf. (зарегистрированная торговая марка АО ДиалогНаука (DialogueScience)). Поскольку Aidstest обнаруживает только уже известные автору вирусы, полезно иметь и программу, обнаруживающую появление на диске новых вирусов. АО ДиалогНаука предлагает один из эффективных и надежных ревизоров - ADinf Д. Мостового, который за несколько секунд просматривает весь диск и сообщает обо всех подозрительных происшествиях.

Norton AntiVirus for Windows 95 (Copiright-Symantec). Пакет включает в себя резидентный мониторинг (Auto-Protect – автозащиту), сканер (Scanner), запускаемый вручную или периодически с помощью планировщика (Scheduler) и проверку при включении компьютера (StartUp) “критических” файлов (config, autoexec, command ит.п.).

Антивирусный пакет AntiViral Toolkit Pro (AVP) для Windows 95 (Windows NT) ЗАО "Лаборатория Касперского" является лучшей программа в своей области. Эта программа - новый шаг в борьбе с компьютерными вирусами. Она представляет из себя полностью 32-х разрядное приложение, оптимизированное для работы в популярной во всем мире среде Microsoft Windows 95 (Windows NT) и использующее все ее возможности. AVP имеет удобный пользовательский интерфейс, характерный для Windows 95, большое количество настроек, выбираемых пользователем, а также одну из самых больших в мире антивирусных баз (свыше 30000), что гарантирует надежную защиту от огромного числа самых разнообразных вирусов.

В ходе работы AVP сканирует: оперативную память (DOS, XMS, EMS), файлы, включая архивные и упакованные, системные сектора, содержащие Master Boot Record, загрузочный сектор (Boot-сектор) и таблицу разбиения диска (Partition Table).

Основные особенности AVP:

Детектирование и удаление огромного числа самых разнообразных вирусов, в том числе:

- полиморфных или самошифрующихся вирусов;

- стелс-вирусов или вирусов-невидимок;

- новых вирусов для Windows 3. XX и Windows 95;

- макро вирусов, заражающих документы Word и таблицы Excel.

Сканирование внутри упакованных файлов (модуль Unpacking Engine).

Сканирование внутри архивных файлов (модуль Extracting Engine).

Сканирование объектов на гибких, локальных, сетевых и CD-ROM дисках.

Эвристический модуль Code Analyzer, необходимый для детектирования неизвестных вирусов.

Поиск в режиме избыточного сканирования.

Проверка объектов на наличие в них изменений.

"AVP Monitor" – резидентный модуль, находящийся постоянно в оперативной памяти компьютера и отслеживающий все файловые операции в системе. Позволяет обнаружить и удалить вирус до момента реального заражения системы в целом.

Заключение

В заключении подведем основные итоги.

Существует несколько основных методов поиска вирусов, которые применяются антивирусными программами: сканирование; эвристический анализ; обнаружение изменений; резидентные мониторы. Антивирусы могут реализовывать все перечисленные выше методики, либо только некоторые из них.

Защита информации каждого пользователя существенно зависит от организации сети. В одноранговой сети все компьютера равноправны и каждый «владелец» компьютера самостоятельно предоставляет его ресурсы в совместное использование в сети (сам себе администратор). При этом не предусмотрена работа множества пользователей с различной степенью доступа (пароль можно задать один) и, по существу, защиты компьютеров в многопользовательском режиме практически нет.

В сетях с выделенным компьютером - сервером реализуется технология «сервер-клиент», которая требует установки сетевой операционной системы (ОС), состоящей из двух компонентов: ОС – сервера (естественно, для установки на сервер) и ОС – рабочей станции (для установки на все остальные компьютеры в сети). Некоторые операционные системы, например, Windows NT, позволяют при установке Windows NT Workstation или более поздней версии Windows 2000 PRO, Windows XP PRO использовать компьютер в качестве сервера и одновременно работать на нем как на рабочей станции (невыделенный сервер).

Для успешной борьбы с вирусами можно воспользоваться различными программными продуктами отечественного производства, некоторые из которых признаются лучшими в мире.

Список литературы

- А. Зубов, М. Шахов – Компьютер, Windows, Программы, ОЛМА-ПРЕСС, 2006 год.
- Виталий Леонтьев – Новейший самоучитель работы на компьютере, ОЛМА-ПРЕСС, Москва 2007 год.
- Виталий Леонтьев - 1000 Лучших программ. Настольная книга пользователя, ОЛМА-ПРЕСС, Москва 2005 год.
- Михаил Крюков – Интернет на все 100 pro, Рипол классик, Москва 2007 год.