Компьютерные вирусы.

М.В.Сапешко[1], И.В. Дворникова[2]

[1] – студентка 1 курса, факультета ВШТ, группы ДТГ-2, Белорусского государственного экономического университета

[2] – ассистент кафедры информационных технологий, Белорусского государственного экономического университета

Аннотация. В этой статье содержится информация о том, что такое компьютерные вирусы, об их разновидностях, о тех, кто их пишет и для каких целей. А также приведены примеры и описание самых популярных антивирусных программ, которые наилучшим образом помогут предостеречь от нежелательного сожителя на компьютере (здесь описано несколько простых правил).

Ключевые слова:
Вирус, макровирусы, антивирус, зараженная дискета, ресурсы компьютера, трояны, самопроизвольное внедрение.

Что такое вирус?

Первые исследования саморазмножающихся искусственных конструкций проводились в середине нынешнего столетия. В работах фон Неймана, Винера и других авторов дано определение и проведен математический анализ конечных автоматов, в том числе и самовоспроизводящихся. Термин «компьютерный вирус» появился позднее - официально считается, что его впервые употребил сотрудник Лехайского университета (США) Ф.Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла, однако строгого определения, что же такое компьютерный вирус, так и не дано, несмотря на то, что попытки дать такое определение предпринимались неоднократно.

На самом деле компьютерный вирус - это просто программа, которая умеет создавать свои функционально идентичные копии. Основная же особенность компьютерных вирусов - возможность их самопроизвольного внедрения в различные объекты операционной системы - присуща многим программам, которые не являются вирусами.

Какие бывают вирусы.

За неполные четверть века существования компьютеров возникла многочисленная армия компьютерных вирусов. В антивирусной базе «Лаборатории Касперского» их уже насчитывается более 50 тыс., и количество их растет день ото дня. Но несмотря на такие внушительные цифры, принципиально новых вирусов немного — в основном это клоны.

По среде обитания вирусы делятся на файловые, загрузочные, макровирусы и сетевые:

1. Файловые вирусы — внедряют свой код в какой-либо исполняемый файл. При запуске такого файла активизируется находящийся в нем вирус, после чего управление передается зараженному файлу.

2. Загрузочные вирусы — записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера. Вирусы активизируются и распространяются в момент загрузки операционной системы — еще до того, как пользователь успел запустить какую-либо антивирусную программу.

3. Макровирусы — используют возможности макроязыков, встроенных в различные системы обработки информации (в текстовые редакторы, электронные таблицы и т.п.). Особенно широко они распространены в таких приложениях, как Microsoft Word и Excel. Вирусы захватывают управление при открытии или закрытии зараженного файла, перехватывают некоторые файловые функции, а затем заражают файлы, к которым происходят последующие обращения. Такие вирусы не только способны функционировать на отдельных компьютерах, но и могут быстро распространяться по сети на все машины, где возможна работа соответствующих приложений.

4. Сетевые вирусы — используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Сейчас наиболее часто встречаются троянские кони (троянцы) и почтовые вирусы (черви), открывающие широкие возможности для хищения информации:

почтовые вирусы — могут относиться к любому типу и к тому же способны распространяться по электронной почте. Когда

человек получает письмо с нейтральным текстом и приложением (например, предложение о сотрудничестве, мое резюме и др.), то при открытии приложения происходит внедрение вируса в систему и начинается рассылка по почте людям из адресной книги текущей почтовой программы от имени пользователя. Каждый раз при использовании почты вирус будет распространяться, следя за появлением новых адресатов;

троянцы — это наиболее опасный тип вирусов, так как основной его задачей является не порча информации, а скрытая ее пересылка автору вируса. Внедряясь в операционную систему (в основном контролируя сеть), троянцы внешне себя никак не проявляют, однако тайком от пользователя они отправляют по сети секретную информацию (номера счетов, пароли на доступ в Интернет и т.д.). Они могут годами «проживать» у беззаботного пользователя, перекачивая данные.

Кто и зачем пишет вирусы

Общественное мнение таково: вирусы пишут либо аморальные хулиганы, либо студенты-дурачки. В последние годы к анализу проблемы подключились профессиональные социологи, психологи и юристы. И вот к каким выводам они пришли.

Все множество авторов вирусов можно условно разделить на три большие группы.

