Н. Пухова, А. Фаренбрух

Компьютерные вирусы: диагноз и лечение

Теперь уже практически все знают, что если компьютерный вирус и может причинить вред здоровью человека, то это будет, скажем, легкий обморок после того, как вы узнали, что безвозвратно утрачены несколько мегабайт трудновосстановимой информации. За последние два года наши представления об этом вопросе претерпели значительные изменения. От сильного недоумения при чтении заметок об их появлении за рубежом, до поголовного всезнайства, которое, впрочем, неудивительно — ведь компьютерные вирусы сродни и медицине, и политике, и спорту.

Лавина статей о вирусах заполонила компьютерные журналы. От робкой и осторожной статьи А.А. Чижова [1] (не лишенной некоторых огрехов), до самоуверенной и, мягко выражаясь, некорректной статьи Д. Стефанкова [3], содержащей ряд ошибок и вместе с тем за гораздо менее серьезные недочеты поливающей грязью многих уважаемых авторов.

Вообще чрезвычайно сложно писать статьи на антивирусную тематику, не рассказывая о принципах жизнедеятельности вирусов, а рассказав, не быть уверенным, что не подтолкнешь кого-либо к написанию своего вируса или, что более вероятно, к усовершенствованию чужого.

К сожалению, вредить легче, чем защищать от вреда. В связи с особенностями психологии разработчиков вирусов вспоминается недоумение Д.Н. Лозинского, который не мог себе представить, что кому-то может быть интересно сделать то, что уже ясно, как делать (см. AidsRead.me к AidsTest).

Выделились явные лидеры среди антивирусных программ. Scan и Clean, безусловно, занимают ведущее место среди распространенных у нас западных пакетов этого назначения, затем с большим отрывом следуют Norton AntiVirus и Turbo AntiVirus. Среди советских антивирусных программ лидерами можно назвать AidsTest и Doctor.

Среди программ-детекторов особое положение занимает программа СТРАЖ. Авторам этой статьи довелось тестировать версии 3.0 и 4.20 этого пакета. Основные задачи и идеи системы оказались очень близки нам.

Но несмотря ни на что, основные боевые позиции сохранились за вирусами. С массовым потоком все новых мутаций скоро уже не смогут справиться никакие антивирусные программы, настроенные на конкретные типы вирусов.

Положение может быть исправлено только путем отсекания вирусов от стандартных способов передачи управления (их количество счетно, следовательно, задача не безнадежна).

Существует большое количество различных классификаций вирусов: от поверхностных, описывающих чисто внешние свойства [9, 10, 12], до чрезвычайно детализированных в академическом стиле, предназначенных для точной идентификации любого вируса [8, 13]. Можно достаточно долго обсуждать достоинства той или иной классификации, но гораздо полезнее сосредоточить свое внимание на такой, которая сможет лечь в основу практической реализации.

Классификация вирусов по способам получения управления:

- вирусы начальных загрузчиков — получают управление из программы начального запуска BIOS (Boot сектор на дискетах и MainBoot сектор на жестком диске) или из программы начальной загрузки в MainBoot секторе на жестком диске (Boot сектор жесткого диска);
- вирусы операционной системы — получают управление при начальном запуске одной из частей операционной системы (IO.SYS, MSDOS.SYS, IBMBIO.COM, IBMDOS.COM). Подселение вируса к этим файлам представляет определенные трудности, но исключать их из рассмотрения по крайней мере преждевременно;
- вирусы исполняемых файлов — получают управление при запуске файлов типа *.COM и *.EXE;
- вирусы драйверов устройств — получают управление от конфигуратора системы при обработке файла config.sys (строки типа device= ...);
- вирусы оверлейных файлов — о вирусах данного типа мы знаем только понаслышке, но судя по отсутствию общесистемных стандартов на передачу управления в оверлейных структурах, мы можем встретиться с оверлейным вирусом, настроенным на конкретную инструментальную систему программирования;
- вирусы объектных библиотек — вирусы подобного типа получают управление в результате целой последовательности действий (трансляция, компоновка, запуск программы), после которой тело вируса оказывается тесно переплетено с выполняемой задачей. Передача управления в тело вируса оказывается в столь сильной зависимости от инструментальной среды и способа подключения к библиотеке, что проще говорить о защите объектных библиотек от любых изменений.

