Содержание:

Введение

В настоящее время очень многие области деятельности человека связаны с применением компьютеров. Почему же эти электронные машины так плотно внедряются в нашу жизнь? Все довольно тривиально. Они выполняют рутинную расчетную и оформительскую работу, освобождая наш мозг для более необходимых и ответственных задач. В результате утомляемость резко снижается, и мы начинаем работать гораздо производительнее, нежели без применения компьютера.

Возможности современных компьютеров поражают самое богатое воображение. Они способны параллельно выполнять несколько задач, сложность которых довольно велика. По этому некоторые производители задумываются над созданием искусственного интеллекта. Да и сейчас работа компьютера напоминает работу интеллектуального электронного помощника человека.

Но кто бы мог подумать, что этому электронному чуду техники свойственны болезни похожие на человеческие. Он, так же как и человек может подвергнуться атаке «вируса» но компьютерного. И если не принять мер, компьютер скоро «заболеет» т.е. начнет выполнять неправильные действия или вообще «умрет» т.е. повреждения нанесенные «вирусом» окажутся очень серьезными. О том что такое компьютерные вирусы и как с ними бороться пойдет речь далее.

1. Компьютерные вирусы. Что такое компьютерный вирус?

Компьютерный вирус — это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам (т.е. «заражать» их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется зараженной.

Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов (FAT) на диске, «засоряет» оперативную память и т.д.).

Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а скажем, при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус остается в памяти компьютера и время от времени заражает программы и выполняет нежелательные действия на компьютере.

Все действия вируса могут выполняться очень быстро и без выдачи каких либо сообщений, по этому пользователю очень трудно, практически невозможно, определить, что в компьютере происходит что-то необычное.

Пока на компьютере заражено относительно мало програм, наличие вируса может быть практически незаметным. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:

некоторые программы перестают работать или начинают работать неправильно;

на экран выводятся посторонние сообщения, символы и т.д.;

работа на компьютере существенно замедляется;

некоторые файлы оказываются испорченными и т.д.

К этому моменту, как правило, уже достаточно много (или даже большинство) тех программ, с которыми вы работаете, являются зараженными вирусом, а некоторые файлы и диски — испорченными. Более того, зараженные программы с Вашего компьютера могли быть уже перенесены с помощью дискет или локальной сети на компьютеры ваших коллег и друзей.

Некоторые вирусы ведут себя очень коварно. Они вначале незаметно заражают большое число программ и дисков, а затем наносят очень серьезные повреждения, например, форматируют весь женский диск на компьютере, естественно после

этого восстановить данные бывает просто невозможно. А бывают вирусы, которые ведут себя очень скрытно, и портят понемногу данные на жестком диске или сдвигают таблицу размещения файлов (FAT).

Таким образом, если не принимать мер по защите от вируса, то последствия заражения могут быть очень серьезными. Например, в начале 1989г. вирусом, написанным американским студентом Моррисом, были заражены и выведены из строя тысячи компьютеров, в том числе принадлежащих министерству обороны США. Автор вируса был приговорен судом к трем месяцам тюрьмы и штрафу в 270 тыс. дол. Наказание могло быть и более строгим, но суд учел, что вирус не портил данные, а только размножался.

Для того, чтобы программа-вирус была незаметной, она должна иметь небольшие размеры. По этому вирусы пишут обычно на низкоуровневых языках Ассемблер или низкоуровневыми командами языка СИ.

Вирусы пишутся опытами программистами или студентами просто из любопытства или для отместки кому-либо или предприятию, которое обошлось с ними недостойным образом или в коммерческих целях или в целях направленного вредительства. Какие бы цели не преследовал автор, вирус может оказаться на вашем компьютере и постарается произвести те же вредные действия, что и у того, для кого он был создан.

Следует заметить, что написание вируса — не такая уж сложная задача, вполне доступная изучающему программирование студенту. Поэтому еженедельно в мире появляются все новые и новые вирусы. И многие из них сделаны в нашей стране.

