Министерство Здравоохранения Украины
Одесский Государственный Медицинский Университет
Кафедра биофизики, информатики и медицинской аппаратуры

Курсовая работа по теме

«Компьютерные вирусы»

Студентки 2-го курса 2-ой группы
Фармацевтического факультета
Сокирной Ольги

Одесса 2009

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ
РАЗДЕЛ 1. СВОЙСТВА КОМПЬЮТЕРНЫХ ВИРУСОВ
1.1 Что такое компьютерный вирус?
РАЗДЕЛ 2. КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ
2.1 Среда обитания
2.2 Способ заражения
2.3 Степень воздействии
2.4 Особенности алгоритма
РАЗДЕЛ 3. ОСНОВНЫЕ ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ
3.1 Основные пути проникновения вирусов
3.2 Обнаружение вирусов
РАЗДЕЛ 4. МЕТОДЫ ЗАЩИТЫ ОТ ВИРУСОВ
4.1 Общие средства защиты информации
РАЗДЕЛ 5. ХАРАКТЕРИСТИКА АНТИВИРУСНЫХ ПРОГРАММ
ЗАКЛЮЧЕНИЕ
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

ВВЕДЕНИЕ

Компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Однако в связи с этим особенно обострилась проблема защиты информации.

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность.

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных саморазмножающихся программ. Совсем недавно заражение вирусом текстовых файлов считалось абсурдом - сейчас этим уже никого не удивишь. Достаточно вспомнить появление "первой ласточки", наделавшей много шума - вируса WinWord. Concept, поражающего документы в формате текстового процессора Microsoft Word for Windows 6.0 и 7.0. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Кто же пишет вирусы? Основную их массу создают студенты и школьники, которые только что изучили язык ассемблера, хотят попробовать

свои силы, но не могут найти для них более достойного применения. Отраден тот факт, что значительная часть таких вирусов их авторами часто не распространяется, и вирусы через некоторое время «умирают» вместе с дискетами, на которых хранятся. Такие вирусы пишутся, скорее всего, только для самоутверждения.

Вторую группу составляют также молодые люди (чаще - студенты), которые еще не полностью овладели искусством программирования, но уже решили посвятить себя написанию и распространению вирусов. Единственная причина, толкающая подобных людей на написание вирусов, это комплекс неполноценности, который проявляет себя в компьютерном хулиганстве.

Из-под пера подобных «умельцев» часто выходят либо многочисленные модификации «классических» вирусов, либо вирусы крайне примитивные и с большим числом ошибок. Значительно облегчилась жизнь подобных вирусописателей после выхода конструкторов вирусов, при помощи которых можно создавать новые вирусы даже при минимальных знаниях об операционной системе и ассемблере, или даже вообще не имея об этом никакого представления. Их жизнь стала еще легче после появления макро-вирусов, поскольку вместо сложного языка Ассемблер для написания 10макро-вирусов достаточно изучить довольно простой Бейсик.

Став старше и опытнее, но, так и не повзрослев, многие из подобных вирусописателей попадают в третью, наиболее опасную группу, которая создает и запускает в мир «профессиональные» вирусы. Эти очень тщательно продуманные и отлаженные программы создаются профессиональными, часто очень талантливыми программистами. Такие вирусы нередко используют достаточно оригинальные алгоритмы, недокументированные и мало кому известные способы проникновения в системные области данных. «Профессиональные» вирусы часто выполнены по технологии «стелс» и (или) являются полиморфик-вирусами, заражают не только файлы, но и

загрузочные сектора дисков, а иногда и выполняемые файлы Windows и OS/2.

Несколько отдельно стоит четвертая группа авторов вирусов - «исследователи». Эта группа состоит из довольно сообразительных программистов, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т.д. Они же придумывают способы внедрения в новые операционные системы, конструкторы вирусов и полиморфик-генераторы. Эти программисты пишут вирусы не ради собственно вирусов, а скорее ради «исследования» потенциалов «компьютерной фауны».

