Компьютерные вирусы-92: от плохого к худшему, или Есть ли вирусы на Марсе?

На горе лежит дискета,
У нее запорчен бут.
Через дырочку в конверте
Ее вирусы грызут.

Тяжела и неказиста
Жизнь простого программиста.
Народный фольклор

Замысел этой статьи родился на традиционной (как оказалось) конференции по системному программированию, проходившей в Абрау-Дюрсо. Собиравшаяся по утрам публика, в ожидании когда нагреются камни на осеннем пляже, развлекала себя докладами, сообщениями и дискуссиями на программистские и околопрограммистские (т.е. наиболее злободневные) темы. Пользователи ЕС-10xx, СМ, PDP-11, VAX, IBM PC рассуждали о программировании реляционных баз данных, спеллчекеров, параллельных систем, мультимедиа и о многом другом. Удалось и нам (Дмитрию Мостовому, Юрию Павловичу Лященко и мне) сказать свое слово в защиту темы компьютерных вирусов, которая, честно говоря, мало волнует пользователей не "MS-DOS на IBM PC".

На мой взгляд, тема вирусов стоит несколько отдельно от всех остальных программистских задач. Практически все проблемы, решаемые при помощи вычислительной техники, являются продолжением целенаправленной борьбы человека с окружающей его природой. Природа ставит человеку длинное нелинейное дифференциальное уравнение в трехмерном пространстве — человек набивает компьютер процессорами, памятью, обвешивает пыльными проводами, много курит и в итоге решает это уравнение (или пребывает в состоянии уверенности, что он его решил). Природа дает человеку кусок провода с вполне определенными характеристиками — человек придумывает алгоритмы передачи как можно большего объема информации по этому проводу, терзает его модуляциями, сжимает байты в биты и терпеливо ждет сверхпроводимости при комнатной температуре. Природа (в лице фирмы IBM) дает человеку 640 Кбайт+12 МГц — и человек не спит ночами, опять много курит*, оптимизируя коды очередной базы данных. И так далее.

А вот борьба с компьютерными вирусами является борьбой человека с человеческим же разумом (тоже в некотором смысле проявлением природных сил, хотя на этот счет имеется более одного мнения). Это — борьба умов, поскольку задачи, стоящие перед вирусологами, ставят тоже люди. Они придумывают новый вирус — а нам с ним разбираться. Затем они придумывают вирус, в котором разобраться очень тяжело — но мы и с ним разбираемся. И сейчас, наверняка, сидит где-то за компьютером парень, который не глупее меня, и мучается над очередным монстром, в котором мне придется разбираться целую неделю, а потом еще одну неделю отлаживать алгоритм "лечилки" против этого вируса.

Но это все околофилософские вопросы, а уже давно пора переходить к конкретным. Итак...

Где водятся вирусы? И как долго они будут нас беспокоить?

Основная питательная среда для массового распространения вируса в ЭВМ, на мой взгляд, состоит из следующих необходимых компонентов:

* Сам автор статьи не курит. (Прим.редакции.)

- незащищенность операционной системы (ОС);
- наличие разнообразной и довольно полной документации по операционной системе и "железу";
- широкое распространение этой ОС и этого "железа".

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 среди профессионалов, на мой взгляд, уровень порядочности все-таки немного выше, чем у потребителей их продукции, и, следовательно, число созданных и запущенных в большую жизнь вирусов сокращается.

Еще для массового производства вирусов необходимо и достаточное количество информации о среде их обитания. Какой процент от общего числа системных программистов, работающих на мини-ЭВМ в операционках UNIX, VMS и т.д., знает систему управления процессами в оперативной памяти, полные форматы выполняемых файлов и загрузочных записей на диске (то есть информацию, крайне необходимую для создания вируса)? И, следовательно, какой процент от их числа в состоянии вырастить настоящего полноценного зверя?

