\компьютер на работе\

© Марек Селль

Антивирусные программы

"Вирус под каждой кроватью" – так была озаглавлена статья в журнале PC-Magazine, посвященная компьютерным вирусам. В этом заголовке отражается паническое состояние одних пользователей ПК и беспечность других. К какой группе присоединиться? Безусловно, не стоит сразу браться за форматирование жесткого диска с полным уничтожением его содержимого при виде прыгающего по экрану дисплея мячика или бегающего "насекомого". С другой стороны, игнорировать проблему тоже не стоит: надо помнить, что одну пятую из примерно 60 известных ныне вирусов написали программисты с террористическими наклонностями. Влияние их "детищ" на ваши файлы лишь незначительно отличается от влияния подложенной рядом с компьютером бомбы.

Что же в такой ситуации делать, как себя обезопасить? Прежде всего надо так организовать работу на компьютере, чтобы опасность заражения свести к минимуму (о принципах "компьютерной гигиены" мы писали в первом выпуске нашего сборника в статье "Десять антивирусных заповедей". – Примеч. ред.). Но полностью ликвидировать ее практически невозможно. Во всяком случае это не легче, чем выработать у себя иммунитет к насморку. Итак, давайте заблаговременно познакомимся с доступными лекарствами: специализированных антивирусных программ возникло уже довольно много.

В принципе существуют три метода программной защиты от вирусов:

* специальные программы, которые присоединяются к операционной системе с целью слежения за активностью запускаемых на ЭВМ программ. Если появляются подозрительные симптомы, они блокируют работу данной программы, предостерегают пользователя и ждут его решения. Иногда такие программы-наблюдатели поддерживаются специальными расширяющими картами, которые физически блокируют доступ к программным ресурсам;

* программы, вычисляющие контрольные суммы всех доступных на дисках программ и записывающие их в специальный файл. При очередной загрузке они проверяют, не подверглась ли какая-либо программа модификации. В случае положительного результата проверки они предупреждают пользователя. В упрощенном, зато более быстродействующем варианте контролируются единственно длина файла и дата его последней модификации. Это, конечно, исключает выявление вируса, не изменяющего эти параметры;

* программы, которые "охотятся" за определенными типами вирусов, чаще всего быстродействующие (хотя бывают и исключения), способные уничтожить "противника" без повреждения программы или дискеты. Некоторые программы такого типа проверяют, есть ли на дискете эффекты разрушительной деятельности вируса.

Я не буду сравнивать здесь достоинства и недостатки разных методов и остановлюсь на рассмотрении первой из указанных групп программ – программ-мониторов, главным свойством которых является то, что они работают вместе с операционной системой и наблюдают за действием других программ. Чтобы хорошо понять идею, заложенную в основу работы этих программ, начнем с механизма функционирования вирусов.

Компьютерные вирусы – это небольшие программы, которые сами не выполняются, а присоединяются к программам-утилитам либо же внедряются на дискету или винчестер и выполняются в момент запуска программы-носителя или загрузки ОС с зараженного диска.

Программа-вирус функционирует в два этапа. Первый этап – это размножение вируса, т.е. код вируса внедряется в различные места вашей системы; куда именно – это зависит от типа вируса. Например:

* в разного рода выполняемые файлы (как в классические программы типа EXE или COM, так и в различные программы-оболочки, системные файлы и т.д.);

* в загрузочный сектор дискеты, в таблицу разделов (partitions) жесткого диска, а также в его секторы, обозначенные как поврежденные, на дополнительные дорожки, в дополнительные секторы или даже во временно свободные секторы корневого каталога.

Некоторые вирусы живут и размножаются в операционной системе, другие – в зараженных программах.

Наличие первого этапа, т.е. размножения, отличает вирусы от давно известных "троянских коней" – программ, которые под прикрытием нормальной работы, нередко полезной или развлекательной, выполняют функции, типичные для второго этапа деятельности вирусов.

Второй этап, который можно назвать фазой разрушения, чаще всего наступает при определенных условиях или же спустя некоторое время, достаточное для того, чтобы вирус широко распространился перед моментом "рассекречивания", к которому эта фаза ведет. То, что делает вирус на этапе разрушения, является производной знаний, больной фантазии и степени недоброжелательности его создателя. Например, вирус может:

* уничтожить на диске системные файлы, что блокирует возможность чтения его содержимого;

* отформатировать всю дискету или некоторые дорожки;

* уничтожить случайно выбранные секторы;

* изменить параметры винчестера или дисковода в памяти конфигурации, в результате чего компьютер "не видит" диск или дискету;

* привести к другим осложнениям (снижение скорости работы компьютера, деформация выводимой на дисплей информации или даже попытка физического повреждения оборудования – дисплея, принтера, дисковода или винчестера).

