УДК: 51:51-3

Тултуков Б.Т., Иязбекова Р.А.
Ысык-Кульский институт им. Ж.Алышбаева

БОРЬБА С КОМПЬЮТЕРНЫМИ ВИРУСАМИ – БОРЬБА ЧЕЛОВЕКА С ЧЕЛОВЕЧЕСКИМ ЖЕ РАЗУМОМ

В раскрывается актуальность данного вопроса на сегодняшний день и статье рассмотрены проблемы компьютерных вирусов, их виды и особенности.

На горе лежит дискета,
У неё запорчен бут:
Через дырочку в конверте
Её вирусы грызут.
(Из народного фольклора)

Компьютерные вирусы. Что это такое и как с этим бороться? На эту тему написаны десятки книг и сотни статей. Борьбой с компьютерными вирусами профессионально занимаются сотни (или тысячи) специалистов в десятках (а может быть, сотнях) компаний. Казалось бы, тема эта не настолько сложна и актуальна, чтобы быть объектом такого пристального внимания. Однако это не так. Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Известны случаи, когда вирусы блокировали работу организаций и предприятий. При этом следует иметь в виду, что антивирусные программы не дают полной гарантии защиты от вирусов. Примерно так же плохо обстоят дела на другой стороне тандема - «человек-компьютер». Как пользователи, так и профессионалы-программисты часто не имеют даже навыков «самообороны», а их представления о вирусе порой являются настолько поверхностными, что лучше бы их и не было.

Все это и послужило толчком к тому, чтобы собрать этот материал, который хоть немного даст представление о компьютерных вирусах, борьбе с ними, их анализ и разработку методов обнаружения и лечения.

К основным техническим феноменам 20-го века относятся, на наш взгляд, появление человека в космосе, утилизация атомной энергии вещества, грандиозный прогресс систем связи и передачи информации и, конечно же, ошеломляющее развитие микро- и макрокомпьютеров. И как скоро появляется упоминание о феномене компьютеров, так тут же возникает еще один феномен конца нашего столетия - феномен компьютерных вирусов.

Быть может, многим покажется смешным или легкомысленным то, что факт возникновения компьютерных вирусов поставлен в один ряд с исследованиями космоса, атомного ядра и развитием электроники. Возможно, что мы не правы в своих рассуждениях, однако используем возможность объясниться.

Во-первых, компьютерные вирусы - это серьезная и довольно заметная проблема, возникновение которой никто не ожидал. Во-вторых, компьютерные вирусы - это первая, вполне удачная попытка создать жизнь. Попытка удачная, но нельзя сказать, что полезная - современные компьютерные «микроорганизмы» более всего напоминают насекомых-вредителей, приносящих только проблемы и неприятности.

Но все-таки - жизнь, поскольку компьютерным вирусам присущи все атрибуты живого - способность к размножению, приспособляемость к среде, движению и т.д. (естественно, только в пределах компьютеров - так же, как все вышесказанное верно для биологических вирусов в пределах клеток организма). Более того, существуют «двуполые» вирусы (см. вирус RMNS), а примером «многоклеточности» могут служить, например, макровирусы, состоящие из нескольких независимых макросов.

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. Они придумывают новый вирус - а нам с ним разбираться. Итак, появление компьютерных вирусов - один из наиболее интересных моментов в истории технического прогресса 20-го века. Вопрос об определении понятия «компьютерный вирус» будет стоять на первом месте. Объяснений, что такое компьютерный вирус, можно привести несколько. Во-первых, вирусы не возникают сами собой - их создают очень злые и нехорошие программисты-хакеры и рассылают затем по сети передачи данных или подкидывают на компьютеры знакомых. Вирус не может сам собой появиться на Вашем компьютере - либо его подсунули на дискетах или

даже на компакт-диске, либо Вы его случайно скачали из компьютерной сети передачи данных, либо вирус жил у Вас в компьютере с самого начала.

Официально считается, что термин «компьютерный вирус» появился в 1984 г. на 7-й конференции по безопасности информации, проходившей в США, что его впервые употребил сотрудник Лехайского университета (США) Ф.Коэн. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла, однако строгого определения, что же такое компьютерный вирус, так и не дано, несмотря на то, что попытки дать такое определение предпринимались неоднократно.

Основная трудность, возникающая при попытках дать строгое определение вируса, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и проч.) либо присущи другим программам, которые никоим образом вирусами не являются, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения). Таким образом, первой из причин, не позволяющих дать точное определение вирусу, является невозможность однозначно выделить отличительные признаки, которые соответствовали бы только вирусам. Второй же трудностью, возникающей при формулировке определения компьютерного вируса является то, что данное определение должно быть привязано к конкретной операционной системе, в которой этот вирус распространяется. Например, теоретически могут существовать операционные системы, в которых наличие вируса просто невозможно. Таким примером может служить система, где запрещено создавать и изменять области выполняемого кода, т.е. запрещено изменять объекты, которые либо уже выполняются, либо могут выполняться системой при каких-либо условиях.

