КОМПЬЮТЕРНЫЕ ВИРУСЫ

А.В. Гринёва[1], Н.А. Малевич[2]

[1] - студентка 1 курса, УЭФ, группы УТ-1, Белорусского государственного экономического университета

[2] – научный руководитель ассистент кафедры информационных технологий Белорусского государственного экономического университета. Минск, 220627, Партизанский проспект 26, тел. (8017)249-19-81. e-mail: petrov@bseu.minsk.by

Аннотация: В данном докладе речь идет о вирусах, их классификации и свойствах. Рассматриваются схемы функционирования различных типов вирусов, пути проникновения их в компьютер и механизм распределения вирусных программ. Насколько это можно было сделать в рамках данного объема, также освещаются признаки появления вирусов, их обнаружение и меры по защите и профилактике.

Ключевые слова: Информация, компьютерные преступления, вирус, сетевые вирусы, файловые вирусы, загрузочные вирусы, файлово-загрузочные вирусы, резидентный вирус, нерезидентные вирусы, антивирусные программы

ВВЕДЕНИЕ

Мы живём на стыке двух тысячелетий, когда человечество вступило в эпоху новой научно-технической революции.

К концу XX века люди овладели многими тайнами превращения вещества и энергии и сумели использовать эти знания для улучшения своей жизни. Но кроме вещества и энергии в жизни человека огромную роль играет ещё одна составляющая – информация. Это самые разнообразные сведения, сообщения, известия, знания, умения.

В середине нашего столетия появились специальные устройства – компьютеры, ориентированные на хранение и преобразование информации и произошла компьютерная революция.

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.

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. Это и послужило стимулом для выбора темы моей работы. Именно об этом я рассказываю в своём реферате. Я показываю основные виды вирусов, рассматриваю схемы их функционирования, причины их появления и пути проникновения в компьютер, а также предлагаю меры по защите и профилактике.

Цель работы – ознакомить пользователя с основами компьютерной вирусологии, научить обнаруживать вирусы и бороться с ними. Метод работы – анализ печатных изданий по данной теме. Передо мной встала непростая задача – рассказать о том, что ещё очень мало исследовалось, и как это получилось – судить вам.

1. КОМПЬЮТЕРНЫЕ ВИРУСЫ, ИХ СВОЙСТВА И КЛАССИФИКАЦИЯ

1.1. Свойства компьютерных вирусов

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? Прежде всего, вирус – это 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 ещё 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, которые 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.

1.2. Классификация вирусов

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

- среде обитания
- способу заражения среды обитания
- воздействию
- особенностям алгоритма

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и 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 Record). Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и 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.

По степени воздействия вирусы можно разделить на следующие виды:

•неопасные, не мешающие работе компьютера, но уменьшающие объём 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.

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, т.к. они перехватывают обращение ОС к пораженным файлам и секторам дисков и подставляют вместо своего тела зараженные участки диска. Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной программы, которые хотя и не способны к самораспространению, но очень опасны, т.к., маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

2. ОСНОВНЫЕ ВИДЫ ВИРУСОВ И СХЕМЫ ИХ ФУНКЦИОНИРОВАНИЯ

Среди всего разнообразия вирусов можно выделить следующие основные группы:

- загрузочные
- файловые
- файлово-загрузочные

Теперь поподробнее о каждой из этих групп.

2.1. Загрузочные вирусы

Рассмотрим схему функционирования очень простого загрузочного вируса, заражающего дискеты. Мы сознательно обойдём все многочисленные тонкости, которые неизбежно встретились бы при строгом разборе алгоритма его функционирования.

Что происходит, когда вы включаете компьютер? Первым делом управление передается программе начальной загрузки, которая хранится в постоянно запоминающем устройстве (ПЗУ) т.е. ПНЗ ПЗУ.

Эта программа тестирует оборудование и при успешном завершении проверок пытается найти дискету в дисководе А:

Всякая дискета размечена на т.н. секторы и дорожки. Секторы объединяются в кластеры, но это для нас несущественно.

Среди секторов есть несколько служебных, используемых операционной системой для собственных нужд (в этих секторах не могут размещаться ваши данные). Среди служебных секторов нас пока интересует один – т.н. сектор начальной загрузки (boot-sector).