Часто авторы подобных вирусов не запускают свои творения в жизнь, однако очень активно пропагандируют свои идеи через многочисленные электронные издания, посвященные созданию вирусов. При этом опасность от таких «исследовательских» вирусов не падает - попав в руки «профессионалов» из третьей группы, новые идеи очень быстро реализуются в новых вирусах.

Отношение к авторам вирусов тройственное. Во-первых, все, кто пишет вирусы или способствует их распространению, являются «кормильцами» антивирусной индустрии, годовой оборот которой оценивается как минимум две сотни миллионов долларов или даже более того (при этом не стоит забывать, что убытки от вирусов составляют несколько сотен миллионов долларов ежегодно и в разы превышают расходы на антивирусные программы). Если общее количество вирусов к концу 1997 года, скорее всего, достигнет 20.000, то нетрудно подсчитать, что доход антивирусных фирм от каждого вируса ежегодно составляет минимум 10 тысяч долларов. Конечно же, авторам вирусов не следует надеяться на материальное вознаграждение: как показывает практика, их труд был и остается бесплатным. К тому же на сегодняшний день предложение (новые вирусы) вполне удовлетворяет спрос (возможности антивирусных фирм по обработке новых вирусов). Во-вторых, несколько жаль авторов вирусов,

особенно «профессионалов». Ведь для того, чтобы написать подобный вирус, необходимо: а) затратить довольно много сил и времени, причем гораздо больше, чем требуется для того, чтобы разобраться в вирусе, занести его в базу данных или даже написать специальный антивирус; и б) не иметь другого, более привлекательного, занятия. Следовательно, вирусописатели – «профессионалы» довольно работоспособны и одновременно с этим маются от безделья – ситуация весьма печальная.

РАЗДЕЛ 1. СВОЙСТВА КОМПЬЮТЕРНЫХ ВИРУСОВ

1.1 Что такое компьютерный вирус

Сейчас применяются персональные компьютеры, в которых пользователь имеет свободный доступ ко всем ресурсам машины. Именно это открыло возможность для опасности, которая получила название компьютерного вируса.

Что такое компьютерный вирус? Формальное определение этого понятия до сих пор не придумано, и есть серьезные сомнения, что оно вообще может быть дано. Многочисленные попытки дать «современное» определение вируса не привели к успеху. Поэтому мы ограничимся рассмотрением некоторых свойств компьютерных вирусов, которые позволяют говорить о них как о некотором определенном классе программ.

Прежде всего, вирус - это программа. Такое простое утверждение само по себе способно развеять множество легенд о необыкновенных возможностях компьютерных вирусов. Вирус может перевернуть изображение на вашем мониторе, но не может перевернуть сам монитор. К легендам о вирусах-убийцах, «уничтожающих операторов посредством вывода на экран смертельной цветовой гаммы 25-м кадром» также не стоит относиться серьезно. К сожалению, некоторые авторитетные издания время от времени публикуют «самые свежие новости с компьютерных фронтов», которые при ближайшем рассмотрении оказываются следствием не вполне ясного понимания предмета.

Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но, и могут вообще с

ним не совпадать! Вирус не может существовать в «полной изоляции»: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

РАЗДЕЛ 2. КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

-среде обитания,

-способу заражения среды обитания,

-воздействию,

-особенностям алгоритма.

2.1 Среда обитания

В зависимости от среды обитания вирусы можно разделить на:

-сетевые,

-файловые,

-загрузочные,

-файлово-загрузочные.

Сетевые вирусы распространяются по различным компьютерным сетям.

Файловые вирусы внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord).

Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

2.2 Способ заражения

По способу заражения вирусы делятся на:

-резидентные,

-нерезидентные.

Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

2.3 Степень воздействия

По степени воздействия вирусы можно разделить на следующие виды:

Неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах.

