Тема 2.1. Вирусы как угроза информационной безопасности

1 Компьютерные вирусы и информационная безопасность

Компьютерные вирусы одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам.

Современный компьютерный вирус – это практически незаметный для обычного пользователя «враг», который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей. Необходимость борьбы с компьютерными вирусами обусловлена возможностью нарушения ими всех составляющих информационной безопасности.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Вирусные эпидемии способны блокировать работу организаций и предприятий.

На тему борьбы с вирусами написаны десятки книг и сотни статей, борьбой с компьютерными вирусами профессионально занимаются тысячи специалистов в сотнях компаний. Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономических величин в сотни миллионов долларов ежегодно. Эти оценки явно занижены, поскольку известно становится лишь о части подобных инцидентов.

В последнее время вирусные эпидемии стали настолько масштабными и угрожающими, что сообщения о них выходят на первое место в мировых новостях. При этом следует иметь в виду, что антивирусные программы и аппаратные средства не дают полной гарантии защиты от вирусов, а большинство пользователей не имеют даже основных навыков «защиты» от вирусов.

Е. Касперский в своей книге «Компьютерные вирусы» отмечает, что «Борьба с компьютерными вирусами является борьбой человека с человеческим же разумом. Эта борьба является борьбой умов, поскольку задачи, стоящие перед вирусологами, ставят такие же люди».

2 Характерные черты компьютерных вирусов

Термин «компьютерный вирус» появился в середине 80-х годов, на одной из конференций по безопасности информации, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла, однако, строгого определения компьютерного вируса так и нет.

Трудность, возникающая при попытках сформулировать строгое определение вируса, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и др.) либо присущи другим программам, которые никакого отношения не имеют к вирусам, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения).

Основная особенность компьютерных вирусов заключается в возможности их самопроизвольного внедрения в различные объекты операционной системы – присуща многим программам, которые не являются вирусами, но именно эта особенность является обязательным (необходимым) свойством компьютерного вируса. К более полной характеристике современного компьютерного вируса следует добавить способность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети или файлы, системные области компьютера и прочие выполняемые объекты.

Приведем одно из общепринятых определений вируса, содержащееся в ГОСТе Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

Невозможность четкой формулировки определения компьютерного вируса сама по себе не является проблемой. Главная проблема, которая следует из этого, заключается в том, что нет четких (однозначных) признаков, по которым можно отличить различные файлы от «вирусов», что не позволяет в полной мере устранить их влияние.

Несмотря на все усилия разработчиков антивирусного программного обеспечения до сегодняшнего дня нет достаточно надежных антивирусных средств и, скорее всего, противостояние «вирусописателей» и их оппонентов будет постоянным.

Исходя из этого, необходимо понимать, что нет достаточных программных и аппаратных средств защиты от вирусов, а надежная защита от вирусов может быть обеспечена комплексным применением этих средств и, что немаловажно, соблюдением элементарной «компьютерной гигиены».

3 Хронология развития компьютерных вирусов

Появление первых компьютерных вирусов, способных дописывать себя к файлам, связывают с инцидентом, который произошел в первой половине 70-х годов на системе Univax 1108. Вирус, получивший название «Pervading Animal», дописывал себя к выполняемым файлам – делал практически то же самое, что тысячи современных компьютерных вирусов.

Можно отметить, что в те времена значимые события, связанные с компьютерными вирусами, происходили один раз в несколько лет. С началом 80-х компьютеры становятся все более и более популярными. Появляется все больше и больше программ, начинают развиваться глобальные сети. Результатом этого является появление большого числа разнообразных «троянских коней» – программ, которые при их запуске наносят системе какой-либо вред. В 1986 г. произошла первая эпидемия IBM-PC вируса «Brain». Вирус, заражающий 360Кб дискеты, практически мгновенно разошелся по всему миру. Причиной такого «успеха» являлась, скорее всего, неготовность компьютерного общества к встрече с таким явлением, как компьютерный вирус.

В 1987 г. произошло событие, которое популяризировало «компьютерные вирусы». Код вируса «Vienna» впервые публикуется в книге Ральфа Бюргера «Computer

Viruses: A High Tech Desease». Сразу же в 1987 г. появляются несколько вирусов для IBM-PC.