Во-первых, это действительно так называемые студенты - молодые люди, стремящиеся к самоутверждению. Самостоятельно разобраться в том, как работает вирус, непросто. Поэтому написание саморазмножающейся программы для "студента" сопряжено с творческим озарением и моральной победой над собой. Студенческие вирусы, как правило, просты по устройству, неспособны к быстрому распространению, а проявления их ограничиваются выдачей на экран сообщений типа "Профессор Иванов - дурак". "Студенты" - самый многочисленный отряд вирусописателей.

Во-вторых, это действительно хулиганы. Их цель - поскорей заявить о своей "крутизне", отомстить кому-нибудь или просто напакостить ближнему. "Творчество" этих аморальных личностей сводится к использованию давно известных вирусных алгоритмов, а подчас - просто автоматических вирусных программ-генераторов (есть и такие). Зато на разрушительные воздействия хулиганы не скупятся. К счастью, хулиганов на свете немного.

Наконец, третья группа - профессионалы. Это весьма квалифицированные программисты, порой и не такие уж юные. Ими движет стремление к познанию нового и азарт интеллектуального противодействия авторам антивирусных программ. Вирусы, создаваемые профессионалами, изощренны, используют малоизвестные особенности операционных систем, способны быстро и скрытно распространяться, а также более-менее эффективно противодействовать попыткам обнаружения и удаления. По замыслу, такие вирусы максимально незаметны, то есть безвредны. Авторы профессиональных вирусов часто даже и не выпускают их в "дикую природу", а сразу отправляют вирусологам или публикуют в специализированных электронных журналах.

Чем опасен компьютерный вирус

Прежде всего вирус, заразив ваш компьютер, пользуется его ресурсами, "откусывая" часть оперативной памяти, замедляя работу обработчиков прерываний и прочее. Во-вторых, даже самый аккуратно написанный безобидный вирус не может быть полностью совместим со всеми программно-аппаратными конфигурациями, что может изредка приводить к неправильной работе отдельных программ, сбоям и тому подобное. И еще одна причина. Несколько лет назад известный болгарский вирусолог Весселин Бончев провел полномасштабный анализ вопроса и пришел к парадоксальному выводу. Оказывается, так называемые "безобидные" вирусы ежегодно наносят мировой экономике ущерб, исчисляемый сотнями миллионов долларов, но в большинстве случаев потому, что пользователь, узнав о наличии у своего компьютера вируса, начинает беспокоиться, прекращает работу и тратит массу времени и денег на лечение.

Как они распространяются

Наиболее частые пути проникновения вирусов на домашние компьютеры - чужие дискеты с "интересными" играми или "полезными" программами. Однако сейчас игры уже не помещаются на небольшое число дискет. Вместо них начинают ходить с компьютера на компьютер компакт-диски (CD). На них тоже могут оказаться зараженные программы, которые никаким антивирусом не вычистишь, так как с CD невозможно что-либо удалить. Особенно были известны своей

"вшивостью" пиратские компакт-диски китайского производства.

Можно ли заразиться при прочтении зараженной дискеты (без запуска оттуда программ)? Однозначно - НЕТ. Для заражения необходимо, чтобы вирусный код получил управление, а это происходит только при запуске программ. После прочтения зараженной дискеты антивирусы могут обнаруживать вирус в памяти. Это вызвано тем, что перед чтением дискеты считывается boot-сектор для определения па- раметров дискеты. Управление на эти данные, естественно, не передается, так что вирус, хотя и оказывается в памяти, активизироваться оттуда не может. (Если на дискете сидит бутовый вирус то можно заразиться, оставив дискету в дисководе и затем случайно загрузившись с нее просто включив компьютер).

Как бороться с вирусами.

Прежде всего, вот простые правила, которые помогут вам предостерегаться от нежелательного сожителя на вашем компьютере:

1. Обязательно установите на свой компьютер антивирусную программу;

2. Проверяйте каждую получаемую дискету и CD;

3. Всегда держите дискеты защищенными от записи;

4. Ограничьте свои потребности. Невозможно переиграть во все игры, невозможно сгрузить из Интернета все программы. Любимых игр на свете немного, как и любимых женщин. Полезных программ и хороших друзей тоже;

5. С подозрением относитесь к пиратским дискам. Проверяйте их обязательно! Пираты не несут никакой ответственности за ущерб, нанесенный вирусом, "подхваченным" с нелегальной копии;

6. Периодически просматривайте свой компьютер. Удаляйте "мусор", а нужные файлы, содержащие невосстановимую информацию - дублируйте на дискеты или на другой диск. Чтобы потеря информации не оказалась катастрофической, будьте к ней всегда готовы;