2. Испорченные и зараженные файлы

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющихся в компьютере дисках. Но некоторые виды файлов вирус может «заразить». Это означает, что вирус может «внедриться» в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Следует заметить, что тексты программ и документов, информационные файлы баз данных, таблицы табличных процессоров и другие аналогичные файлы не могут быть заражены обычным вирусом, он может их только испортить. Заражение

подобных файлов делается только Макро-вирусами. Эти вирусы могут заразить даже ваши документы.

Обычным вирусом могут быть заражены (табл.1):

Таблица 1. Угроза вирусами

Как правило, каждая конкретная разновидность вируса может заражать только один или два типа файлов. Чаще всего встречаются вирусы, заражающие исполняемые файлы. На втором месте по распространенности загрузочные вирусы. Некоторые вирусы заражают и файлы, и загрузочные области дисков. Вирусы, заражающие драйверы устройств, встречаются крайне редко, обычно такие вирусы умеют заражать и исполняемые файлы.

3. Классификация вирусов

Вирусы можно делить на классы по разным признакам На схеме отображены основные признаки и классы компьютерных вирусов.

Возможно деление вирусов по признаку вероломности: вирусы, моментально поражающие компьютер, форматируют жесткий диск, портят таблицу размещения файлов, портят загрузочные сектора, стирают так называемое Flash-ПЗУ (где находится BIOS) компьютера (вирус «Чернобыль»), другими словами, как можно быстрее наносят непоправимый урон компьютеру.

Сюда же можно отнести и результаты обид программистов, пишущих вирусы, на антивирусные программы. Имеются в виду так называемые аллергии на определенные антивирусные программы. Эти вирусы достаточно вероломны. Вот, например, аллергия на Dr.Weber при вызове этой программы, не долго думая, блокирует антивирус, портит все, что находится в директории с антивирусом и C:\WINDOWS. В результате приходится переустанавливать операционную систему и затем бороться с вирусом другими средствами.

Существуют вирусы, рассчитанные на продолжительную жизнь в компьютере. Они постепенно и осторожно заражают программу за программой, не афишируя, свое присутствие и производят подмену стартовых областей программ на ссылки к месту, где расположено тело вируса. Кроме этого они производят незаметное для пользователя изменение структуры диска, что даст о себе знать, только когда некоторые данные уже будут безнадежно утеряны (например, вирус «OneHalf-

3544″,»Yankey-2C»).

По признаку способов передачи и размножения тоже можно провести разделение.

Раньше вирусы в основном поражали только исполняемые файлы (с расширениями .com и .exe). Действительно, ведь вирус это программа и она должна выполняться.

Теперь вирусы отправляют электронной почтой как демонстрационные программки или как картинки, например, если по электронной почте пришел файл «PicturesForYou.jpg», не спешите его смотреть, тем более что он пришел неизвестно откуда. Если посмотреть на название повнимательнее, то окажется, что оно имеет еще 42 пробела и действительное расширение .exe. То есть реально полное имя файла будет таким: «PicturesForYou.jpg .exe». Теперь любому понятно, что на самом деле несет в себе эта картинка. Это не файл рисунка, который при активизации вызывает осмотрщик рисунков, а наглый чуточку завуалированный вирус, который только и ждет когда его активизируют щелчком мыши или нажатием клавиши . Такой вирус вы сами загружаете себе на компьютер, под оболочкой какой-нибудь картинки, как «Троянского коня». Отсюда и жаргонное название таких вирусов как «Трояны».