Опасные вирусы, которые могут привести к различным нарушениям в работе компьютера очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

2.4 Особенности алгоритма

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия.

Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.

Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

Известны вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Имеются и так называемые квазивирусные или «троянские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

РАЗДЕЛ 3. ОСНОВНЫЕ ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

3.1 Основные пути проникновения 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 A 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.

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.

3.2 Обнаружение вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов.

К ним можно отнести следующие:

-прекращение работы или неправильная работа ранее успешно функционировавших программ;

-медленная работа компьютера;

-невозможность загрузки операционной системы;

-исчезновение файлов и каталогов или искажение их содержимого;

-изменение даты и времени модификации файлов;

-изменение размеров файлов;

-неожиданное значительное увеличение количества файлов на диске;

-существенное уменьшение размера свободной оперативной памяти;

-вывод на экран непредусмотренных сообщений или изображений;

-подача непредусмотренных звуковых сигналов;

-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.

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

РАЗДЕЛ 4. МЕТОДЫ ЗАЩИТЫ ОТ ВИРУСОВ

Для защиты от вирусов можно использовать:

-общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;

-профилактические меры, позволяющие уменьшить вероятность заражения вирусом;

-специализированные программы для защиты от вирусов.

4.1 Общие средства защиты информации

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

а) копирование информации - создание копий файлов и системных областей дисков;

б) 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 недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

ПРОГРАММЫ-ДЕТЕКТОРЫ позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. 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 режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны". Некоторые программы-детекторы могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам. Тем не мение невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова - в ней могут сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, неизвестные программам-детекторам.

Многие программы-детекторы не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Дело в том, что для чтения диска они используют функции DOS, а они перехватываются вирусом, который говорит, что все хорошо. Правда детекторы пытаются выявить вирус путем просмотра оперативной памяти, но против некоторых "хитрых" вирусов это не помогает. Так что надежный диагноз программы-детекторы дают только при загрузке DOS с "чистой", защищенной от записи дискеты, при этом копия программы-детектора также должна быть запущена с этой дискеты.

Некоторые детекторы умеют ловить "невидимые" вирусы, даже когда они активны. Для этого они читают диск, не используя вызовы DOS. Правда, этот метод работает не на всех дисководах.

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

Большинство программ-докторов умеют "лечить" только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. Но

некоторые программы могут обучаться не только способам обнаружения, но и способам лечения новых вирусов.

ПРОГРАММЫ-РЕВИЗОРЫ имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Чтобы проверка состояния программ и дисков проходила при каждой загрузке операционной системы, необходимо включить команду запуска программы-ревизора в командный файл AUTOEXEC.BAT. Это позволяет обнаружить заражение компьютерным вирусом, когда он еще не успел нанести большого вреда. Более того, та же программа-ревизор сможет найти поврежденные вирусом файлы.

Многие программы-ревизоры являются довольно "интеллектуальными" - они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Понятно, что в нормальной ситуации такие изменения практически никогда не встречаются, поэтому программа-ревизор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они вызваны именно вирусом.

Другие программы часто используют различные полумеры – пытаются обнаружить вирус в оперативной памяти, требуют вызовы из первой строки файла AUTOEXEC.BAT, надеясь работать на "чистом" компьютере, и т.д. Увы, против некоторых "хитрых" вирусов все это бесполезно.

Для проверки того, не изменился ли файл, некоторые программы-ревизоры проверяют длину файла. Но эта проверка недостаточна - некоторые

вирусы не изменяют длину зараженных файлов. Более надежная проверка - прочесть весь файл и вычислить его контрольную сумму. Изменить файл так, чтобы его контрольная сумма осталась прежней, практически невозможно.

В последнее время появились очень полезные гибриды ревизоров и докторов, т.е. ДОКТОРА-РЕВИЗОРЫ,- программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние. Такие программы могут быть гораздо более универсальными, чем программы-доктора, поскольку при лечении они используют заранее сохраненную информацию о состоянии файлов и областей дисков. Это позволяет им вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы.