В пятницу 13-го мая 1988-го года сразу несколько фирм и университетов нескольких стран мира «познакомились» с вирусом «Jerusalem» – в этот день вирус уничтожал файлы при их запуске. Вместе с несколькими другими вирусами, вирус «Jerusalem» распространился по тысячам компьютеров, оставаясь незамеченным – антивирусные программы еще не были распространены в то время так же широко как сегодня, а многие пользователи и даже профессионалы еще не верили в существование компьютерных вирусов. Не прошло и полгода, как в ноябре повальная эпидемия сетевого вируса Морриса (другое название – Internet Worm) заразила более 6000 компьютерных систем в США и практически парализовала их работу. По причине ошибки в коде вируса он неограниченно рассылал свои копии по другим компьютерам сети и, таким образом, полностью забрал под себя ее ресурсы. Общие убытки от вируса Морриса были оценены в 96 миллионов долларов.

В 1992 году появились первые конструкторы вирусов VCL и PS-MPC, которые увеличили и без того немаленький поток новых вирусов. В конце этого года первый вирус для Windows, заражающий выполняемые файлы этой операционной системы, открыл новую страницу компьютерных вирусов.

В дальнейшем развитие компьютерных вирусов напоминает сводку с полей сражений. Создатели вирусов становятся все более изощренными, количество антивирусных программ растет, но ни одна из них не защищает в полной мере. В компьютерном обществе появляется синдром «компьютерного вируса».

К борьбе с вирусами подключаются правоохранительные органы: летом 1994 года автор вируса SMEG был арестован. Примерно в то же самое время в той же Великобритании арестована целая группа вирусописателей, называвшая себя ARCV (Assotiation for Really Cruel Viruses). Некоторое время спустя еще один автор вирусов был арестован в Норвегии.

Август 1995 г. один из поворотных моментов в истории вирусов и антивирусов: обнаружен первый вирус для Microsoft Word («Concept»). Так начиналось время макровирусов.

В 1998 году появились первые полиморфные Windows32-вирусы-»Win95. HPS» и «Win95. Marburg». Разработчикам антивирусных программ пришлось спешно адаптировать к новым условиям методики детектирования полиморфных вирусов, рассчитанных до того только на DOS-вирусы.

Наиболее заметной в 1998 г. была эпидемия вируса «Win95. CIH», ставшая сначала массовой, затем глобальной, а затем повальной – сообщения о заражении компьютерных сетей и домашних персональных компьютеров исчислялись сотнями, если не тысячами. Начало эпидемии зарегистрировано на Тайване, где неизвестный заслал зараженные файлы в местные Интернет-конференции.

С середины 90-х годов основным источником вирусов становится глобальная сеть Интернет.

С 1999 года макровирусы начинают постепенно терять свое господство. Это связано со многими факторами. Во-первых, пользователи осознали опасность, таящуюся в простых doc- и xls-файлах. Люди стали более внимательными, научились пользоваться стандартными механизмами защиты от макровирусов, встроенными в MS Office.

В 2000 году происходят очень важные изменения на мировой «вирусной арене». На свет появляется новый тип вредных кодов – сетевые черви. В это же время появляется супервирус – «Чернобыль». «Чернобыль» исполняемый вирус под Windows, имеющий следующие особенности.

Во-первых, зараженный файл не меняет своего размера по сравнению с первоначальным вариантом. Такой эффект достигается благодаря структуре исполняемых файлов Windows: каждый exe-файл разбит на секции, выровненные по строго определенным границам. В результате между секциями почти всегда образуется небольшой зазор. Хотя такая структура приводит к увеличению места, занимаемого файлом на

диске, она же позволяет существенно повысить скорость работы операционной системы с таким файлом. «Чернобыль» либо записывает свое тело в один такой зазор, либо дробит свой код на кусочки и копирует каждый из них в пустое место между границами. В результате антивирусу сложнее определить, заражен ли файл или нет, и еще сложнее вылечить инфицированный объект.

Во-вторых, «Чернобыль» стал первопроходцем среди программ, умеющих портить аппаратные средства. Некоторые микросхемы позволяют перезаписывать данные, хранящиеся в их мини ПЗУ. Этим и занимается этот вирус.