7. Антивирусные программы обычно предлагают создать аварийную дискету (Rescue Disk). Не пренебрегайте этой возможностью. Храните созданную дискету на случай, если вирус все же проникнет в ваш компьютер. Тогда, загрузившись с помощью этой дискеты, вы будете уверены, что в памяти компьютера нет резидентных вирусов. С помощью антивирусной программы, которая находится на этой же дискете, можно восстановить поврежденный загрузочный сектор, а также просканировать жесткий диск, чтобы найти и обезвредить вредителей;

8. В антивирусных программах, как в любви, важна не интенсивность, а регулярность. Если у вас имеется не самый крутой антивирус, но есть возможность его постоянного обновления, то это лучше, чем пользоваться программой - чемпионом прошлого года;

9. И наконец, не паникуйте, узнав, что на вашем компьютере поселился вирус. По наблюдениям знающих людей, основной вред от антивируса заключается в неправильных действиях перепуганного пользователя. Выключите компьютер, выпейте кофе, посоветуйтесь с друзьями и знакомыми. А затем - к делу. Если у вас есть достаточно "свежая" антивирусная программа, удаление вируса - процедура почти рутинная.

За недолгую историю существования вирусов антивирусная индустрия разработала целый ряд эффективных мер борьбы с «компьютерной заразой». Со временем некоторые из них устаревали и постепенно сходили со сцены, и на смену им приходили новые технологии, более современные и эффективные. Такая смена поколений характерна и для антивирусных программ. Постоянно происходит противостояние «вирус — антивирус». За появлением нового вируса, использующего новые механизмы распространения (слабости в защите ОС или какого-либо приложения), немедленно следуют адекватные действия — безопасность прежде всего. Наглядным примером может служить разработка технологии эвристического анализатора как механизма защиты от неизвестных вирусов. Сегодня можно выделить пять основных типов антивирусных программ: сканеры, мониторы, ревизоры изменений, иммунизаторы и поведенческие блокираторы.

1. Сканеры — принцип их работы состоит в поиске в файлах, памяти, загрузочных секторах сигнатур вирусов, то есть уникального программного кода вируса. 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.

2. Мониторы — эти резидентные программы являются разновидностью сканеров и осуществляют автоматическую проверку всех используемых файлов в реальном времени.

Современные мониторы производят проверку в момент открытия и закрытия файла, исключая таким образом запуск ранее инфицированных файлов и заражение файла резидентным вирусом.

3. Ревизоры изменений — принцип работы ревизоров основан на снятии оригинальных контрольных сумм с возможных объектов заражения (файлы, загрузочные секторы, системный реестр) и сохранении их в базе данных. Дело в том, что, несмотря на все способы маскировки, вирусы — обычные компьютерные программы. Они, конечно же, имеют возможность тайно создавать новые или внедряться в уже существующие объекты, но все равно оставляют следы своей деятельности в операционной системе. При следующем запуске ревизор сравнивает текущие контрольные суммы с контрольными суммами своей базы данных и сообщает пользователю об изменениях, выделяя вирусоподобные действия.

4. Иммунизаторы — такие программы делятся на два вида: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса. Первые обычно записываются в конец файла, и каждый раз при запуске файла производится проверка на его на изменение. Второй тип иммунизаторов защищает систему от поражения определенным вирусом. Файлы модифицируются таким образом, что вирус принимает их за уже зараженные. Сейчас этот тип антивирусных программ почти не используется из-за неспособности обнаружить заражение вирусами-невидимками.

5. Поведенческие блокираторы — эти резидентные программы перехватывают различные события и в случае подозрительных действий (то есть действий, которые может производить вирус или другая вредоносная программа), запрещают это действие или запрашивают разрешение у пользователя. Блокираторы не совершают поиска уникального программного кода вируса (как это делают сканеры и мониторы) и не сравнивают файлы с их оригиналами (как ревизоры изменений), а отслеживают и нейтрализуют вредоносные программы по их характерным действиям. В перспективе именно такие программы имеют реальную возможность со 100-процентной гарантией противостоять атакам новых вирусов.

Естественно, полагаться только на какой-то один тип антивирусной программы не стоит. У каждого типа антивирусных программ есть как свои достоинства, так и свои недостатки и только комплексное использование нескольких типов антивирусных программ может привести к приемлемому результату.

Популярные антивирусные программы.