Как видно, не все виды передач управления имеют свои стандарты, но грамотно написанный вирус, чтобы получить управление, может рассчитывать только на стандартизованный механизм.

Такая или похожая классификация, конечно, не является изобретением авторов, однако практических реализаций, опирающихся на нее, почти нет.

Опираясь на данную классификацию, мы попытались подготовить свою систему антивирусной защиты и, как нам кажется, не без успеха. Быть может основные принципы и решения, заложенные в нашей системе, могут показаться небезынтересными и читателям PC Magazine/USSR.

Один из основных принципов — *ничто не должно ускользнуть от внимания*. Это означает, что пользователь должен быть проинформирован о любом вмешательстве в исполняемую часть задач и операционной системы. Мы предполагаем, что человек, применяющий нашу программу, имеет минимальную компьютерную грамотность, необходимую для принятия решения о допустимости или недопустимости данного вмешательства. При любых сомнениях в правомочности обнаруженных изменений рекомендуется отказаться от исполнения поврежденной задачи.

Не менее банальный принцип — *минимальные издержки*. Во-первых, в

системе, не подвергшейся нападению вирусов, не должно ощущаться сколько-нибудь заметного снижения быстродействия. Во-вторых, объем резидентной контролирующей части должен быть минимален.

Следующий принцип — *глубина, прозрачность и универсальность.* Система должна охватывать контролем все или большинство интерфейсов передач управления, быть абсолютно незаметной для операционной системы и большинства прикладных программ, а также минимально зависимой от версии операционной системы. Все три перечисленных свойства кажутся взаимоисключающими, однако опыт авторов говорит о существовании компромиссных решений.

Еще один принцип — *"лучше перебдеть, чем недобдеть"*. Под этим принципом мы понимаем принятие мер по пресечению заведомо некорректных способов обхода интерфейсов передач управления. Примером пренебрежения этим принципом может служить популярная программа Д.Лозинского — AIDSTEST. Пользуясь заимствованным из вируса механизмом нахождения "чистых" векторов прерывания, программа "не задумывается" о том, что кто-либо может бороться с этим. Потребовались дополнительные усилия, чтобы избавить AIDSTEST от зацикливания.

И последний принцип — *"диагноз — все, лечение — ничто"*. Лечиться от известных болезней — легко, лечиться от неизвестных болезней может быть уже поздно. Вовремя поставленный диагноз — залог минимальности ваших потерь. Поэтому мы посвятили большую часть своих (отнюдь не избыточных) сил на разработку универсальной диагностической системы, снабдив, однако, последние версии системы достаточно мощной программой восстановления зараженных файлов, охватываемых нашей системой, не вступая в борьбу за сферы влияния с такими "бизонами", как фирма McAfee, и такими "зубрами", как Д.Н.Лозинский: мы занимаемся только своими "пациентами". Мы не хотим умалять важность программ-"фагов". По нашему мнению, в будущем антивирусные системы примут форму комплексов диагностических и "лечащих" средств, причем основной упор будет делаться на диагностику.

Рассмотрим основные возможные подходы к проблеме контроля исполняемых частей задач:

- *самоконтроль.* Задачи строятся таким образом, что при запуске проверяют свою длину, контрольную сумму или отдельные свои критические участки. Этот метод хорош при построении антивирусных программ-"фагов", которым по роду своей деятельности приходится работать в "зоне риска". Однако для общесистемных приложений он неприменим, так как большинство программ обычно разрабатывают без учета вирусной опасности;

- *вырожденный вирус.* Является универсальной разновидностью первого подхода. Система строится в виде вируса, который следит за тем, чтобы никакой другой вирус не поселился на обработанной задаче.