2000 год еще можно назвать годом «Любовных Писем». Вирус «LoveLetter», обнаруженный 5 мая, мгновенно разлетелся по всему миру, поразив десятки миллионов компьютеров практически во всех уголках планеты. Причины этой глобальной эпидемии кроются в чрезвычайно высокой скорости распространения. Вирус рассылал свои копии немедленно после заражения системы по всем адресам электронной почты, найденным в адресной книге почтовой программы Microsoft Outlook. Подобно обнаруженному весной 1999 года вирусу Melissa, LoveLetter это делал, якобы, от имени владельца зараженного компьютера, о чем тот, естественно, даже не догадывался. Немаловажную роль при распространении вируса сыграл и психологический аспект: мало кто сможет удержаться, чтобы не прочитать любовное письмо от своего знакомого. Именно на это была сделана основная ставка в процессе разработки вируса. О масштабах заражения вирусами в начале 21 века свидетельствует тот факт, что только в мае атаке вируса LoveLetter подверглись более 40 миллионов компьютеров. Уже за первые 5 дней эпидемии вирус нанес мировой экономике убытки в размере 6,7 миллиардов долларов.

С 2000 года сетевые черви начинают полностью преобладать на вирусной арене мира. Сегодня, по данным Лаборатории Касперского, на их долю приходится 89,1 % всех заражений. В структуре распространенности сетевых червей традиционно преобладают почтовые, использующие e-mail в качестве основного транспорта для доставки на целевые компьютеры.

В 2001 году был обнаружен новый тип вредоносных кодов, способных активно распространяться и работать на зараженных компьютерах без использования файлов – «бестелесные черви». В процессе работы такие вирусы существуют исключительно в системной памяти, а при передаче на другие компьютеры - в виде специальных пакетов данных.

Такой поворот событий поставил сложные задачи перед разработчиками антивирусных пакетов. Традиционные технологии (антивирусный сканер и монитор) проявили неспособность эффективно противостоять новой угрозе, поскольку их алгоритм борьбы с вредоносными программами основан именно на перехвате файловых операций. Решением проблемы стал специальный антивирусный фильтр, который в фоновом режиме проверяет все поступающие на компьютер пакеты данных и удаляет «бестелесных» червей. Глобальная эпидемия сетевого червя CodeRed, начавшаяся 20 июля 2001 года, подтвердила действенность технологии «бестелесности». Но еще серьезнее оказалась недавняя эпидемия вируса Helkern' 25 января 2003 года.

4 Выводы по теме 2.1

1) Компьютерные вирусы одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам.

2) Современный компьютерный вирус – это практически незаметный для обычного пользователя «враг», который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей. Необходимость борьбы с компьютерными вирусами обусловлена возможностью нарушения ими всех составляющих информационной безопасности.

3) Антивирусные программы и аппаратные средства не дают полной гарантии защиты от вирусов.

4) Термин «компьютерный вирус» появился в середине 80-х годов на одной из конференций по безопасности информации, проходившей в США.

5) Основная особенность компьютерных вирусов заключается в возможности их самопроизвольного внедрения в различные объекты операционной системы.

6) Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

7) Надежная защита от вирусов может быть обеспечена комплексным применением аппаратных и программных средств и, что немаловажно, соблюдением элементарной «компьютерной гигиены».

Тема 2.2. Классификация компьютерных вирусов

1 Классификация компьютерных вирусов по среде обитания

По среде «обитания» вирусы делятся на:

- файловые;
- загрузочные;
- макровирусы;
- сетевые.

Файловые вирусы внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик жесткого диска (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макровирусы заражают файлы-документы и электронные таблицы популярных офисных приложений.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Существует большое количество сочетаний – например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс- и полиморфик-технологии. Другой пример такого сочетания – сетевой макровирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Заражаемая операционная система является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких OS – DOS, Windows, и т. д. Макровирусы заражают файлы форматов Word, Excel, пакета Office. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

2 Классификация компьютерных вирусов по особенностям алгоритма работы

По особенностям алгоритма работы вирусы делятся на:

- резидентные;
- стелс-вирусы;
- полиморфик-вирусы;
- вирусы, использующие нестандартные приемы.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. К резидентным относятся макровирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

В многозадачных операционных системах время «жизни» резидентного DOS-вируса также может быть ограничено моментом закрытия зараженного DOS-окна, а активность загрузочных вирусов в некоторых операционных системах ограничивается моментом инсталляции дисковых драйверов ОС.

Использование стелс-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов операционной системы на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макровирусов наиболее популярный способ – запрет вызовов меню просмотра макросов.