В секторе начальной загрузки хранится информация о дискете – количество поверхностей, количество дорожек, количество секторов и пр. Но нас сейчас интересует не эта информация, а небольшая программа начальной загрузки (ПНЗ), которая должна загрузить саму операционную систему и передать ей управление.

Таким образом, нормальная схема начальной загрузки следующая: ПНЗ (ПЗУ) – ПНЗ (диск) – СИСТЕМА

Теперь рассмотрим вирус. В загрузочных вирусах выделяют две части – т.н.. голову и т.н. хвост, который, вообще говоря, может быть пустым.

Пусть у вас имеются чистая дискета и зараженный компьютер, под которым мы понимаем компьютер с активным резидентным вирусом. Как только этот вирус обнаружит, что в дисководе появилась подходящая жертва – в нашем случае не защищенная от записи и еще не заражен-

• выделяет некоторую область диска и помечает её как недоступную ОС, это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные (bad)

• копирует программу начальной загрузки в загрузочном секторе (настоящем) своей головой

• организует цепочку передачи управления согласно схеме.

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору. В цепочке ПНЗ (ПЗУ) – ПНЗ (диск) – СИСТЕМА появляется новое звено: ПНЗ (ПЗУ) – ВИРУС – ПНЗ (диск) – СИСТЕМА

Мораль ясна: **никогда не оставляйте (случайно) дискет в дисководе А.**

Мы рассмотрели схему функционирования простого вируса, живущего в загрузочных секторах дискет. Как правило, вирусы способны заражать не только загрузочные секторы дискет, но и загрузочные секторы винчестеров. При этом, в отличие от дискет, на винчестере имеются 2 типа загрузочных секторов, содержащих программы начальной загрузки, которые получают управление. При загрузке компьютера с винчестера первой берёт на себя управление программа начальной загрузки в MBR (Master Boot Record – главная загрузочная запись). Если ваш жесткий диск разбит на несколько разделов, то лишь один из них помечен как загрузочный (boot). ПНЗ в MBR находит загрузочный раздел винчестера и передает управление на ПНЗ этого раздела. Код последней совпадает с кодом программы начальной загрузки, содержащейся на обычных дискетах, а соответствующие загрузочные секторы отличаются только таблицами параметров. Таким образом, на винчестере имеются два объекта атаки загрузочных вирусов – ПНЗ в MBR и ПНЗ в бут-секторе загрузочного диска.

2.2. Файловые вирусы

Рассмотрим теперь схему работы простого файлового вируса. В отличие от загрузочных вирусов, которые практически всегда резидентны, файловые вирусы совсем не обязательно резидентны. Рассмотрим схему функционирования нерезидентного файлового вируса. Пусть у нас имеется инфицированный исполняемый файл. При запуске такого файла вирус получает управление, производит некоторые действия и передает управление "хозяину" (хотя ещё неизвестно, кто в такой ситуации хозяин).

Какие же действия выполняет вирус? Он ищет новый объект для заражения – подходящий по типу файл, который ещё не заражен (в том случае, если вирус "приличный", а то попадаются такие, что заражают сразу, ничего не проверяя). Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. Кроме своей основной функции – размножения, вирус вполне сделать что-нибудь замысловатое (сказать, спросить, сыграть) – это уже зависит от фантазии автора вируса. Если файловый вирус резидентный, то он установится в память и получит возможность заражать файлы и проявлять прочие способности не только во время работы зараженного файла. Заражая исполняемый файл, вирус всегда изменяет его код – следовательно, заражение исполняемого файла всегда можно обнаружить. Но, изменяя код файла, вирус не обязательно вносит другие изменения:

• он не обязан менять длину файла

• он не обязан менять неиспользуемые участки кода

• он не обязан менять начало файла

Наконец, к файловым вирусам часто относят вирусы, которые "имеют некоторое отношение к файлам", но не обязаны внедряться в их код. Рассмотрим в качестве примера схему функционирования вирусов известного семейства Dir-II. Нельзя не признать, сто появившись в 1991г., эти вирусы стали причиной настоящей эпидемии чумы в России. Рассмотрим модель, на которой ясно видна основная идея вируса. Информация о файлах хранится в каталогах. Каждая запись каталога включает в себя имя файла, дату и время создания, некоторую дополнительную информацию, номер первого кластера файла и т.н. резервные байты. Последние отправлены "про запас" и самой MS-DOS не используется.