Антивирусы бывают разными,но как выбрать лучший из них, и в чем именно они отличаются? Этот вопрос уже посложнее, и не каждый даже компьютерно грамотный чувак и пуперспециалист на него ответит. А все из-за безразмерного увеличения количества различных антивирусов, которые на первый взгляд мало чем отличаются друг от друга. Впрочем, и на второй тоже. Большинство современных антивирусов представляет собой раскрашенные копии одного и того же алгоритма, разработанного более менее правильно и относительно быстро. Единственное, что будет полезно пользователю, так это знать, что антивирус проведет тщательную проверку и обнаружит все вирусы, которыми несчастный юзер успел разжиться за время блуждания по просторам Сети. Но чтобы привлечь пользователя именно к своему антивирусу, многие горе-программеры начинают придумывать различные фишки. Впрочем, иногда им удается придумать действительно что-то полезное и оригинальное, например, эвристические анализаторы кода.

Поэтому немудрено, что в этом диком многообразии антивирусов легко может заблудиться не только новичок, но и даже продвинутый юзер. Ведь каждый месяц появляется по два-три новых антивируса.

Существует несколько критериев-условий, по которым сисадмины с умным видом тестируют антивирусы. Первый критерий - это количество пойманных вирусов и количество реально на компьютере находящихся. Чем больше пойманных, тем лучше. Для тех антивирей, которые поддерживают эвристический анализ, также очень важно, сколько неизвестных (то есть не содержащихся в базе антивируса) вирусов они смогли обнаружить. Второй критерий - это количество ложных срабатываний, когда на любимый Sin.exe антивирусы говорят, что там сидит злобный вирь и надо его полечить, а еще лучше удалить, хотя на самом деле никаких вирусов в нем нет, но глупый антивирус принимает нормальный файл за тело или личинку какого-нибудь суперопасного ЧИХа. Третий критерий - это скорость работы, правда, все современные антивирусы обеспечивают ее на довольно высоком уровне. И последнее - это

всякие мелочи, наподобие автоматической доставки обновленных баз данных с вирусными штаммами с сайта производителя, маленький размер файлов, наличие монитора, который будет перехватывать все сообщения и проверять файлы "на лету", не дожидаясь, пока пользователь запустит проверку. Ниже я привела пример самых популярных антивирусов:

1. Антивирус Касперского (AVP) Personal.

Этот российский антивирусный пакет — один из лидеров антивирусной индустрии. В состав пакета входят: поведенческий блокиратор Office Guard — обеспечивает 100-про-центную защиту от макровирусов; ревизор Inspector — отслеживает все изменения, происходящие на компьютере, и при обнаружении вирусной активности позволяет восстановить оригинальное содержимое диска и удалить вредоносные коды; фоновый перехватчик вирусов Monitor — постоянно присутствует в памяти компьютера и проводит антивирусную проверку всех файлов в момент их запуска, создания или копирования. Это позволяет программе полностью контролировать все файловые операции и предотвращать заражение даже самыми технологически совершенными вирусами; антивирусный модуль Scanner — дает возможность проводить полномасштабную проверку всего содержимого локальных и сетевых дисков. Можно запустить сканер вручную или автоматически в заданное время.

В пакете реализована уникальная технология поиска неизвестных вирусов благодаря эвристическому анализатору второго поколения. С его помощью программа способна защитить компьютер от неизвестных вирусов.

Кроме того, осуществляется постоянная антивирусная фильтрация электронной почты и комплексная проверка почтовой корреспонденции, имеется перехватчик вирусов для MS Office и система перехвата скрипт-вирусов, поддержка архивированных и компрессированных файлов. Обновления антивирусной базы осуществляются через Интернет.

Приобрести эту программу можно на сайте: http://www.kaspersky.ru

2. Dr.Web.

Популярная российская антивирусная программа для Windows 9x/NT/2000/XP предназначена для поиска и обезвреживания файловых, загрузочных и файлово загрузочных вирусов. Программа включает в себя резидентный сторож SplDer Guard, автоматическую систему получения обновлений вирусных баз через Интернет и планировщик расписания автоматических проверок. Реализована проверка почтовых файлов. Кроме того, программа обнаруживает вирусы внутри архивов, упакованных и вакцинированных файлов, в файлах документов для MS Word и Excel. В настоящий момент вирусная база содержит более 28 тыс. записей, но это

не значит, что она менее полная, чем у других программ, — просто в программе Doctor Web одной записью в базе может определяться до нескольких сотен вирусов. Существенной особенностью программы Dr.Web, выделяющей ее среди других, является использование оригинального эвристического анализатора наряду с традиционным методом обнаружения вирусов по их сигнатурам. Использование эвристического анализатора позволяет выявлять вирусы, сигнатуры которых еще неизвестны. Алгоритмы, используемые в Dr.Web, позволяют выявлять все известные в настоящее время типы вирусов.