Но они могут лечить не от всех вирусов, а только от тех, которые используют "стандартные", известные на момент написания программы, механизмы заражения файлов.

Существуют также ПРОГРАММЫ-ФИЛЬТРЫ, которые 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 пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы, на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

ПРОГРАММЫ-ВАКЦИНЫ, или ИММУНИЗАТОРЫ, модифицируют программы и диски таким образом, что это не отражается на работе

программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

РАЗДЕЛ 5. ХАРАКТЕРИСТИКА АНТИВИРУСНЫХ ПРОГРАММ

Итак, что же такое антивирус? Почему-то многие считают, что антивирус может обнаружить любой вирус, то есть, запустив антивирусную программу или монитор, можно быть абсолютно уверенным в их надежности. Такая точка зрения не совсем верна. Дело в том, что антивирус - это тоже программа, конечно, написанная профессионалом. Но эти программы способны распознавать и уничтожать только известные вирусы. То есть антивирус против конкретного вируса может быть написан только в том случае, когда у программиста есть в наличии хотя бы один экземпляр этого вируса. Вот и идет эта бесконечная война между авторами вирусов и антивирусов, правда, первых в нашей стране почему-то всегда больше, чем вторых. Но и у создателей антивирусов есть преимущество! Дело в том, что существует большое количество вирусов, алгоритм которых практически скопирован с алгоритма других вирусов. Как правило, такие вариации создают непрофессиональные программисты, которые по каким-то причинам решили написать вирус. Для борьбы с такими "копиями" придумано новое оружие - эвристические анализаторы. С их помощью антивирус способен находить подобные аналоги известных вирусов, сообщая пользователю, что у него, похоже, завелся вирус. Естественно, надежность эвристического анализатора не 100%, но все же его коэффициент полезного действия больше 0,5. Таким образом, в этой информационной войне, как, впрочем, и в любой другой, остаются сильнейшие. Вирусы, которые не распознаются антивирусными детекторами, способны написать только наиболее опытные и квалифицированные программисты.

Таким образом, на 100% защититься от вирусов практически невозможно (подразумевается, что пользователь меняется дискетами с друзьями и играет в игры, а также получает информацию из других источников, например из сетей). Если же не вносить информацию в компьютер извне, заразиться вирусом невозможно - сам он не родится.

В последнее время стремительно растет популярность антивирусной программы - Doctor Web. Dr.Web относится к классу детекторов - докторов, имеет так называемый "эвристический анализатор" - алгоритм, позволяющий обнаруживать неизвестные вирусы. "Лечебная паутина", как переводится с английского название программы, стала ответом отечественных программистов на нашествие самомодифицирующихся вирусов-мутантов. Последние при размножении модифицируют свое тело так, что не остается ни одной характерной цепочки байт, присутствовавшей в исходной версии вируса.

Управление режимами осуществляется с помощью ключей. Пользователь может указать программе, тестировать как весь диск, так и отдельные подкаталоги или группы файлов, либо же отказаться от проверки дисков и тестировать только оперативную память. В свою очередь можно тестировать либо только базовую память, либо, вдобавок, ещё и расширенную (указывается с помощью ключа /H). Doctor Web может создавать отчет о работе (ключ /P), загружать знакогенератор Кириллицы (ключ /R), поддерживает работу с программно-аппаратным комплексом Sheriff (ключ /Z).