При запуске исполняемых файлов система считывает из записи в каталоге первый кластер файла и далее все остальные кластеры. Вирусы семейства Dir-II производят следующую "реорганизацию" файловой системы: сам вирус записывается в некоторые свободные секторы диска, которые он помечает как сбойные. Кроме того, он сохраняет информацию о первых кластерах исполняемых файлов в резервных битах, а на место этой информации записывает ссылки на себя.

Таким образом, при запуске любого файла вирус получает управление (ОС запускает его сама), резидентно устанавливается в память и передает управление вызванному файлу.

2.3. Загрузочно-файловые вирусы

Мы не станем рассматривать модель загрузочно-файлового вируса, ибо никакой новой информации вы при этом не узнаете. Но здесь представляется удобный случай кратко обсудить крайне "популярный" в последнее время загрузочно-файловый вирус OneHalf, заражающий главный загрузочный сектор (MBR) и исполняемые файлы. Основное разрешительное действие - шифрование секторов винчестера. При каждом запуске вирус шифрует очередную порцию секторов, а зашифровав половину жесткого диска, радостно сообщает об этом. Основная проблема при лечении данного вируса состоит в том, сто

недостаточно просто удалить вирус из MBR и файлов, надо расшифровать зашифрованную им информацию. Наиболее "смертельное" действие – просто переписать новый здоровый MBR. Главное – не паникуйте. Взвесьте все спокойно, посоветуйтесь со специалистами.

2.4. Полиморфные вирусы

Большинство вопросов связано с термином "полиморфный вирус". Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным. Объясним же, что это такое.

Полиморфные вирусы – вирусы, модифицирующие свой код в зараженных программах таким образом, что 2 экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат год генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Полиморфные вирусы – это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать сам себя всего сразу, а может выполнить такую расшифровку "по ходу действия", может вновь шифровать уже отработавшие участки. Всё это делается ради затруднения анализа кода вируса.

3. ПРИЗНАКИ ПОЯВЛЕНИЯ 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.

4. ОБНАРУЖЕНИЕ ВИРУСОВ И МЕРЫ ПО ЗАЩИТЕ И ПРОФИЛАКТИКЕ

4.1. Как обнаружить вирус? Традиционный подход

Итак, некий вирусописатель создает вирус и запускает его в "жизнь". Некоторое время он, возможно, погуляет вволю, но рано или поздно "лафа" закончится. Кто-то заподозрит что-нибудь неладное. Как правило, вирусы обнаруживают обычные пользователи, которые замечают те или иные аномалии в поведении компьютера. Они, в большинстве случаев, не способны самостоятельно справиться с заразой, но этого от них и не требуется.

Необходимо лишь, чтобы как можно скорее вирус попал в руки специалиста. Профессионалы будут его изучать, выяснять, "что он делает", "как он делает", "когда он делает" и пр. В процессе такой работы собирается вся необходимая информация о данном вирусе, в частности, выделяется сигнатура вируса - последовательность байтов, которая вполне определенно его характеризует. Для построения сигнатуры обычно берутся наиболее важные и характерные участки кода вируса. Одновременно становятся ясны механизмы работы вируса, где находится оригинальный загрузочный сектор, а в случае файлового – способ заражения файла. Полученная информация позволяет выяснить:

- как обнаружить вирус, для этого уточняются методы поиска сигнатур в потенциальных объектах вирусной атаки – файлах или загрузочных секторах
- как обезвредить вирус, если это возможно, разрабатываются алгоритмы удаления вирусного кода из пораженных объектов

4.2. Программы обнаружения и защиты от вирусов

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называют *антивирусными.* Различают следующие виды антивирусных программ: программы-детекторы, программы-доктора или фаги, программы-ревизоры, программы-фильтры, программы-вакцины или иммунизаторы.

Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в

оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора или *фаги*, а также *программы-вакцины* не только находят зараженные вирусами файлы, но и "лечат" их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известные из них: Aidstest, Scan, Norton AntiVirus, Doctor Web.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление версий.

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки ОС. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная в России программа Adinf.

Программы-фильтры или "*сторожа*" представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться: попытки коррекции файлов с расширениями COM, EXE; изменение атрибутов файла; прямая запись на диск по абсолютному адресу; запись в загрузочные сектора диска; загрузка резидентной программы. При попытке какой-либо программы произвести указанные действия "сторож" посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, т.к. способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако, они не "лечат" файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их "назойливость" (например, они постоянно выдают предупреждение о любой попытке копирования испоняемого файла), а также возможные конфликты с другим программным обеспечением. Примером программы-фильтра является программа Vsafe, входящая в состав пакета утилит MS DOS.

Вакцины или *иммунизаторы* – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, "лечащие" этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

4.3. Основные меры по защите от вирусов

Для того, чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:

- оснастите свой компьюте современными антивирусными программами, например Aidstest, Doctor Web, и постоянно возобновляйте их версии
- перед считыванием с дискет информации, записанной на других компьютерах, всегда проверяйте эти дискеты на наличие вирусов, запуская антивирусные программы своего компьютера
- при переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами
- периодически проверяйте на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив ОС с защищенной от записи системной дискеты
- всегда защищайте свои дискеты от записи при работе на других компьютерах, если на них не будет производится запись информации
- обязательно делайте архивные копии на дискетах ценной для вас информации
- не оставляйте в кармане дисковода А дискеты при включении или перезагрузки ОС, чтобы исключить заражение компьютера загрузочными вирусами

◆ используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей

◆ для обеспечения большей безопасности применения Aidstest и Doctor Web необходимо сочетать с повседневным использованием ревизора диска Adinf.

ЗАКЛЮЧЕНИЕ

Итак, можно привести массу фактов, свидетельствующих о том, что угроза информационному ресурсу возрастает с каждым днем, подвергая в панику ответственных лиц в банках, на предприятиях и в компаниях во всем мире. И угроза эта исходит от компьютерных вирусов, которые искажают или уничтожают жизненно важную, ценную информацию, что может привести не только к финансовым потерям, но и к человеческим жертвам.

Компьютерный вирус – специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера.

В настоящее время известно более 5000 программных вирусов, число которых непрерывно растет. Известны случаи, когда создавались учебные пособия, помогающие в написании вирусов.

Основные виды вирусов: загрузочные, файловые, файлово-загрузочные. Наиболее опасный вид вирусов – полиморфные.

Причины появления и распространения вирусов скрыты с одной стороны в психологии человека, с другой стороны – с отсутствием средств защиты у ОС.

Основные пути проникновения вирусов – съемные диски и компьютерные сети. Чтобы этого не случилось, соблюдайте меры по защите. Также для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, называемых антивирусными. Если вы все же обнаружили в компьютере вирус, то по традиционному подходу лучше позвать профессионала, чтобы тот дальше разобрался.

Но некоторые свойства вирусов озадачивают даже специалистов. Ещё совсем недавно трудно было себе представить, что вирус может пережить холодную перегрузку или распространиться через файлы документов. В таких условиях нельзя не придавать значение хотя бы начальному антивирусному образованию пользователей. При всей серьезности проблемы ни один вирус не способен принести столько вреда, сколько побелевший пользователь с дрожащими руками!

Итак, **здоровье ваших компьютеров, сохранность ваших данных – в ваших руках!**

Библиографический список

1. Информатика: Учебник / под ред. Проф. Н. В Макаровой. – М.: Финансы и статистика, 1997.
2. Энциклопедия тайн и сенсаций / Подгот. Текста Ю. Н. Петрова. – Мн.: Литература, 1996.
3. Безруков Н. Н. Компьютерные вирусы. – М.: Наука, 1991.
4. Мостовой Д. Ю. Современные технологии борьбы с вирусами // Мир ПК. -№8. –1993.