Итак, главным объектом атаки (а на этапе размножения единственным) являются диски вашего компьютера. Это наводит на мысль, что можно попытаться заблокировать атаку, непрерывно контролируя обращения к дисководам и отфильтровывая те, которые выглядят подозрительно. Именно эта идея заложена в основу работы рассматриваемых здесь антивирусных программ.

Давайте подумаем, что должна уметь такая программа?

1. Чтобы заблокировать присоединение кода вируса к ОС, она должна предостерегать в случае по-

пытки неизвестной программы стать резидентной.

2. Чтобы пресечь возможность размножения вирусов, программа должна противодействовать такой модификации исполняемых файлов, которая не является частью нормальной работы системы и в то же время необходима для заражения файла вирусом.

3. Попытки непосредственного (в обход системы файлов ДОС) доступа к дискам, особенно к их системным областям (загрузочный сектор, таблица разделов жесткого диска, каталоги или таблицы размещения файлов), могут быть результатом размножения вируса или элементом этапа разрушения. Пользователь должен знать об этом заранее. Стоит вести своего рода дневник модификаций винчестера, что в случае повреждения файлов облегчит поиск виновника.

4. Программа должна регулярно проверять содержимое памяти конфигурации компьютера PC/AT, что позволит избежать трудностей с распознаванием дискеты после рестарта ОС. Необходимой является также возможность восстановления первичных параметров конфигурации при выявлении незапланированных изменений.

5. Программа-монитор должна сравнивать контрольные суммы запускаемой программы с вычисленными ранее и записанными в отдельный файл величинами. Это позволит выявить изменения в программе, прежде чем она будет выполнена.

Итак, ясно, какими свойствами должны обладать антивирусные программы рассматриваемой группы, чтобы предупреждать разрушительную деятельность вирусов. (Есть ряд программ, которые позволяют лишь констатировать то, что уже случилось, и уничтожить вирус.)

Остается еще ответить на вопрос, насколько "прочны" антивирусные программы-мониторы?

Ответ был бы прост, если можно было бы допустить, что вирусы – это "хорошо написанные программы", т.е. такие, которые любые действия осуществляют посредством функций ДОС или в крайнем случае BIOS, а также что антивирусная программа запускается на компьютере, память которого свободна от вирусов (иначе говоря, к операционной системе вирус не "прицепил" дополнительные процедуры в виде резидентных программ).

К сожалению, по нескольким причинам из таких предпосылок исходить нельзя. Рассмотрим эти причины.

1. Довольно многочисленна группа вирусов загрузочного сектора и таблицы разделов жесткого диска, которые активизируются в памяти перед загрузкой ОС, т.е. перед загрузкой антивирусной программы. Со стороны многих антивирусных программ действие таких вирусов не контролируется. Случается также, что вирус нельзя обнаружить при чтении сектора, в котором он "поселился", – сектор выглядит таким же, каким был до заражения.

2. Существует возможность присоединения фрагмента кода к системе путем манипулирования величинами в заголовках блоков памяти без использования функций ДОС. Это можно выявить, периодически проверяя содержимое заголовков, но пока я не встречал программ (ни коммерческих, ни общедоступных), которые это делают.

3. Начинают появляться вирусы, которые в ПЗУ находят адреса начала процедур обслуживания дисководов и выполняют непосредственный переход на найденный адрес. Это невозможно выявить чисто программным путем. Но все известные мне вирусы такого типа выполняют одну из операций через ДОС, благодаря чему они могут обнаруживаться программами-мониторами. Тем не менее возможно создание вируса, который все свои функции выполнит путем описанных выше непосредственных переходов. В таком случае возникает вопрос: стоит ли вообще пользоваться программами-мониторами? Безусловно, стоит, и причин тому несколько:

* вирусов, заражающих программы, намного больше, чем вирусов, заражающих загрузочные секторы;

* заражение загрузочного сектора легче предотвратить организационными методами;

* не все авторы вирусов отличаются изобретательностью, поэтому большинство их "шедевров" можно выявить с помощью программ-мониторов;

* метод, состоящий в проверке контрольной суммы программы перед ее выполнением, чрезвычайно эффективен по отношению к вирусам, заражающим программы.

Итак, обсудив все "за" и "против", можно прийти к следующему выводу: программы-мониторы стоит применять в качестве антивирусной защиты, однако следует помнить, что они не полностью исключают возможность заражения.

Для того чтобы повысить безопасность, необходимо помнить об упомянутой "антивирусной гигиене" и организационных мерах. В ситуации, когда опасность заражения системы резко возрастает (например, при работе на ней многочисленных пользователей), стоит также время от времени использовать антивирусную программу, проверяющую контрольные суммы, характерные байты или же выявляющую вирусы какими-либо другими методами (лучше всего после загрузки системы со специально подготовленной для этой цели дискеты с закрытым вырезом маркера защиты).