Ну а по поводу широкого распространения ОС как необходимого условия для вирусного нашествия и говорить надоело: на 1000 программистов приходится 100, способных написать вирус, на эту сотню приходится один, который эту идею претворит в жизнь. Теперь полученную пропорцию умножаем на число тысяч программистов — и получаем результат: 1500 или даже 2000 полностью IBM-совместимых вирусов. Десятки (или сотни?) вирусов для Apple Macintosh.

Вот и получается, что вирус в IBM PC — явление не случайное, а подчиненное неким законам и правилам, а, следовательно, ответ на вопрос, вынесенный в заголовок, будет следующим: если на Марсе есть MS-DOS на IBM PC, то там обязаны присутствовать и вирусы.

Для того чтобы прикинуть продолжительность нашествия компьютерных вирусов, надо оценить время одновременного сосуществования приведенных выше необходимых условий.

Довольно очевидно, что в обозримом будущем фирмы IBM и Apple не собираются уступать массовый рынок своим конкурентам (на радость Apple- и IBM-программистам), даже если для этого им придется объединить усилия. Не представляется возможным и усечение потока информации по наиболее распространенным системам, так как это ударит по числу приложений для них, а, следовательно, и по их продаваемости.

Остается одно: защита ОС. Когда это произойдет? Когда на столы секретарш, бухгалтеров, брокеров и т.д., и т.п. придут ОС с разграничением доступа к ресурсам системы? Вопрос для меня сложный, и пусть он прогнозируется не мною. Допустим, на это потребуется *5* лет (для стран отдельно построенного социализма — плюс еще *5* лет). Стало быть, время вирусного нашествия ограничивается пятью или десятью годами. Остается только ждать.

История компьютерных вирусов: от древности до наших дней

Мнений по поводу того, когда появился первый компьютерный вирус, очень много. Мне доподлинно известно только одно: на машине Бебиджа его не было, а на IBM-360/370 уже был (вирус "Christmas tree").

На этом разговор о вымерших ископаемых предлагаю считать завершенным. Поговорим о новейшей истории: от "Венского", "Падающих букв" и далее. Те, кто начал работать на IBM PC аж *5* или *8* лет назад, еще не забыли повальную эпидемию этих вирусов. Буквы сыпались по экранам, а толпы пользователей неслись к специалистам по ремонту дисплеев (сейчас все наоборот: винчестер сдох от старости, а валят на неизвестный передовой науке вирус). Затем компьютер заиграл чужеземный гимн "Yankee Doodle", но чинить динамики уже никто не бросился — очень быстро разобрались, что это — вирус, да не один, а целый десяток.

Так вирусы начали заражать файлы. Скачущий по экрану шарик ознаменовал победу вируса и над Boot-сектором (см. эпиграф). Все это очень не нравилось пользователям IBM PC — и появились противоядия. Первым попавшимся мне антивирусом был Anti-Kot: это легендарный Олег Котик выпустил в свет первые версии своей программы, которая уничтожала целых 4 (четыре!) вируса. Кстати, всем, кто до сих пор сохранил копию этого антивируса, предлагаю немедленно ее стереть (да простит меня Олег Котик!) как программу вредную и ничего, кроме траты лишних нервов и ненужных телефонных звонков, не приносящую. К сожалению, Anti-Kot определяет "Иерусалимский" вирус по комбинации "MsDos" в конце файла, а какой-то другой антивирус эти самые буквы аккуратно прицепляет ко всем файлам с расширением COM или EXE.

Время шло, вирусы плодились. Все они были чем-то похожи друг на друга, лезли в память, цеплялись к файлам и секторам, периодически грохали файлы, дискеты и винчестеры. Одним из первых откровений стал вирус "V-4096" — первый из известных мне файловых вирусов-невидимок. Этот вирус перехватывал int 21h и, при обращении через DOS к зараженным файлам, изменял информацию таким образом, что файл появлялся перед пользователем в незараженном виде. Но это была только надстройка вируса над MS-DOS. Не прошло и года, как электронные тараканы полезли внутрь DOS (вирус-невидимка "V-512"). Идея невидимости продолжала приносить свои плоды и далее: летом 1991 года пронесся, кося компьютеры как бубонная чума, вирус "Driver-1024". "Да-а-а!"— сказали все, кто в нем копался.

