КОМПЬЮТЕРНЫЕ ВИРУСЫ

Д.Ю.Волков [1],Крошинская [2] Л.И.

[1] - студент 1 курса, экономико-правового факультета, 1 группы, Белорусского института правоведения

[2] – научный руководитель, доцент кафедры экономико-математиматических дисциплин и информатики Белорусского института правоведения, Минск, 220004 ,ул.Короля 3 (8017) 211-01-58 e-mail:bip@telecom.by

Анатация: В данном докладе даётся общая характеристика компьютерных вирусов, а также описание некоторых антивирусных программ.

Ключевые слова: Компьютерный вирус, антивирусная программа, программы ревизоры, иммунизаторы.

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять нежелательные различные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а, скажем, при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает так же, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Несмотря на широкую распространенность антивирусных программ, предназначенных для борьбы с вирусами, в среднем в месяц появляется около 300 новых разновидностей. Естественно, что вирусы появляются не самостоятельно, а их создают кракеры. Количество вирусов увеличивается с каждым годом:

1990 год – 500 вирусов
1992 год – 1500 вирусов
1994 год – 4000 вирусов
1996 год – 8000 вирусов
1998 год – более 14000 вирусов
2001 год – более 40000 вирусов.

Различные вирусы выполняют различные действия:

- выводят на экран мешающие текстовые сообщения (поздравления, политические лозунги, рекламу и т.д.);
- создают звуковые эффекты (проигрывают гимн, гамму или популярную мелодию);
- создают видео эффекты (переворачивают или сдвигают экран, вызывают опадание букв в тексте, выводят на экран рисунки и т.д.);
- замедляют работу ЭВМ, постепенно уменьшают объем свободной оперативной памяти;
- вызывают отказ отдельных устройств, зависание или перезагрузку компьютера и крах работы всей ЭВМ;
- имитируют повторяющиеся ошибки работы операционной системы (например, с целью заключения договора на гарантированное обслуживание ЭВМ);
- форматируют жесткий диск, стирают BIOS, стирают секторы на диске, уничтожают или искажают данные, стирают антивирусные программы;
- осуществляют научный, технический, промышленный или финансовый шпионаж;

- выводят из строя системы защиты информации, дают злоумышленникам тайный доступ к вычислительной машине;
- делают незаконные отчисления с каждой финансовой операции и т.д.

Основные симптомы вирусного заражения следующие:

- замедление работы некоторых программ;
- увеличение размеров файлов (особенно выполняемых);
- появление не существующих ранее «странных» файлов;
- уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы);
- появление сбоев в работе операционной системы;
- запись информации на диски в моменты времени, когда этого не должно происходить;
- прекращение работы или неправильная работа ранее нормально функционирующих программ.

Таким образом, если не предпринимать мер по защите от вируса, то последствия заражения компьютера могут быть очень серьезными.

Каждая конкретная разновидность вируса может заражать только один или два типа файлов. Чаще всего встречаются вирусы, заражающие исполнимые файлы. Некоторые вирусы заражают и файлы, и загрузочные области дисков. Вирусы, заражающие драйверы устройств, встречаются крайне редко, обычно такие вирусы умеют заражать и исполнимые файлы.

Существует большое число различных классификаций вирусов. Рассмотрим основные виды вирусов.

По среде обитания они делятся на сетевые, файловые, загрузочные и файлово-загрузочные.

По способу заражения – на резидентные и нерезидентные вирусы.

По степени опасности – не неопасные, опасные и очень опасные вирусы.

По особенности алгоритма – на вирусы-компаньоны, паразитические вирусы, вирусы-черви, невидимки, полиморфные вирусы, макро-вирусы, троянские программы.

Сетевые вирусы распространяются по различным компьютерным сетям (пример — вирус Melissa).

Файловые вирусы. Инфицируют исполняемые файлы компьютера, имеющие расширение COM, EXE. К этому же классу относятся и макро вирусы, написанные с помощью макрокоманд. Они заражают неисполняемые файлы (например, в текстовом редакторе или в электронных таблицах)

Загрузочные вирусы внедряются в загрузочный сектор диска (BOOT-сектор) или в сектор, содержащий программу загрузки диска (Master Boot Record – MBR).

Загрузочно-файловые вирусы способны заражать и загрузочные сектора и файлы.