Теперь я предлагаю краткий обзор существующих в начале 1990 г. программ-мониторов и их сравнение с описанным выше "идеалом". Рассматриваться будут только программы типа shareware и общедоступные программы (так как не думаю, чтобы кто-либо из читателей собирался израсходовать на коммерческий продукт такого типа сумму, нередко превышающую 100 дол.).

DPROTECT.COM версия 1.01, автор Джи М. Уонг

Примитивная программа, написанная в период, когда главной опасностью были "троянские кони". Она блокирует на указанных дисководах все разрушающие операции (запись, форматирование), проводимые посредством дискового BIOS. В случае выявления запрещенной операции программа требует рестарта системы. Для снятия защиты необходима перезагрузка системы. Программа может пригодиться лишь при проверке работы новых программ неизвестного происхождения.

HDSENTRY.COM версия 1.01, автор Эндрю М. Фрайд

Программа напоминает DPROTECT. Ее главное отличие – в возможности продолжения работы после выявления запрещенной операции записи или форматирования. Обнаружив попытку такой операции, программа сообщает о ней, после чего, заблокировав ее, продолжает наблюдение. Дискеты защищаются также от разрушающих операций, использующих прерывание 16h. Программа полезна только при проверке новых программ.

BOMBSQUAD.COM версия 1.2, автор Энди Хопкинз

По своей работе программа также напоминает DPROTECT, но она гораздо более "дружественна". При выявлении запрещенной операции можно разрешить ее выполнение. Конфигурация программы изменяется без повторной загрузки системы. Полезность программы – на уровне DPROTECT.

TRAPDISK.COM версия 1.0

Вариант программы BOMBSQUAD, разработан неизвестным автором, который, не считая косметических изменений, добавил обслуживание дополнительных функций дискового BIOS.

VIRBLOCK.EXE версия 2.1, автор Михель Фитц

Работа известного автора антивирусных программ из Вены. Программа блокирует запись в файлы типа COM и EXE. В случае выявления нелегальной операции – обращается с запросом к оператору, а затем действует в зависимости от ответа. Выполняется только часть функций, которых следовало бы ожидать от программы-монитора, однако за неимением другого она может использоваться против некоторых типов вирусов.

ANTI4US2.EXE версия 1.00, автор Э. Лантинг

Полноценное антивирусное средство, несмотря на отсутствие некоторых функций приведенной выше идеальной программы. ANTI4US2.EXE отличается простотой обслуживания благодаря системе МЕНЮ, которое позволяет изменять параметры работы. Программа способна блокировать непосредственный доступ к дисководу (в обход системы файлов ДОС), операцию форматирования, модификацию программ и файлов типа BAT. Она также проверяет, не пытаются ли выполняемые программы присоединиться к ОС. В случае выявления действий, которые пользователь определил как нелегальные, на дисплее появляется предостерегающее сообщение и вопрос о разрешении или запрете выполнения данной операции. Еще одним достоинством программы является встроенный "дневник работы". Сюда записывается информация о всех запускаемых программах и список модифицированных ими файлов.

Недостатком является большой объем ANTI4US2.EXE (50 Кбайт). Кроме того, ее можно вызвать комбинацией клавиш Alt-4 только тогда, когда COMMAND.COM первого уровня ожидает директив. Попытка вызвать программу в других условиях, например при загруженном Norton Commander, активизирует звуковой сигнал, который не прекращается до тех пор, пока программа не начнет работу – в данном случае до выхода из Norton Commander.

FLUSHOT2

FLUSHOT3

FSP версия 1.00

FSP версия 1.41, автор Росс М. Гринберг

Очередные версии популярной программы-монитора, которая вначале распространялась как общедоступная (Public Domain), а в последней версии (FluShot Plus) является продуктом типа shareware с низкой регистрационной оплатой (10 дол.). Программа защищает от непосредственного доступа к дисководам и от определенных в специальном конфигурирующем файле таких операций, как:

* запуск программы, контрольная сумма которой не соответствует сумме, записанной в конфигурирующем файле. Все суммы проверяются также в момент запуска программы FSP;

* попытка загрузки резидентной программы, которая не содержится в конфигурирующем файле;

* запись или чтение определенных файлов.

Программа небольшая (10–15 Кбайт) и относительно "умная". К ее недостаткам можно отнести отсутствие контроля за прерыванием BIOS номер 40h, разрешающим запись, а также довольно сложную процедуру предварительного вычисления контрольных сумм. Однако это не уменьшает ценности программы, которая считается одной из лучших в своем классе.

FLUSHOT 2 и 3 отличаются от предыдущих версий отсутствием конфигурирующего файла, в связи с чем список защищаемых программ является постоянным. Кроме того, ими не вычисляются контрольные суммы.

Я представил здесь лишь те программы, которые у меня есть. Безусловно, их гораздо больше. Замечания, сделанные в начале статьи, помогут читателям оценить их качество самостоятельно.

Перевод Анджея Поплавского