Но, конечно, главной особенностью "Лечебной паутины" является наличие эвристического анализатора, который подключается ключом /S. Баланса между скоростью и качеством можно добиться, указав ключу уровень эвристического анализа: 0 - минимальный, 1 - оптимальный, 2 - максимальный; при этом, естественно, скорость уменьшается пропорционально увеличению качества. К тому же Dr.Web позволяет тестировать файлы, вакцинированные CPAV, а также упакованные LZEXE, PKLITE, DIET. Для этого следует указать ключ /U (при этом распаковка файлов будет произведена на текущем устройстве) или /U диск: (где диск: - устройство, на котором будет производиться распаковка), если дискета, с которой запущен Doctor Web защищена от записи. Многие программы упакованы таким способом, хотя пользователь может и не подозревать об

этом. Если ключ /U не установлен, то Doctor Web может пропустить вирус, забравшийся в запакованную программу.

Важной функцией является контроль заражения тестируемых файлов резидентным вирусом (ключ /V). При сканировании памяти нет стопроцентной гарантии, что "Лечебная паутина" обнаружит все вирусы, находящиеся там. Так вот, при задании функции /V Dr.Web пытается воспрепятствовать оставшимся резидентным вирусам, заразить тестируемые файлы.

Тестирование винчестера Dr.Web-ом занимает много времени, поэтому не каждый пользователь может себе позволить тратить столько времени на ежедневную проверку всего жесткого диска. Таким пользователям можно посоветовать более тщательно (с опцией /S2) проверять принесенные извне дискеты. Если информация на дискете находится в архиве (а в последнее время программы и данные переносятся с машины на машину только в таком виде; даже фирмы-производители программного обеспечения, например Borland, пакуют свою продукцию), следует распаковать его в отдельный каталог на жестком диске и сразу же, не откладывая, запустить Dr.Web, задав ему в качестве параметра вместо имени диска полный путь к этому подкаталогу. И все же нужно хотя бы раз в две недели производить полную проверку "винчестера" на вирусы с заданием максимального уровня эвристического анализа.

При начальном тестировании не стоит разрешать программе лечить файлы, в которых она обнаружит вирус, так как нельзя исключить, что последовательность байт, принятая в антивирусе за шаблон может встретиться в здоровой программе. Если по завершении тестирования Dr.Web выдаст сообщения о том, что нашел вирусы, нужно запустить его с опцией /P (если эта опция не была указана) для того, чтобы посмотреть, какой файл заражен. После этого нужно скопировать файл на дискету или на электронный диск и попытаться удалить, указав "Лечебной паутине" ключ /F.

ADinf относится к классу программ-ревизоров. Антивирус имеет высокую скорость работы, способен с успехом противостоять вирусам, находящимся в памяти. Он позволяет контролировать диск, читая его по секторам через BIOS и не используя системные прерывания DOS, которые может перехватить вирус.

Для лечения заражённых файлов применяется модуль ADinf Cure Module, не входящий в пакет ADinf и поставляющийся отдельно. Принцип работы модуля - сохранение небольшой базы данных, описывающей контролируемые файлы. Работая совместно, эти программы позволяют обнаружить и удалить около 97% файловых вирусов и 100% вирусов в загрузочном секторе. К примеру, нашумевший вирус SatanBug был легко обнаружен, и заражённые им файлы автоматически восстановлены. Причем, даже те пользователи, которые приобрели ADinf и ADinf Cure Module за несколько месяцев до появления этого вируса, смогли без труда от него избавиться.

В отличие от других антивирусов Advansed Diskinfoscope не требует загрузки с эталонной, защищённой от записи дискеты. При загрузке с винчестера надежность защиты не уменьшается.

ADinf имеет хорошо выполненный дружественный интерфейс, который реализован в графическом режиме. Программа работает непосредственно с видеопамятью, минуя BIOS, при этом поддерживаются все графические адаптеры. Наличие большого количества ключей позволяет пользователю создать максимально удобную для него конфигурацию системы. Можно установить, что именно нужно контролировать: файлы с заданными расширениями, загрузочные сектора, наличие сбойных кластеров, новые файлы на наличие Stealth-вирусов, файлы из списка неизменяемых и т.д. По своему желанию пользователь может запретить проверять некоторые каталоги (это нужно, если каталоги являются рабочими и в них всё время происходят изменения). Имеется возможность изменять способ доступа к диску (BIOS, Int13h или Int25h/26h), редактировать список расширений

проверяемых файлов, а также назначить каждому расширению собственный вьюер, с помощью которого будут просматриваться файлы с этим расширением. В традициях современного программного обеспечения реализована работа с мышью. Как и вся продукция фирмы "ДиалогНаука", ADinf поддерживает программно-аппаратный комплекс Sheriff.