На данный момент существуют такие оболочки информационных каналов как Internet Explorer, Outlook Express, Microsoft Office. Сейчас появились немногочисленные классы так называемых «Макро-вирусов». Они содержат скрытые команды для данных оболочек, которые нежелательны для рядового пользователя. И этот код уже не является кодом для компьютера, то есть это уже не программа, а текст программы, выполняемый оболочкой. Таким образом, он может быть записан в любом необходимом формате: .html, .htm — для Internet Explorer, .doc, .xls, .xlw, .txt, .prt, или любой другой — для Microsoft Office и т. д.. Такие вирусы наносят вред только определенного характера, ведь оболочка не имеет команд, к примеру, для форматирования жесткого диска. Но все же этот вид вирусов заслуживает внимания, ведь с помощью скрытых гиперссылок он способен самостоятельно загрузить из Интернета на ваш компьютер тело вируса, а некоторые вирусы способны обновляться и загружаться по частям через Интернет с определенных серверов. Вот, например, одним из японских студентов разработан именно такой вирус, который подключает небольшой «загрузчик» к любому формату входных данных из Интернета. Далее этот загрузчик самостоятельно скачивает из Интернета с сервера с IP-адресом Babilon5 тела вируса. Этих тел четыре. Каждая из них способна самостоятельно разрушать ваш компьютер, но имеет определенное назначение. Этот вирус по типу является гибридом между

макро-вирусами и обычными вирусами. Но надо отметить, что именно гибриды являются наиболее живучими, хитрыми, опасными и многочисленными среди вирусов. Совсем недавно нашумел скандал о программисте, который, как утверждают эксперты, создал и начал распространение макро-вируса, заражавшего текстовые файлы для Microsoft Word. Его вычислили по дате и времени создания исходного документа, которое хранится в невидимых частях .doc файлов. Возможно, что файл был создан другим человеком до того, как к нему был приделан вирус, тогда вопрос о злоумышленнике остается открытым. Но эксперты утверждают, что это именно он.

Например, вирус Win32.HLLM.Klez. один из разновидностей опасного сетевого червя распространяется путем рассылки своих копий по электронной почте. Кроме того, этот червь может распространяться по локальной сети, заражая компьютеры, диски которых являются разделяемыми сетевыми ресурсами, доступными для записи. Попадая в систему, червь рассылает себя по адресам, найденным в адресной книге Windows, в базе данных ICQ и в локальных файлах. Зараженные письма, рассылаемые данным червем, используют одну из сравнительно давно известных ошибок в системе безопасности Internet Explorer, которая позволяет вложенному в письмо программному файлу (с вирусом) автоматически запуститься при простом просмотре почты в программах Outlook и Outlook Express.

4. Маскировка вирусов

Попробуем рассмотреть способы маскировок и защит, применяемых вирусами против нас рядовых пользователей и антивирусных программ.

Вероломность — это основной и самый быстрый способ сделать пакость до обнаружения. Вирус «Чернобыль», например, полностью стирает BIOS (стартовую программу, расположенную в микросхеме ПЗУ, обеспечивающую работу компьютера). После такого компьютер вообще ничего не сможет выдать на экран. Но его работа легко блокируется, если внутри компьютера установлен переключатель, запрещающий писать в область ПЗУ. По этому это был первый, но и, как я думаю, последний представитель аппаратных вирусов.

Регенеративные вирусы делят свое тело на несколько частей и сохраняют их в разных местах жесткого диска. Соответственно эти части способна самостоятельно находить друг друга и собираться для регенерации тела вируса. Программа — антивирус обнаруживает и убивает лишь тело вируса, а части этого тела не

заложены в антивирусной базе, так как являются измененными. От таких вирусов помогает целенаправленное низкоуровневое форматирование жесткого диска. Предварительно необходимо принять осторожные меры по сохранению информации.

Хитрые вирусы прячутся не только от нас, но и от антивирусных программ. Эти «хамелеоны» изменяют сами себя с помощью самых хитрых и запутанных операций, применяя и текущие данные (время создания файла) и используя чуть ли не половину всего набора команд процессора. В определенный момент они, конечно же, по хитрому алгоритму превращаются в подлый вирус и начинают заниматься нашим компьютером. Это самый трудно обнаруживаемый тип вирусов, но некоторые антивирусные программы, такие как «Dr.Weber», способны с помощью так называемого эвристического анализа обнаруживать и обезвреживать и подобные вирусы.