Но бороться с невидимками было довольно просто: почистил RAM — и будь спокоен, ищи гада и лечи его на здоровье. Побольше хлопот доставляли самошиф-

рующиеся вирусы. Ведь для их идентификации и удаления приходилось писать специальные подпрограммы, отлаживать их. Но на это никто тогда не обращал внимания, пока... Пока не появились вирусы нового поколения, те, что на Западе называют polymorphic-вирусы. Эти вирусы используют другой подход к невидимости: они шифруются (в большинстве случаев), а в расшифровщике используют команды, которые могут не повторяться при заражении различных файлов. Простейшим примером этого является следующий расшифровщик (пока еще не polymorphic!):

```
    mov reg_1, count        ; reg_1, reg_2, reg_3
mov reg_2, key              ; выбираются из
mov reg_3, _offset          ; AX,BX,CX,DX,SI,DI,BP
                            ; count, key, _offset
                            ; также могут меняться
_loop:
    xxx byte ptr [reg_3], reg_2 ; xor, add или sub
    dec reg_1
    jxx _loop               ; ja или jnc
    ; а дальше следуют зашифрованные коды и данные
```

Похожие алгоритмы используются в вирусах "Word", "Phoenix" и многих других. В результате НИ ОДИН байт кода самого вируса и его расшифровщика не является постоянным при заражении различных файлов. Но и это не составляет большой проблемы, так как остаются постоянные биты, по которым и можно зацепиться за вирус и начать его расшифровку (можно, конечно, расшифровывать все файлы подряд, даже те, которые вируса не содержат, но это отразится на скорости работы антивирусной программы).

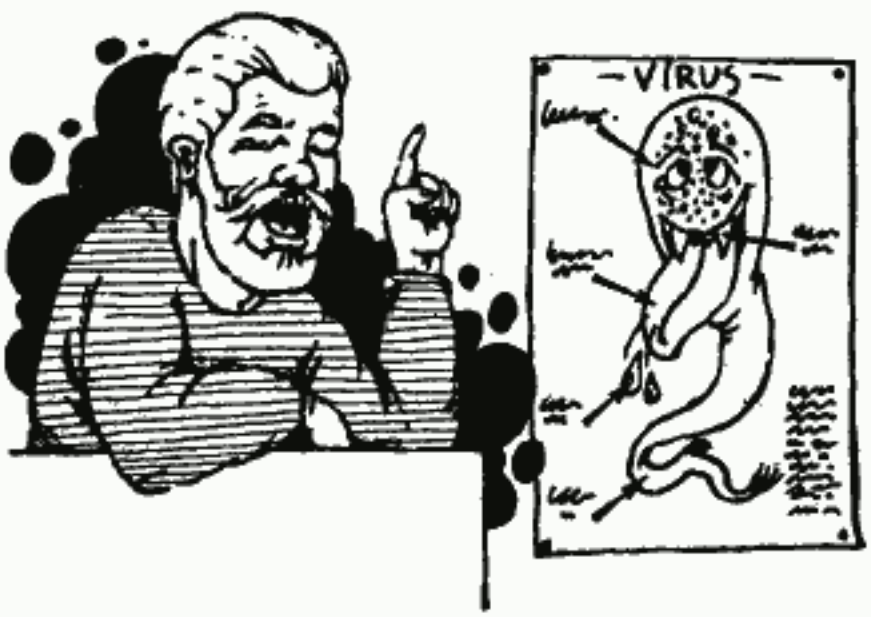
Следующий шаг компьютерных мичуринцев был в селекции мутантов, в которых нет ни одного постоянного БИТА информации. Это было достигнуто довольно легко: приведенные выше инструкции (или их эквиваленты) переставлялись местами от заражения к заражению, разбавлялись ничего не меняющими командами типа NOP, STI, CLI, STC, CLC, DEC неиспользуемый регистр, XCHG неиспользуемые регистры и т.д. В результате в начале файла, зараженного подобным вирусом, идет набор бессмысленных, на первый взгляд, инструкций, причем некоторые комбинации, которые вполне работоспособны, не берутся фирменными дизассемблерами (например, сочетание CS:CS: или CS:NOP). И среди этой "каши" из команд и данных изредка проскальзывают MOV, XOR, LOOP, JMP — инструкции, которые действительно являются "рабочими". К подобным вирусам можно отнести "Starship", "Amoeba", "Mutant", причем последний вирус, видимо, отечественного происхождения (умеем, если захотим!). Но и с этими уродами справиться не составило труда. Это было достигнуто двумя методами (или их комбинацией):