Общими недостатками обоих указанных подходов являются большие издержки на каждый из защищенных файлов, а главное, что контроль проводится в то время, когда возможный вирус уже стартовал. Теоретически возможна разработка вируса, осуществляющего полную свою маскировку во время своей активности. Зародыши такой маскировки уже нашли целый ряд воплощений;

- *программы-ревизоры.* Эти системы с различной степенью тщательности проверяют все (или заданные списком) файлы на изменения. Главным недостатком такого подхода являются большие временные издержки на тщательный контроль файлов, а следовательно, малая частота их использования. Также остается нерешенной проблема маскирующихся вирусов;

- *вирусозащищенная операционная система.* Этот подход позволяет аккуратно проработать все интерфейсы и обеспечить надежную их защиту, однако, не выдерживает критики с экономической точки зрения. Невозможно быстро и оперативно разрабатывать защищенные от вирусов версии операционных систем, не являясь фирмой, для которой этот вид деятельности является основным. Однако фирмы IBM и Microsoft пока не спешат приступить к разработке защищенных от вирусов версий своих операционных систем. Впрочем, быть может, причина этого — понимание того, что к универсальному замку можно легко сделать столь же универсальную отмычку.

Мы попытались взять большинство положительных черт перечисленных выше подходов, сведя, как нам кажется, к минимуму их отрицательные свойства. В основе нашего подхода лежит создание системы "прослоек" между частями операционной системы, основная задача которых — преградить все пути, которыми вирусы могут получить управление. Прослойки модифицируют среду так, что она приобретает неожиданные для вирусов свойства. Механизм антивирусной защиты заимствован непосредственно у самих врагов: она реализована как система взаимодействующих вирусов различных классов. Эти специальные вирусы обладают рядом особенностей. Выделим главные из них: во-первых, приоритетность в получении управления, эти вирусы должны занять свои места ранее прочих желающих; во-вторых, полное "срастание" с операционной средой во всех случаях, за исключением посягательств возможных вредителей. Кроме того, необходимо обеспечить максимальную независимость защиты от версии ОС и минимальное потребление ресурсов процессора, памяти, диска. В связи с тем, что преимущества защиты тесно связаны с ее секретностью, далее авторы вынуждены ограничиться кратким описанием составных частей системы антивирусной защиты и методов реализации вышеназванных особенностей.

Система защиты при таком подходе включает в себя следующие взаимодействующие компоненты:

- защита от несанкционированного доступа к жесткому диску. Представляет собой не что иное, как MAINBOOT-вирус. Она ограждает диск от сторонних пользователей (при помощи пароля), блокирует дискетную загрузку (как возможный путь внесения вирусов), обеспечивает сбор и сохранение информации, доступной только в момент загрузки и необходимой для оценки ситуации другим компонентам системы (к такой информации относятся, например, векторы прерываний). В общей системе выполняет задачи по защите операционной среды, приоритетность запуска достигается расположением и самоконтролем, автоматически уничтожающим все другие MAINBOOT-вирусы (в том числе и стартовавшие ранее);

- контроль системной информации. Обеспечивает диагностику состояния частей DOS: Boot, Ibmbio.com, Ibmdos.com (или им подобных). Выполняется в момент инициализации специального драйвера, где проверяется, что загрузка операционной среды прошла плотно (т.е. не было сторонних вмешательств от момента вызова до завершения загрузки системных файлов). Для выполнения этой задачи используется информация, полученная от модуля MAINBOOT. Надо отметить, что это тот единственный случай, когда контроль проводится после того, как неприятные события уже могли иметь место, это связано с необходимостью обеспечить независимость защиты от версии DOS, но запаздывание диагностики не повлечет за собой дальнейшего распространения инфекции, так как в ряде случаев предоставляется возможность восстановить системную информацию (используя восстановительную дискету, созданную в момент инсталляции системы). В общем комплексе контроль системной информации решает задачи по защите операционной среды. Приоритетность получения управления обусловлена свойствами специального драйвера;
- защита исполняемых и загружаемых файлов. Представляет собой совокупность вырожденных файловых вирусов и резидентной программы-ревизора. Вырожденный файловый вирус играет роль "удостоверения личности", файлы снабжаются им по мере необходимости. Программа-ревизор — подмененный интерфейс стандартного запуска задач, старт которой находится в том месте, где можно гарантировать, что между ним и средой никто посторонний не вклинился. Эта программа осуществляет контроль файла в момент запуска/загрузки, взаимодействуя с его вырожденным вирусом. Способ построения вырожденного вируса позволяет не только выявить запретное изменение файла, но и сделать это с минимальными издержками (без дополнительного чтения файла и лишь с незначительным увеличением его длины). Контролем охватываются COM-, EXE-, OVL-, SYS-, BIN-файлы. Система гибко адаптируется к операционным системам MS DOS и PC DOS (в диапазоне версий от 3.30 до 5.00).