«Невидимые» вирусы чтобы предотвратить свое обнаружение применяют так называемый метод «Stelth». Он заключается в том, что вирус, находящийся в памяти резидентно, перехватывает обращения DOS (и тем самым прикладных программ) к зараженным файлам и областям диска и выдает их в исходном (незараженном) виде. Разумеется этот эффект наблюдается только на зараженном компьютере — на «чистом» компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить. Но некоторые антивирусные программы могут обнаруживать вирусы — «невидимки» даже на зараженных компьютерах.

Сетевой червь «Randon» появился в марте 2003 года. Распространятся по IRC-каналам и ресурсам локальных сетей и заражает компьютеры под управлением операционных систем Windows2000 и Windows XP. Для проникновения на компьютер он подключается к локальной сети или IRC-серверу, сканирует находящийся на нем пользователей, устанавливает с ними соединение по порту 445 и пытается подобрать пароль из встроенного списка наиболее часто используемых фраз. В случае успешного взлома системы «Random» пересылает на нее троянскую программу «Apher», которая, в свою очередь, загружает с удаленного Web-сайта остальные компоненты червя. После этого «Randon» устанавливает свои компоненты в системном каталоге Windows, регистрирует свой основной файл. Для сокрытия присутствия в памяти использует специальную утилиту «HideWindows», которая также является компонентом червя. Благодаря ей он оказывается невидимым для пользователя, так что активный процесс «Randon» можно обнаруживать только в диспетчере задач Windows. Его побочные эффекты – создание на зараженной машине большого объема избыточного трафика и

переполнение IRC-каналов.

«Лаборатория Касперского», один из ведущих разработчиков антивирусных программ, представляет обзор вирусной активности за март 2003г.(табл.2)

Таблица 2. Двадцатка наиболее распространенных вредоносных программ

*не вошедшие в 20 наиболее распространенных

5. Профилактика и борьба с компьютерными вирусами. Основные методы защиты от компьютерных вирусов

Для защиты от вирусов можно использовать:

Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;

профилактические меры, позволяющие уменьшить вероятность заражения вирусом;

специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

копирование информации — создание копий файлов и системных областей дисков;

разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо применять специализированные программы для защиты от вирусов. Эти программы можно разделить на несколько видов:

Программы — детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.

Программы — доктора, или фаги, «лечат» зараженные программы или диски, «выкусывая» из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.

Программы — ревизоры сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий, об этом сообщается пользователю.

Доктора — ревизоры — это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.

Программы — фильтры располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Программы — вакцины, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает эти программы и диски уже зараженными. Эти программы крайне неэффективны и далее не рассматриваются.

Ни один тип антивирусных программ по отдельности не дает, к сожалению, полной защиты от вирусов. По этому наилучшей стратегией защиты от вирусов является многоуровневая, «эшелонная» оборона. Опишем структуру этой обороны.

Средствам разведки в «обороне» от вирусов соответствуют программы — детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На переднем крае обороны находятся программы-фильтры (резидентные программы для защиты от вируса). Эти программы могут первыми сообщить о вирусной атаке и предотвратить заражение программ и диска.

Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры. Ревизоры обнаруживают нападение даже тогда, когда вирус сумел «просочиться» через передний край обороны. Программы-доктора

применяются для восстановления зараженных программ, если ее копий нет в архиве. Но они не всегда лечат правильно. Доктора-ревизоры обнаруживают нападение вируса и лечат зараженные файлы, причем контролируют правильность лечения.

Самый глубокий эшелон обороны — это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.

И, наконец, в «стратегическом резерве» находятся архивные копии информации и «эталонные» дискеты с программными продуктами. Они позволяют восстановить информацию при ее повреждении на жестком диске.

В большинстве случаев для обнаружения вируса, заразившего компьютер, можно найти уже разработанные программы-детекторы. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режим лечения или уничтожения зараженных файлов.