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования (обнару-

жения) вируса. Полиморфик-вирусы (polymorphic) – это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные нестандартные приемы часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре операционной системы, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т. д.

3 Классификация компьютерных вирусов по деструктивным возможностям

По деструктивным возможностям вирусы можно разделить на:

- безвредные, т. е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске;
- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже повредить аппаратные средства компьютера.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия.

4 Выводы по теме 2.2

1) По среде «обитания» вирусы делятся на файловые, загрузочные, макровирусы, сетевые.

2) Файловые вирусы внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы.

3) Загрузочные вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик жесткого диска.

4) Макровирусы заражают файлы-документы и электронные таблицы офисных приложений.

5) Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

6) По особенностям алгоритма работы вирусы делятся на резидентные, стелс-вирусы, полиморфик-вирусы и вирусы, использующие нестандартные приемы.

7) Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них.

8) Стелс-вирусы скрывают свое присутствие в «среде обитания».

9) Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования (обнаружения) вируса.

10) По деструктивным возможностям вирусы можно разделить на безвредные, неопасные, опасные и очень опасные вирусы.

Тема 2.3. Характеристика «вирусоподобных» программ

1 Виды «вирусоподобных» программ

К «вредным программам», помимо вирусов, относятся:

- «троянские программы» (логические бомбы);
- утилиты скрытого администрирования удаленных компьютеров;
- «intended»-вирусы;
- конструкторы вирусов;
- полиморфик-генераторы.

2 Характеристика «вирусоподобных» программ

1) «Троянские» программы (логические бомбы). К «троянским» программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий. Например, уничтожение информации на дисках при каждом запуске или по определенному графику и т. д. Большинство известных «троянских» программ являются программами, которые маскируются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по электронным конференциям. По сравнению с вирусами «троянские» программы не получают широкого распространения по достаточно простым причинам – они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем. К «троянским» программам также относятся так называемые «дропперы» вирусов – зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют присутствие вируса в файле. Например, файл шифруется или упаковывается неизвестным архиватором, что не позволяет антивирусу «увидеть» заражение.

2) Отметим еще один тип программ (программы – «злые шутки»), которые используются для устрашения пользователя, о заражении вирусом или о каких либо предстоящих действиях с этим связанных, т. е. сообщают о несуществующих опасностях, вынуждая пользователя к активным действиям. Например, к «злым шуткам» относятся программы, которые «пугают» пользователя сообщениями о форматировании

диска (хотя никакого форматирования на самом деле не происходит), детектируют вирусы в незараженных файлах, выводят странные вирусоподобные сообщения и т. д. К категории «злых шуток» можно отнести также заведомо ложные сообщения о новых «супер-вирусах». Такие сообщения периодически появляются в Интернете и обычно вызывают панику среди пользователей.

3) Утилиты скрытого администрирования

Утилиты скрытого администрирования являются разновидностью «логических бомб» («троянских программ»), которые используются злоумышленниками для удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов. Единственная особенность этих программ заставляет классифицировать их как вредные «троянские» программы: отсутствие предупреждения об инсталляции и запуске. При запуске такая программа устанавливает себя в систему и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях программы в системе. Чаще всего ссылка на такую программу отсутствует в списке активных приложений. В результате пользователь может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все, что в них заложил их автор: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д. В результате эти программы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т. п.

4) «Intended»-вирусы

К таким вирусам относятся программы, которые, на первый взгляд, являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении не помещает в начало файла команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо

неправильно устанавливает адрес перехватываемого прерывания (в большинстве приводит к «зависанию» компьютера) и т. д. К категории «intended» также относятся вирусы, которые по приведенным выше причинам размножаются только один раз – из «авторской» копии. Заразив какой-либо файл, они теряют способность к дальнейшему размножению. Появляются «intended»-вирусы чаще всего из-за неумелой перекомпиляции какого-либо уже существующего вируса, либо по причине недостаточного знания языка программирования, либо по причине незнания технических тонкостей операционной системы.

5) Конструкторы вирусов

К данному виду «вредных» программ относятся утилиты, предназначенные для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS, Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы. Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты (COM и/или EXE), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса и т. п.

6) Полиморфные генераторы

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т. е. открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика. Обычно полиморфные генераторы распространяются в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор.

3 Выводы по теме 2.3

1) Вирусоподобная» программа – это программа, которая сама по себе не является вирусом, она может использоваться для внедрения, скрытия или создания вируса.