1) в каждом конкретном вирусе алгоритм шифровки не менялся, поэтому можно извлечь ключ шифровки прямо из шифрованного участка в файле, если это не получается, значит файл не заражен;
2) сканирование начала файла: отбрасывание мусора и поиск действительно "рабочих" команд.

В результате скорость обнаружения этих polymorphic-вирусов совсем незначительно отразилась на общем быстродействии антивирусов. Но дальше — больше. Наступил год 1992-й. Он был ознаменован новой победой селекционеров: на свободу выполз вирус "Pogue" (другое название — "MtE"). Это животное использует чрезвычайно сложный polymorphic-алгоритм, в результате работы которого в расшифровщике вируса могут встретиться операции SUB, ADD, XOR, ROR, ROL в произвольном количестве и порядке. Загрузка и изменение ключей и других параметров шифровки производятся также произвольным набором операций, в котором могут встретиться более половины инструкций процессора 8086 (ADD, SUB, TEST, XOR, OR, SHR, SHL, ROR, MOV, XCHG, JNZ, PUSH, POP...) со всеми возможными режимами адресации. И самое смешное в том, что эта штука работает, причем работает без ошибок!

Вот так. Задача обнаружения вируса значительно усложнилась. Как теперь отличить зараженный файл от незараженного? Ведь и в зараженных, и в незараженных файлах могут встретиться самые разнообразные инструкции в самом разнообразном порядке. Не говорю уже о том, что надо бы вытащить из расшифровщика алгоритм шифровки, его ключи и расшифровать тело вируса.

Решал я эту проблему около недели, копался в листингах, залез в сотню зараженных файлов. В результате за 3 дня был написан эмулятор (довольно примитивный) процессора 8086, который эмулирует (не трассирует!) работу файла, и, если файл заражен вирусом, выдает его (вируса) расшифрованное тело. В большинстве случаев незараженные файлы отметаются эмулятором сходу. Но если файл заражен или "похож" на зараженный, то антивирус "приседает" в среднем на 1 секунду на каждый "подозрительный" файл (справедливо для AT-286/16). Умножим эту цифру на число проверяемых на винчестере файлов... Итого: вместо 1 минуты на 32-Мбайтный винчестер в скором будущем потребуется минут 10. Что будет, когда таких вирусов появится два, три,... а потом много? Если честно, то сейчас их уже 4, причем один из



них (вирус "Bomber") использует несколько большее число команд при выработке своего начала. Так что скоро могут появиться таблички: "С 9:00 до 13:00 компьютер на антивирусной профилактике".

Плохо? Плохо. Но все вышесказанное — мышиная возня по сравнению с дальнейшим развитием событий: вирус "Pogue" был расхакан, затем из него был извлечен алгоритм генерации расшифровщиков (MtE-алгоритм), этот алгоритм был откомпилирован в OBJ-файл, снабжен необходимой документацией (довольно полной) и помещен на BBS. БИ-БИ-ЭС! Вы не ослышались! Лежит теперь этот аккуратненький ZIP, в котором исходники, OBJ-файлы, примеры и подробные объяснения, как вызывать из любого вируса MtE-алгоритм, как линковаться и т.д. И сейчас любой козел может превратить самый безобидный вирус в жуткого мутанта! И не исключено, что, если не будут разработаны алгоритмы быстрого поиска MtE, время сканирования винчестера будет измеряться ЧАСАМИ, а не минутами! Таблички сменятся на: "С 1-го по 15-е число ежемесячно компьютер находится на профилактике".