Другая существенная особенность программы Dr.Web — использование эмулятора процессора, что позволяет обнаруживать сложные шифрованные и полиморфные вирусы, для которых в принципе не работает обычный Сигнатурный поиск.

Приобрести эту программу можно на сайте: http://www.drweb.ru

3.Norton AntiVirus 2002.

Программа предназначена для обнаружения и обезвреживания вирусов, злонамеренных программ ActiveX, аплетов Java. Как и все современные антивирусные пакеты, содержит сканер и монитор. Реализована новая технология эвристического анализа Bloodhound. Производится автоматическое сканирование электронной почты (MS Outlook, MS Outlook Express, Eudora Pro, Eudora Lite, Netscape Messenger, Netscape Mail). Поддерживается функция Script Blocking, которая по-стоянно проверяет скрипты и оповещает пользователя о наличии вредоносной программы, останавливая и обезвреживая вирус до того, как он распространится и заразит файлы. Программа осуществляет обнаружение и лечение вирусов в сжатых файлах (MIME/UU, LHA/LZH, ARJ, CAB, PKLite, LZEXE, ZIP). LiveUpdate проверяет наличие обновлений к базам данных по вирусам при загрузке системы (с центрального сервера), автоматически

скачивает и устанавливает последние версии на вашу систему.

Приобрести эту программу можно на сайте: http://www.symantec.com

4. AntiVir Personal Edition.

Эта мощная антивирусная программа обладает почти такими же возможностями, как Dr.Web, AVP и другие антивирусные программы. В комплект поставки входят: сканер дисков, резидентный сторож, программа управления, планировщик. Программа сканирует файлы, загружаемые из Интернета. Продукт бесплатен для частного некоммерческого использования и выпускается в двух вариантах — для Windows 9x и Windows NT/2000/XP. Большая антивирусная база (более 40 тыс. записей) обновляется раз в неделю и доступна на сайте производителя. Есть также функция автоматической проверки и загрузки обновлений через Интернет. Поддерживается технология drag-and-drop: любой файл, архив, каталог, перенесенные в основное окно программы, тут же будут проверены. Программа проверяет память, загрузочные сектора. Имеется обширный справочник по вирусам.

Для коммерческого использования доступна версия AntiVir Professional с расширенным набором функций, работающая с различными операционными системами.

Приобрести эту программу можно на сайте: http://www.free-av.com/

Заключение.

Компьютерные вирусы подобны таракану. Если посмотреть непредвзято, вирус - это всего-навсего программа, которая может копировать себя на другие программы, чтобы, выполняясь вместе с ними, продолжать размножение. 95% вирусных программ только это и делают. Ну, могут еще дать звуковой сигнал или вывести "приветственную" надпись. Так почему, если вирус не делает ничего, кроме того, что копирует себя, нет желающих терпеть его на своем компьютере?

Самая главная причина - люди хотят иметь "здоровые" программы, подобно тому, как они хотят иметь здоровое тело и здоровый дух. Зараженная, пусть даже безвредным вирусом, программа лишает вас уверенности, что не подведет именно тогда, когда будет особенно нужна.

Если у вас в компьютере вирусов, как блох, - нет никакого сомнения, что довольно скоро они "перейдут" на компьютеры ваших друзей и - что хуже - заказчиков или работодателей. Друзья, может быть, и простят, а вот работы можно лишиться.

Кроме того, вирусы - это лишние и бесполезные (в лучшем случае) программы, "пожирающие" компьютерные ресурсы. 99% вирусов находятся в оперативной памяти работающего компьютера, следовательно, есть вероятность того, что они войдут в конфликт с работающими полезными программами. Модуль зараженной программы занимает больше места на диске, а если таких программ много, то мегабайты, за которые плачены ваши кровные денежки, расходуются совсем не по назначению.

Литература:

1. Игорь Жеку «Старые песни о главном». // Компьютер пресс, №3, март 2002, с. 81-86.
2. http://www.kaspersky.ru
3. http://www.drweb.ru
4. http://www.symantec.com
5. http://www.free-av.com/