При инсталляции ADinf в систему имеется возможность изменить имя основного файла ADINF.EXE и имя таблиц, при этом пользователь может задать любое имя. Это очень полезная функция, так как в последнее время появилось множество вирусов, "охотящихся" за антивирусами (например, есть вирус, который изменяет программу Aidstest так, что она вместо заставки фирмы "ДиалогНаука" пишет: "Лозинский - пень"), в том числе и за ADinf.

Полезной функцией является возможность работы с DOS, не выходя из программы. Это бывает полезно, когда нужно запустить внешний антивирус для лечения файла, если у пользователя нет лечащего блока ADinf Cure Module.

Ещё одна интересная функция - запрещение работы с системой при обнаружении изменений на диске. Эта функция полезна, когда за терминалами работают пользователи, не имеющие ещё большого опыта в общении с компьютером. Такие пользователи, по незнанию или по халатности, могут проигнорировать сообщение ADinf и продолжить работу, как ни в чём не бывало, что может привести к тяжёлым последствиям.

Если же установлен ключ -Stop в строке вызова Adinf AUTOEXEC.BAT, то при обнаружении изменений на диске программа потребует позвать системного программиста, обслуживающего данный терминал, а если пользователь нажмет ESC или ENTER, то система перезагрузится и все повторится снова.

Принцип работы ADinf основан на сохранении в таблице копии MASTER-BOOT и BOOT секторов, список номеров сбойных кластеров, схему дерева каталогов и информацию обо всех контролируемых файлах.

Кроме того, программа запоминает и при каждом запуске проверяет, не изменился ли доступный DOS объем оперативной памяти (что бывает при заражении большинством загрузочных вирусов), количество установленных винчестеров, таблицы параметров винчестера в области переменных BIOS.

При первом запуске программа запоминает объем оперативной памяти, находит и запоминает адрес обработчика прерывания Int 13h в BIOS, который будет использоваться при всех последующих проверках, и строит таблицы для проверяемых дисков. При этом проверяется, показывал ли вектор прерывания 13h в BIOS перед загрузкой DOS.

При последующих запусках ADinf проверяет объем оперативной памяти, доступной DOS, переменные BIOS, загрузочные сектора, список номеров сбойных кластеров (так как некоторые вирусы, записавшись в кластер, помечают его, как сбойный, чтобы их не затёрли другие данные, а также не обнаружили примитивные антивирусы). К тому же антивирус ищет вновь созданные и уничтоженные подкаталоги, новые, удаленные, переименованные, перемещённые и изменившиеся файлы (проверяется изменение длины и контрольной суммы). Если ADinf обнаружит, что, изменился файл из списка неизменяемых, либо в файле произошли изменения без изменения даты и времени, а также наличие у файла странной даты (число больше 31, месяц больше 12 или год больше текущего) или времени (минут больше 59, часов больше 23 или секунд больше 59), то он выдаст предупреждение о том, что возможно заражение вирусом.

Если обнаружены изменения BOOT-секторов, то можно в режиме диалога сравнить системные таблицы, которые были до и после изменения, и по желанию восстановить прежний сектор. После восстановления измененный сектор сохраняется в файле на диске для последующего анализа. Новые сбойные кластеры (вернее информация о них в FAT) могут появиться после запуска какой-либо утилиты, лечащей диск (например, NDD) или благодаря действиям вируса. Если Adinf выдал сообщение, а пользователь не запускал никаких подобных утилит, то, скорее всего в компьютер забрался

вирус. При получении такого сообщения следует продолжить проверку, внимательно следя за всеми сообщениями об изменениях файлов и загрузочных секторов. Если в системе действительно вирус, то такие сообщения не заставят себя долго ждать (ведь если все тело вируса будет находиться в "сбойном" кластере, ему никогда не передастся управление).