Следует отметить, программа — детектор может обнаруживать только те вирусы, которые ей известны (т.е. занесены в антивирусную базу данных этой программы). Одной из таких программ является AVP Касперского. Все в ней отличается удобным и понятным интерфейсом. Программа выполнена для операционной системы Windows’95/’98/NT, что позволяет ей работать параллельно с другими приложениями. «Лаборатория Касперского» является российским лидером в области разработки систем антивирусной безопасности. Компания предлагает широкий спектр программных продуктов для обеспечения информационной безопасности: антивирусные программы, системы контроля целостности данных, комплексы защиты карманных компьютеров и электронной почты. В конце 2002 года вышла новая версия 4.29 программ семейства Dr.Web. В сканере Dr. Web для Windows усовершенствован режим проверки стартовых файлов для платформы Windows 2000/XP, оптимизировано использование памяти для проверки архивов в режиме по формату.

Большинство программ — детекторов имеют также и функцию «доктора», т.е. они пытаются вернуть зараженные файлы и области диска в их исходное состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или удаляются.

6. Профилактика против заражения вирусом

Рассмотрим некоторые меры, которые позволяют уменьшить вероятность заражения компьютера вирусом, а также свести к минимуму ущерб от заражения вирусом, если оно все-таки произойдет.

Неплохо бы иметь и при необходимости обновлять архивные и эталонные копии используемых пакетов программ и данных. Перед архивацией данных целесообразно проверить их на наличие вируса.

Целесообразно так же скопировать на дискеты служебную информацию вашего диска (FAT, загрузочные сектора) и CMOS (энергонезависимая память компьютера). Копирование и восстановление подобной информации можно выполнить с помощью программы Rescue программного комплекса Norton Utilities.

Следует устанавливать защиту от записи на архивных дискетах.

Не следует заниматься нелицензионным и нелегальным копированием программного обеспечения с других компьютеров. На них может быть вирус.

Все данные, поступающие извне, стоит проверять на вирусы, особенно файлы, «скачанные» из Интернета.

Надо заблаговременно подготовить восстанавливающий пакет на дискетах с защитой от записи.

На время обычной работы, не связанной с восстановлением компьютера, стоит отключить загрузку с дискеты. Это предотвратит заражение загрузочным вирусом.

Используйте программы — фильтры для раннего обнаружения вирусов.

Периодически проверяйте диск программами -детекторами или докторами — детекторами или ревизорами для обнаружения возможных провалов в обороне.

Обновляйте базу антивирусных программ.

Не допускайте к компьютеру сомнительных пользователей.

Заключение

В заключение хотелось бы предостеречь от слишком рьяной борьбы с компьютерными вирусами. Ежедневный запуск полного сканирования жесткого диска на наличие вирусов так же не блестящий шаг в профилактике заражений. Единственный цивилизованный способ защиты от вирусов я вижу в соблюдении профилактических мер предосторожности при работе на компьютере. А так же нужно прибегать к помощи специалистов для борьбы с компьютерным вирусом. Кроме того, даже если вирус все-таки проник на компьютер, это не повод для паники.

Нередко главной бедой Интернета являются не вирусы и хакеры, а такое распространенное явление, как компьютерная безграмотность. Пользуясь аналогией Касперского, незнание правил дорожного движения. Люди, недавно научившиеся принимать и отправлять почту, демонизируют компьютерные вирусы, чуть ли не представляя их себе в виде невидимых черных червячков, лобзающих по проводам. Вот несколько простых правил, соблюдая которые можно постараться избежать заражение вирусами. Первое: не боятся компьютерных вирусов, все они лечатся. Второе: перевести Microsoft Outlook в режим функционирования в зоне ограниченных узлов, что запретит ей автоматическое выполнение некоторых программ – основной принцип размножения компьютерных вирусов. Третье: не открывайте письма от подозрительных адресатов. Четвертое: использовать свежий антивирус.

Список использованных источников

1. Атака из Internet/И. Д. Медведовский, П. В. Семьянов, Д.Г. Леонов,

2. А.В. Лукацкий – М.: Солон-Р, 2002. — 368 с.

3. Бояринов Д., Интернет скоро умрет? // Новое время, 2003, №5, с.39

4. Козлов Д. А., Парандовский А. А., Парандовский А. К. Энциклопедия компьютерных вирусов.- М: Солон-Р, 2002.- 458 с.