2) К «вирусоподобным программам» относятся: «троянские программы» (логические бомбы), утилиты скрытого администрирования удаленных компьютеров, «intended»-вирусы, конструкторы вирусов и полиморфик-генераторы.

3) К «троянским» программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий.

4) Утилиты скрытого администрирования являются разновидностью «логических бомб» («троянских программ»), которые используются злоумышленниками для удаленного администрирования компьютеров в сети.

5) Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все, что в них заложил их автор: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д.

6) Конструкторы вирусов предназначены для создания новых компьютерных вирусов.

7) Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами, поскольку в их алгоритм не закладываются функции размножения; главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

Тема 2.4. Антивирусные программы

1 Особенности работы антивирусных программ

Одним из наиболее эффективных способов борьбы с вирусами является использование антивирусного программного обеспечения.

Антивирусная программа – программа, предназначенная для поиска, обнаружения, классификации и удаления компьютерного вируса и вирусоподобных программ.

Вместе с тем необходимо признать, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, поскольку на любой алгоритм антивируса всегда можно предложить новый алгоритм вируса, невидимого для этого антивируса.

При работе с антивирусными программами необходимо знать некоторые понятия:

Ложное срабатывание – детектирование вируса в незараженном объекте (файле, секторе или системной памяти).

Пропуск вируса – недетектирование вируса в зараженном объекте.

Сканирование по запросу – поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.

Сканирование налету – постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т. п.). В этом режиме антивирус постоянно активен, он присутствует в памяти «резидентно» и проверяет объекты без

2 Классификация антивирусных программ

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры, CRC-сканеры (ревизоры). Существуют также антивирусы блокировщики и иммунизаторы.

Сканеры. Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски». Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски или длина этой

маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик-вирусов.

Во многих сканерах используются также алгоритмы «эвристического сканирования», т. е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей. Например, чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Сканеры также можно разделить на две категории – «универсальные» и «специализированные». Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов.

Сканеры также делятся на «резидентные» (мониторы), производящие сканирование «на лету», и «нерезидентные», обеспечивающие проверку системы только по запросу. Как правило, «резидентные» сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как «нерезидентный» сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам – размеры антивирусных баз, которые сканерам приходится хранить и пополнять, и относительно небольшая скорость поиска вирусов.

CRC-сканеры. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая

другая информация: длины файлов, даты их последней модификации и т. д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие «анти-стелс» алгоритмы реагируют практически на 100 % вирусов сразу после появления изменений на компьютере. Характерный недостаток этих антивирусов заключается в невозможности обнаружения вируса с момента его появления и до тех пор, пока не будут произведены изменения на компьютере. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в восстанавливаемых файлах или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах.

Блокировщики. Антивирусные блокировщики – это резидентные программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. К «вирусоопасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочный сектор диска и др., которые характерны для вирусов в моменты из размножения.

К достоинствам блокировщиков относится их способность обнаруживать и блокировать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно активизируется.

Иммунизаторы. Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

3 Факторы, определяющие качество антивирусных программ

Качество антивирусной программы определяется несколькими факторами. Перечислим их по степени важности:

1) Надежность и удобство работы – отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.

2) Качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц, упакованных и архивированных файлов. Отсутствие «ложных срабатываний». Возможность лечения зараженных объектов.

3) Существование версий антивируса под все популярные платформы (DOS, Windows, Linux и т. д.).

4) Возможность сканирование «налету».

5) Существование серверных версий с возможностью администрирования сети.

6) Скорость работы.

4 Выводы по теме 2.4

1. Использование антивирусного программного обеспечения является одним из наиболее эффективных способов борьбы с вирусами.

2. Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры, CRC-сканеры (ревизоры).

3. К антивирусным программам также относятся антивирусы: блокировщики и иммунизаторы.

4. Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти, и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски».

5. Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса.

6. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов.

7. CRC-сканеры, использующие «анти-стелс» алгоритмы реагируют практически на 100% вирусов сразу после появления изменений на компьютере.

8. Антивирусные блокировщики – это резидентные программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю.

9. Качество антивирусной программы определяют надежность и удобство работы, качество обнаружения вирусов, возможность сканирования «на лету» и скорость работы.