ОБЯЗАТЕЛЬНЫМ (НЕОБХОДИМЫМ) СВОЙСТВОМ КОМПЬЮТЕРНОГО ВИРУСА является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Мнений по поводу даты рождения первого компьютерного вируса очень много. Нам доподлинно известно только одно: на машине Беббиджа его не было, а на Univac 1108 и IBM-360/370 они уже были («Pervading Animal» и «Christmas tree»). Таким образом, первый вирус появился где-то в самом начале 70-х или даже в конце 60-х годов, хотя «вирусом» его никто еще не называл.

Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- операционная система (ОС);
- особенности алгоритма работы;
- деструктивные возможности.

По среде обитания вирусы можно разделить на:

- файловые;
- загрузочные;
- макро;
- сетевые.

Файловые вирусы либо различными способами 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 винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макровирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

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 (вернее, ОС, объекты которой подвержены заражению) является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких OS - DOS, Windows, Win95/NT, OS/2 и т.д. Макровирусы заражают файлы форматов Word, Excel, Office97. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Среди ОСОБЕННОСТЕЙ АЛГОРИТМА РАБОТЫ вирусов выделяются следующие пункты:

- резидентность;
- использование стелс-алгоритмов;
- самошифрование и полиморфичность;
- использование нестандартных приемов.

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. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными. Резидентными можно считать 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 ОС 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. Один из первых файловых стелс-вирусов — вирус «Frodo», первый загрузочный стелс-вирус — «Brain».

САМОШИФРОВАНИЕ и ПОЛИМОРФИЧНОСТЬ используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик-вирусы (polymorphic) - это достаточно труднообнаруживаемые 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 ОС (как это делает вирус «ЗАРАЗА»), защитить от обнаружения свою резидентную копию (вирусы «TPVO», «Trout2»), затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т.д.

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 с графическими, звуковыми и пр. эффектами;
- 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, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некоторых типов винчестеров.

А что же будет дальше? И как долго вирусы будут нас беспокоить? - вопросы, которые в той или иной мере беспокоят практически всех пользователей.

Чего ожидать от компьютерного вируса в последующие годы? Скорее всего, основными проблемами останутся: 1) полиморфик-DOS-вирусы, к которым добавятся проблемы

полиморфизма в макровирусах и вирусах для Windows и OS/2; 2) макровирусы, которые будут находить все новые и новые приемы заражения и скрытия своего кода в системе; 3) сетевые вирусы, использующие для своего распространения протоколы и команды компьютерных сетей.

Сетевые вирусы находятся пока только на самой ранней стадии - вирусы делают первые робкие попытки самостоятельно распространять свой код по MS Mail, пользуясь ftp, однако все еще впереди.

Не исключено, что появятся и другие проблемы, которые принесут немало неприятностей пользователям и достаточное количество неурочной работы разработчикам антивирусных программ, вирусописателей. Основная питательная среда для массового распространения вируса в ЭВМ, на наш взгляд, обязана содержать следующие необходимые компоненты:

- незащищенность операционной системы (ОС);
- наличие разнообразной и довольно полной документации по ОС;
- широкое распространение этой ОС.

Если в операционной системе присутствуют элементы защиты информации, как это сделано практически во всех ОС, вирусу будет крайне трудно поразить объекты своего нападения, так как для этого потребуется (как минимум) взломать систему паролей и привилегий. В результате работа, необходимая для написания вируса, окажется по силам только профессионалам высокого уровня (вирус Морриса для VAX - пример этому). А у профессионалов, на наш взгляд, уровень порядочности все-таки намного выше, чем в среде потребителей их продукции, и, следовательно, число созданных и запущенных в большую жизнь вирусов еще более сократится.

Приведенным выше трем условиям «расцвета» компьютерных вирусов удовлетворяют сразу несколько OS (включая редакторы), производимых фирмой Microsoft (DOS, Windows, Win95/NT и Word, Excel, Office97), что дает благодатную почву для существования самых разнообразных файловых и макровирусов. Удовлетворяют приведенным условиям также и стандарты разбиения жестких дисков. Результат - разнообразные варианты загрузочных вирусов, поражающих систему в момент ее загрузки.

Исходя из вышесказанного, можно сделать единственный вывод: вирусы успешно внедрились в повседневную компьютерную жизнь и покидать ее в обозримом будущем не собираются.

Однако мы смотрим в будущее с оптимизмом: все проблемы, когда-либо вставшие в истории развития вирусов, были довольно успешно решены. Скорее всего, так же успешно будут решаться и будущие проблемы, пока еще только витающие идеями в воспаленном разуме.

Литература

1. Симонович С., Евсеев Г. Компьютер и уход за ним. Практическое руководство. – Москва: АТС Пресс, 2005.
2. Зозуля Ю., Пришивалко Н. Трюки и эффекты Windows XP –СПб.: ПИТЕР, 2006.
3. Справка Adif.
4. http://www.apl.ru/isvwsolaris.htm.
5. http://www.act.ru/av/Solomon/DrSolom_report.asp.