После проверки ADinf выдаёт сводную таблицу, сообщающую об изменениях на диске. По таблице можно перемещаться стрелками и просматривать подробную информацию, нажав ENTER на интересующем пункте. Существует возможность перехода к любому пункту с помощью "быстрых" клавиш. Изменившиеся файлы можно просмотреть в классическом режиме (шестнадцатеричный дамп / ASCII-коды) с помощью встроенного вьюера, который читает диск через BIOS. Можно также воспользоваться внешним вьюером, предварительно указав к нему путь. Подключив внешний редактор, можно отредактировать изменившийся файл.

Не совсем привычно выглядит форма, в которой ADinf сообщает об обнаруженных подозрительных изменениях: вместо выдачи сообщения о конкретных изменениях он выводит красное окно со списком всех возможных и помечает галочкой пункты, соответствующие изменениям, произошедшим в настоящий момент. Если после получения такого сообщения нажать ESC, то программа запросит о дальнейших действиях: обновить информацию о диске, не обновлять её, лечить (при наличии лечащего модуля ADinf Cure Module) или записать протокол. Для лечения можно воспользоваться внешним антивирусом, загрузив его из окна работы с DOS, которое вызывается комбинацией клавиш ALT+V.

ЗАКЛЮЧЕНИЕ

В заключении хотелось бы предостеречь от слишком рьяной борьбы с компьютерными вирусами. Не стоит переоценивать возможностей этих подлых программ. Например, очень неразумным будет распоряжение начальника отформатировать все жесткие диски на компьютерах в отделе только из-за того, что на одном из них было обнаружено подозрение на такой-то вирус. Это приведет к неоправданной потере информации и сильной потери времени и сил, что, по нанесенному ущербу, будет больше, чем смог бы сделать вирус. Ежедневный за пуск полного сканирования жесткого диска на наличие вирусов так же не блестящий шаг в профилактике заражений. Не превращайте компьютер в неприступную крепость, вооруженную до зубов, а то может не хватить ресурсов для выполнения необходимых задач. На мой взгляд, достаточно установить на компьютере программу Dr.Web. Она не требовательна к ресурсам в отличие от Антивируса Касперского и Norton Antivirusra, да и базы у неё пополняются довольно часто. Единственный цивилизованный способ защиты от вирусов я вижу в соблюдении профилактических мер предосторожности при работе на компьютере.

А, кроме того, даже если вирус все-таки проник на компьютер, это не повод для паники. Методы борьбы с ним описаны во многих изданиях.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Информатика. Базовый курс. / Под ред. С.В.Симоновича. - СПб., 2000 г.
2. А.П.Микляев, Настольная книга пользователя IBM PC 3-издание М.:, "Солон-Р", 2000
3. Симонович С.В., Евсеев Г.А., Мураховский В.И. Вы купили компьютер: Полное руководство для начинающих в вопросах и ответах. - М.: АСТ-ПРЕСС КНИГА; Инфорком-Пресс, 2001
4. Ковтанюк Ю.С., Соловьян С.В. Самоучитель работы на персональном компьютере - К.:Юниор, 2001
5. Информатика: Учебник / под ред. Проф. Н.В. Макаровой. - М.: Финансы и статистика, 1997.
6. Энциклопедия тайн и сенсаций / Подгот. текста Ю.Н. Петрова. - Мн.: Литература, 1996.
7. Безруков Н.Н. Компьютерные вирусы. - М.: Наука, 1991.
8. Мостовой Д.Ю. Современные технологии борьбы с вирусами // Мир ПК. - №8. - 1993.