Тема 2.5. Профилактика компьютерных вирусов

1 Характеристика путей проникновения вирусов в компьютеры

Рассмотрим основные пути проникновения вирусов в компьютеры пользователей:

1) Глобальные сети – электронная почта.
2) Электронные конференции, файл-серверы ftp.
3) Пиратское программное обеспечение.
4) Локальные сети.
5) Персональные компьютеры «общего пользования».
6) Сервисные службы.

1) Глобальные сети – электронная почта

Основным источником вирусов на сегодняшний день является глобальная сеть Интернет, такова расплата за возможность доступа к массовым информационным ресурсам и службам. Наибольшее число заражений вирусом происходит при обмене электронными письмами через почтовые серверы E-mail. Пользователь получает электронное письмо с вирусом, который активизируется (причем, как правило, незаметно для пользователя) после просмотра файла-вложения электронного письма. После этого вирус (стелс) выполняет свои функции. В первую очередь вирус «заботится» о своем размножении, для этого формируются электронные письма от имени пользователя по всем адресам адресной книги. Далее идет цепная реакция.

Для полноты картины приведем характеристику (вирусные новости «Лаборатории Касперского») наиболее распространенного на 1 марта 2004 г. сетевого червя «Netsky. D».

«Netsky. D» распространяется через письма электронной почты. Зараженные сообщения могут иметь самый разный внешний вид: червь случайным образом выбирает заголовок из 25 вариантов, текст письма (6 вариантов), имя вложенного файла (21 вариант). Вложенный файл имеет фиктивное расширение. PIF, в действительности представляя собой обычную EXE-программу (размер около 17 Кб). Если пользователь имел

неосторожность запустить этот файл, то червь устанавливает себя в систему и запускает процедуры распространения. При установке «Netsky. D» копирует себя с именем WINLOGON. EXE в каталог Windows и регистрирует этот файл в ключе автозапуска системного реестра. Таким образом, он обеспечивает свою активизацию при каждой загрузке операционной системы. Для дальнейшей рассылки червь сканирует файлы наиболее распространенных интернет-приложений (например, WAB, EML, DOC, HTML, MSGи др.), считывает из них адреса электронной почты и незаметно для владельца компьютера отсылает на них свои копии. Важно отметить, что рассылка писем осуществляется в обход установленного на компьютере почтового клиента, но с использованием встроенной SMTP-подпрограммы. С ее помощью «Netsky. D» распространяется через 23 прокси-сервера, расположенных в разных концах мира. Червь имеет ряд побочных действий. В частности, он удаляет из системного реестра ключи другого сетевого червя – «Mydoom», а также пытается нарушить работу антивируса Касперского.

2) Локальные сети

Другой путь «быстрого заражения» – локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере. Далее пользователи при очередном подключении к сети запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.

3) Персональные компьютеры «общего пользования»

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из студентов принес на своих дискетах вирус и заразил какой-либо учебный компьютер, то очередной вирус будет гулять по всему учебному заведению, включая домашние компьютеры студентов и сотрудников.

4) Пиратское программное обеспечение

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных «зон риска». Часто пиратские копии на дискетах и даже на CD-

дисках содержат файлы, зараженные самыми разнообразными типами вирусов. Необходимо помнить, что низкая стоимость программы может дорого обойтись при потере данных.

5) Сервисные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре в сервисных центрах.

2 Правила защиты от компьютерных вирусов

Учитывая возможные пути проникновения вирусов, приведем основные правила защиты от вирусов.

1) Внимательно относитесь к программам и документам, которые получаете из глобальных сетей.

2) Перед тем, как запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте его на наличие вирусов.

3) Используйте специализированные антивирусы – для проверки «на лету» (например, SpIDer Guard из пакета Dr. Web и др.) всех файлов, приходящих по электронной почте (и из Интернета в целом).

4) Для уменьшения риска заразить файл на сервере администраторам сетей следует активно использовать стандартные возможности защиты сети, такие как: ограничение прав пользователей; установку атрибутов «только на чтение» или «только на запуск» для всех выполняемых файлов (к сожалению, это не всегда оказывается возможным) и т. д.

5) Регулярно проверяйте сервер обычными антивирусными программами, для удобства и системности используйте планировщики заданий.

6) Целесообразно запустить новое программное обеспечение на тестовом компьютере, не подключенном к общей сети.

7) Используйте лицензионное программное обеспечение, приобретенное у официальных продавцов.