Вот так. Тенденция развития событий — от плохого к наихудшему. Что ожидать дальше? Что готовит нам год 1993-й???

Тенденции развития компьютерной ассенизации

Жизнь принесла десяток типов антивирусных программ (фаги, полифаги, детекторы, сторожа, иммунизаторы и т.д.) и несколько сотен антивирусных разработок. На мой взгляд, практически все они потеряли актуальность: сторожа (или блокировщики) из-за того, что появилось много вирусов, которые либо встраиваются в DOS, и их вызовы невозможно отличить от "родного" вызова DOS, либо используются принципиально новые идеи, например, заражение файлов только при их копировании. Иммунизаторы же бессильны против вирусов-невидимок, к тому же они могут испортить иммунизируемые файлы, и т.д.

Теряют актуальность и наиболее популярные антивирусы — полифаги, то есть программы, обнаруживающие и удаляющие массу вирусов, конкретных и известных автору (авторам) данного антивируса. Да-да! Полифаги становятся неактуальными! В том числе и старые версии программы -V.EXE.

При современном положении дел, когда число новых вирусов измеряется десятками (а иногда и сотней) экземпляров в месяц, подобные полифаги не могут обеспечить надежной защиты. Просто не хватает времени, чтобы подключать все новинки в антивирусную базу. И довольно часто большое число вирусов стоит в очереди на обработку, а зараженные пользователи либо ждут и мучаются, либо ищут другие способы избавления от заразы (например, путем форматирования всего, что форматируется). Тем более смешна ситуация, когда пользователи антивируса прошлого года изготовления живут в уверенности абсолютной защиты их любимых "писишек" от злобных пришельцев. Как бы не так, господа! Версию антивируса следует менять как можно чаще, а антивирусы, изготовленные в прошлом году, следует пустить под нож ради экономии места на диске.

Чем же следует пользоваться!

Остались программы проверки целостности файлов и секторов на дисках. Наиболее симпатичная для меня разработка в этой области — система ADINF Дмитрия Мостового. Она показалась мне настолько интересной, что часть ее функций я решил вставить в новую версию -V.EXE.

А что же делать, если программа ADINF кричит, что все файлы увеличились в размере на 2 Кбайта? Вот тут следует применять полифаги второго поколения, разработкой одного из которых моя команда занималась более *5* месяцев. Отличительная особенность этой системы состоит в том, что база данных, по которой антивирус определяет и удаляет вирусы, является ОТКРЫТОЙ. То есть квалифицированный пользователь (если он, конечно, во-первых, в состоянии самостоятельно разобраться в алгоритме работы вируса, а, во-вторых, приобретет редактор базы) может быстро и самостоятельно написать обнаруживалку и лечилку на новый внезапно появившийся вирус. Тщательно протестировав свое изделие (то есть добавку к основной антивирусной базе), он может положить новую базу на BBS и этим избавить многих других пользователей от многочасовых мучений. В базу данных заложен алгоритм поиска вирусов в файлах и около 20 стандартных методов удаления вирусов (в том числе метод DELETE). Если же метод удаления вируса нестандартный, то оказавшийся неподалеку системщик может написать на языке Си или Ассемблере собственную программу для обнаружения и удаления вируса, откомпилировать ее в OBJ-файл и поместить в базу данных. При старте антивируса этот OBJ будет считан из базы и автоматически слинкован с основным EXE-модулем. Хочу добавить, что база данных, поставляемая с антивирусным комплексом, зашифрована, что практически исключает ее модификацию злоумышленником.

Этим в значительной степени снижается нагрузка на разработчиков антивирусных программ. И теперь больше времени можно потратить на борьбу с новой чумой — вирусами типа polymorphic и другими зверями, которые окажутся не по зубам простому честному пользователю.

Е.Касперский
E-mail: eugene@kaml.npimsu.msk.su
Тел.: (095) 499-15-00