Возможность такой адаптационной способности обусловлена тщательным выбором средств, используемых вирусами защиты.

К сожалению, размеры статьи и требования безопасности исключают более подробный и откровенный разговор о принципах построения описанной системы HEALTH. Однако отметим некоторые ее преимущества по сравнению с другими известными нам антивирусными системами. Мы ни в коей мере не хотим умалить достоинства этих систем и бросить тень недоверия на их авторов, глубоко понимая всю сложность решаемой ими задачи. Мы благодарны коллегам Д.Н. Лозинскому, А.Е. Гутникову и прочим, знакомство с работой антивирусов которых позволило учесть недостатки подобных систем при разработке HEALTH.

К преимуществам относятся следующие свойства:

- диагностика программ проводится в момент возможного заражения, и пользователь имеет возможность сразу пресечь поползновения вирусов. Программы-ревизоры осуществляют отсроченный контроль, когда количество зараженных файлов может быть велико, а потери невосполнимы. В HEALTH сохранена возможность и такого контроля, милого сердцу многих пользователей, но результаты его могут быть печальны только в том случае, если пользователь сознательно старался расселить вирус, несмотря на предупреждения HEALTH;
- HEALTH способен выявить любое вмешательство в работу программы, будь то известные, неизвестные или не существовавшие в момент создания системы вирусы, в то время как большинство антивирусов предполагают работу на ограниченном, заранее определенном наборе вирусов (расширяемом от версии к версии) или, в лучшем случае, на пополняемом наборе вирусов, но при этом включение в список вирусов еще одного нового отнесено к компетенции пользователя, который, конечно, не должен быть совсем неграмотным, но ожидать от него сверхвысокой квалификации тоже не следует;
- HEALTH ни при каких условиях не становится разносчиком инфекции, а за многими другими антивирусами замечено интересное свойство: после выполнения операций контроля, очистки, восстановления среды количество зараженных файлов может заметно возрасти;
- HEALTH-стратегия восстановления зараженных файлов такова, что избавляет пользователя от необходимости обновлять версию системы каждые две недели, обеспечивая спасение файлов от широкого потока заболеваний.

Говорят, что если от болезни есть много лекарств, то эта болезнь неизлечима. С другой стороны, лекарства, которое лечило бы от всех существующих болезней (в средние века его называли панацеей), тоже не бывает. В конце концов медики говорят, что каждый вылечивается тем, что ему помогает. А компьютерные вирусы — это не одна болезнь, а много. Так что у нас есть все основания надеяться, что плод нашего труда найдет свое место в коллекции антивирусных средств. Для тех, кого это интересует, сообщаем свой контактный телефон: (812) 310-63-39.

Литература

1. Чижов А.А. "Некоторые соображения по поводу компьютерных вирусов". В мире ПК, 1988, № 1.

2. Карасик И.Ш. "Несколько слов о компьютерных вирусах". Интеркомпьютер, 1989, № 1.

3. Стефанков Дмитрий. "Пятница, 13-е". Интерфейс, 1990, № 1.

4. Карасик И.Ш. "Анатомия и физиология вирусов". Интеркомпьютер, 1990, № 1.

5. Кадлоф Анджей. "Вирусы". Компьютер, 1990, № 1.

6. Агасандян Г. "Не вреди ближнему своему". Компьютер, 1990, № 1.

7. "10 антивирусных заповедей". Компьютер, 1990, № 1.

8. Безруков Н.Н. "Классификация вирусов. Попытка стандартизации". Интеркомпьютер, 1990, № 2.

9. Карасик И.Ш. "Классификация антивирусных программ". Интеркомпьютер, 1990, № 12.

10. Шерстюк Ф.Н. "Вирусы и антивирусы на IBM-совместимых ПК". Интеркомпьютер, 1990, № 2.

11. Селль Марек. "Антивирусные программы". Компьютер, 1990, № 2.

12. Осипенко А.С. "Компьютерные вирусы". Мир ПК, 1990, № 3.

13. Безруков Н.Н.. Компьютерная вирусология. КИИГА, 1990.