8) Дистрибутивы копий программного обеспечения (в том числе копий операционной системы) необходимо хранить на защищенных от записи дисках.

9) Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов.

10) Постоянно обновляйте вирусные базы используемого антивируса.

11) Старайтесь не запускать непроверенные файлы, в том числе полученные из компьютерной сети. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами.

12) Ограничьте (по возможности) круг лиц допущенных к работе на конкретном компьютере.

13) Пользуйтесь утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т. д.).

14) Периодически сохраняйте на внешнем носителе файлы, с которыми ведется работа.

15) При работе с Word/Excel включите защиту от макросов, которая сообщает о присутствии макроса в открываемом документе и предоставляет возможность запретить этот макрос. В результате макрос не только не выполняется, но и не виден средствами Word/Excel.

3 Выводы по теме 2.5

1) Профилактика – один из способов защиты компьютеров от вирусов.

2) Компьютерная профилактика предполагает соблюдение правил («компьютерной гигиены»), позволяющих значительно снизить вероятность заражения вирусом и потери каких-либо данных.

3) Профилактика компьютерных вирусов начинается с выявления путей проникновения вируса в компьютер и компьютерные сети.

4) Основными путями проникновения вирусов в компьютеры пользователей являются: глобальные и локальные сети, пиратское программное обеспечение, персональные компьютеры «общего пользования», сервисные службы.

5) Основной источник вирусов на сегодняшний день - глобальная сеть Интернет.

6) Наибольшее число заражений вирусом происходит при обмене электронными письмами через почтовые серверы E-mail.

7) Для исключения заражения вирусами внимательно относитесь к программам и документам, которые получаете из глобальных сетей.

8) Прежде чем запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте его на наличие вирусов.

9) Используйте специализированные антивирусы – для проверки «налету» (например, SpIDer Guard из пакета Dr. Web и др.) всех файлов, приходящих по электронной почте (и из Интернета в целом).

10) Постоянно обновляйте вирусные базы используемого антивируса.

Тема 2.6. Обнаружение неизвестного вируса

1 Обнаружение загрузочного вируса

В загрузочных секторах дисков расположены, как правило, небольшие программы, назначение которых состоит в определении размеров и границ логических дисков (для MBR винчестера) или загрузке операционной системы (для boot-сектора).

В начале следует прочитать содержимое сектора, подозрительного на наличие вируса. Для этой цели удобно использовать DISKEDIT из «Нортоновских утилит». Некоторые загрузочные вирусы практически сразу можно обнаружить по наличию различных текстовых строк, выводимых на экран при активизации вируса. Другие вирусы, поражающие boot-секторы дисков, наоборот, определяются по отсутствию строк, которые обязательно должны присутствовать в boot-секторе. К таким строкам относятся имена системных файлов и строки сообщений об ошибках. Отсутствие или изменение строки-заголовка boot-сектора (строка, название фирмы-производителя программного обеспечения) также может служить сигналом о заражении вирусом.

Однако существуют вирусы, которые внедряются в загрузчик без изменения его текстовых строк и с минимальными изменениями кода загрузчика. Для того чтобы обнаружить такой вирус, в большинстве случаев достаточно отформатировать дискету на заведомо незараженном компьютере, сохранить в виде файла ее boot-сектор, затем некоторое время использовать ее на зараженном компьютере (записать/прочитать несколько файлов), а после этого на незараженном компьютере сравнить ее boot-сектор с оригинальным. Если в коде загрузочного сектора произошли изменения – вирус обнаружен.

2 Обнаружение резидентного вируса

Если в компьютере обнаружены следы деятельности вируса, но видимых изменений в файлах и системных секторах дисков не наблюдается, то вполне возможно, что компьютер поражен одним из «стелс»-вирусов.

Обнаружение резидентного Windows-вируса является крайне сложной задачей. Вирус, находясь в среде Windows как приложение или VxD-двайвер, практически невидим, поскольку одновременно активны несколько десятков приложений и VxD, и

вирус по внешним признакам от них ничем не отличается. Для того чтобы обнаружить программу-вирус в списках активных приложений и VxD, необходимо разбираться во всех тонкостях Windows и иметь полное представление о драйверах и приложениях, установленных на данном компьютере, поэтому приемлемый способ обнаружить резидентный Windows-вирус – загрузить DOS и проверить запускаемые файлы Windows.