Резидентные вирусы оставляют в оперативной памяти компьютера свою резидентную часть, которая затем перехватывает обращения неинфицированных программ к операционной системе, и внедряются в них. Свои действия и заражение других файлов, резидентные вирусы могут выполнять многократно.

Нерезидентные вирусы не заражают оперативную память компьютера и проявляют свою активность лишь однократно при запуске инфицированной программы.

Действия вирусов могут быть *не опасными*, например, на экране может быть сообщение и далее никаких действий происходить не будет.

Значительно *опаснее* последствия действия вируса, который уничтожает часть файлов на диске.

Очень опасные вирусы самостоятельно форматируют жесткий диск и этим уничтожают всю имеющуюся информацию. Примером очень опасного вируса может служить вирус CIH (Чернобыль), активизирующийся 26 числа и способный уничтожать данные на жестком диске и в BIOS.

Компаньон вирусы – это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE-файлов новые файлы-спутники (дубликаты), имеющие то же самое имя, но с расширением COM. Например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет одноименный EXE-файл. При запуске такого

файла DOS первым обнаружит и выполнит COM-файл, т.е. вирус, который затем запустит и EXE-файл.

Паразитические вирусы при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу относятся все вирусы, которые не являются «червями» или «компаньонами».

Вирусы-черви распространяются в компьютерной сети и, так же как и компаньон – вирусы, не изменяют файлы или секторы на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Черви уменьшают пропускную способность сети, замедляют работу серверов.

В конце 80-х годов сетевой вирус «Червь Морриса» парализовал несколько глобальных сетей в США.

Вирусы-невидимки используют некоторый набор средств для маскировки своего присутствия в ЭВМ. Эти вирусы трудно обнаружить, так как они перехватывают обращения операционной системы к пораженным файлам или секторам дисков «подставляют» незараженные участки файлов.

Полиморфные вирусы – это вирусы, которые шифруют собственное тело различными способами. Эти вирусы достаточно трудно обнаружить, так как их копии практически не содержат полностью совпадающих участков кода. Это достигается тем, что в программы вирусов добавляются пустые команды, которые не изменяют алгоритм работы вируса, но затрудняют их выявление.

Макро-вирусы используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы и электронные таблицы.) В настоящее время широко распространяются макро-вирусы, заражающие документы Word и Excel.

Троянская программа маскируется под полезную или интересную программу, выполняя, во время своего функционирования еще и разрушительную работу, или собирает на компьютере информацию, не подлежащую разглашению. В отличие от вирусов троянские программы не обладают свойством самовоспроизводства.

Троянская программа маскируется, как правило, под коммерческий продукт. Ее другое название «троянский конь».

Монолитный вирус представляет собой единый блок, который можно обнаружить после инфицирования.

Программа *распределенного вируса* разделена на части. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать вирус. Таким образом, вирус почти все время находится в распределенном состоянии, и лишь на короткое время собирается в единое целое.

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

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

*копирование информации - создание копий файлов и системных областей дисков;

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

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их 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, заражен-

ные 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 какомлибо 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". Программа Scan фирмы McAfee Associates и Aidstest Д.Н.Лозинского позволяют обнаруживать около 1000 вирусов, но всего их более пяти тысяч! Некоторые программы-детекторы, например Norton AntiVirus или AVSP фирмы "Диалог-МГУ", могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам. Тем не менее, невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Многие программы-детекторы (в том числе и Aidstest) 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, Aidstest и другие 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.

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.

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.

Следует заметить, что многие программы-ревизоры не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Но некоторые программы-ревизоры, например ADinf фирмы "Диалог-Наука", все же умеют

делать это, не используя вызовы DOS для чтения диска 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.

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.

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.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Опишу структуру этой обороны.

Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На переднем крае обороны находятся программы-фильтры. Эти программы могут первыми сообщить о работе вируса и предотвратить заражение программ и дисков.

Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры.

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

В "стратегическом резерве" находятся архивные копии информации. Это позволяет восстановить информацию при её повреждении.

Это неформальное описание позволяет лучше понять методику применения антивирусных средств.

Литература:

1.Основы экономической информатики под ред. А.Н. Морозевича, Минск, БГЭУ, 2001г.

2.Компьютерная газета» №5-9, 2000г.