3 Обнаружение макровируса

Характерными проявлениями макровирусов являются:

1) Word: невозможность конвертирования зараженного документа Word в другой формат.

2) Word: зараженные файлы имеют формат Template (шаблон), поскольку при заражении Word-вирусы конвертируют файлы из формата Word Document в Template.

3) Excel/Word: в STARTUP (Автозагрузка)-каталоге присутствуют «посторонние» файлы.

4) Excel: наличие в Книге (Book) лишних и скрытых Листов (Sheets).

Для проверки системы на предмет наличия вируса можно использовать пункт меню Сервис/макрос. Если обнаружены «чужие макросы», то они могут принадлежать вирусу. Однако этот метод не работает в случае стелс-вирусов, которые запрещают работу этого пункта меню, что, в свою очередь, является достаточным основанием считать систему зараженной.

Многие вирусы имеют ошибки или некорректно работают в различных версиях Word/Excel, в результате чего Word/Excel выдают сообщения об ошибке.

Если такое сообщение появляется при редактировании нового документа или таблицы и при этом заведомо не используются какие-либо пользовательские макросы, то это также может служить признаком заражения системы.

Сигналом о вирусе являются и изменения в файлах и системной конфигурации Word, Excel и Windows. Многие вирусы тем или иным образом меняют пункты меню, разрешают или запрещают некоторые функции, устанавливают на файлы пароль при их заражении. Большое количество вирусов создает новые секции и/или опции в файле конфигурации Windows (WIN. INI).

Естественно, что к проявлениям вируса относятся такие очевидные факты, как появление сообщений или диалогов с достаточно странным содержанием или на языке, не совпадающем с языком установленной версии Word/Excel.

4 Общий алгоритм обнаружения вируса

При анализе алгоритма вируса необходимо выяснить:

- способ(ы) размножения вируса;
- характер возможных повреждений, которые вирус нанес информации, хранящейся на дисках;
- метод лечения оперативной памяти и зараженных файлов (секторов).

1) При анализе файлового вируса необходимо выяснить, какие файлы (COM, EXE, SYS) поражаются вирусом, в какое место (места) в файле записывается код вируса - в начало, конец или середину файла, в каком объеме возможно восстановление файла (полностью или частично), в каком месте вирус хранит восстанавливаемую информацию.

2) При анализе загрузочного вируса основной задачей является выяснение адреса (адресов) сектора, в котором вирус сохраняет первоначальный загрузочный сектор.

3) Для резидентного вируса требуется также выделить участок кода, создающий резидентную копию вируса. Необходимо также определить, каким образом и где в оперативной памяти вирус выделяет место для своей резидентной копии.

4) Для анализа макровирусов необходимо получить текст их макросов. Для нешифрованных («не-стелс») вирусов это достигается при помощи меню Сервис/Макрос. Если же вирус шифрует свои макросы или использует «стелс»-приемы, то необходимо воспользоваться специальными утилитами просмотра макросов. Такие специализированные утилиты есть практически у каждой фирмы-производителя антивирусов, однако, они являются утилитами «внутреннего пользования» и не распространяются за пределы фирм.

В любом случае, если есть возможность, правильнее всего передавать зараженные файлы специалистам антивирусных лабораторий.

5 Выводы по теме 2.6

1. Некоторые загрузочные вирусы практически сразу можно обнаружить по наличию различных текстовых строк выводимых на экран при активизации вируса.

2. Отсутствие или изменение строки-заголовка boot-сектора (строка, название фирмы-производителя программного обеспечения) также может служить сигналом о заражении вирусом.

3. Если в компьютере обнаружены следы деятельности вируса, но видимых изменений в файлах и системных секторах дисков не наблюдается, то вполне возможно, что компьютер поражен одним из «стелс»-вирусов.

4. Обнаружить резидентный Windows-вирус можно, если загрузить DOS и проверить запускаемые файлы Windows.

5. Для проверки системы на предмет наличия вируса можно использовать пункт меню Сервис/макрос, если обнаружены неизвестные макросы, то они могут принадлежать вирусу.

6. Сигналом о вирусе являются и изменения в файлах и системной конфигурации Word, Excel и Windows.

7. При анализе алгоритма вируса необходимо выяснить: способ(ы) размножения вируса, характер возможных повреждений, которые вирус нанес информации, хранящейся на дисках, метод лечения оперативной памяти и зараженных файлов (секторов).