

Методы обнаружения и удаления компьютерных вирусов

Антивирусные программы

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Однако сразу хотелось бы отметить, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, и заявления о существовании таких систем можно расценить как либо недобросовестную рекламу, либо непрофессионализм. Таких систем не существует, поскольку на любой алгоритм антивируса всегда можно предложить контр-алгоритм вируса, невидимого для этого антивируса (обратное, к счастью, тоже верно: на любой алгоритм вируса всегда можно создать антивирус). Более того, невозможность существования абсолютного антивируса была доказана математически на основе теории конечных автоматов, автор доказательства - Фред Коэн.

Следует также обратить внимание на несколько терминов, применяемых при обсуждении антивирусных программ:

"Ложное срабатывание" (False positive) - детектирование вируса в незараженном объекте (файле, секторе или системной памяти). Обратный термин - "False negative", т.е. недетектирование вируса в зараженном объекте.

"Сканирование по запросу" ("on-demand") - поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания (system scheduler).

"Сканирование на-лесту" ("real-time", "on-the-fly") - постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т.п.). В этом режиме антивирус постоянно активен, он присутствует в памяти "резидентно" и проверяет объекты без запроса пользователя.

Типы антивирусов

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры (другие названия: фаги, полифаги). Следом за ними по эффективности и популярности следуют CRC-сканеры (также: ревизор, checksumer, integrity checker). Часто оба приведенных метода объединяются в одну универсальную антивирусную программу, что значительно повышает ее мощность. Применяются также различного типа блокировщики и иммунизаторы.

Сканеры

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые "маски". Маской вируса является некоторая постоянная

последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски, или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфных вирусов.

Во многих сканерах используются также алгоритмы "эвристического сканирования", т.е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения ("возможно заражен" или "не заражен") для каждого проверяемого объекта. Поскольку эвристическое сканирование является во многом вероятностным методом поиска вирусов, то на него распространяются многие законы теории вероятностей. Например, чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Сканеры также можно разделить на две категории - "универсальные" и "специализированные". Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макро-вирусов. Специализированные сканеры, рассчитанные только на макро-вирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Сканеры также делятся на "резидентные" (мониторы), производящие сканирование "на-лету", и "нерезидентные", обеспечивающие проверку системы только по запросу. Как правило, "резидентные" сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как "нерезидентный" сканер способен опознать вирус только во время своего очередного запуска.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам - размеры антивирусных баз, которые сканерам приходится "таскать за собой", и относительно небольшую скорость поиска вирусов.

CRC-сканеры

Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

CRC-сканеры, использующие анти-стелс алгоритмы, являются довольно сильным оружием против вирусов: практически 100% вирусов оказываются

обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту "слабость" CRC-сканеров, заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для них.

Блокировщики

Антивирусные блокировщики - это резидентные программы, перехватывающие "вирусо-опасные" ситуации и сообщающие об этом пользователю. К "вирусо-опасным" относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или MBR винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения.

К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно "выползает неизвестно откуда". К недостаткам относятся существование путей обхода защиты блокировщиков и большое количество ложных срабатываний, что, видимо, и послужило причиной для практически полного отказа пользователей от подобного рода антивирусных программ (мне, например, неизвестно ни об одном блокировщике для Windows95/NT - нет спроса, нет и предложения).

Необходимо также отметить такое направление антивирусных средств, как антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера ("железа"). Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера. Однако, как и в случае с программными блокировщиками, такую защиту легко обойти прямой записью в порты контроллера диска, а запуск DOS-утилиты FDISK немедленно вызывает "ложное срабатывание" защиты.

Существует несколько более универсальных аппаратных блокировщиков, но к перечисленным выше недостаткам добавляются также проблемы совместимости со стандартными конфигурациями компьютеров и сложности при их установке и настройке. Все это делает аппаратные блокировщики крайне непопулярными на фоне остальных типов антивирусной защиты.

Иммунизаторы

Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса. Первые обычно записываются в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение. Недостаток у таких иммунизаторов всего один, но он летален:

абсолютная неспособность сообщить о заражении стелс-вирусом. Поэтому такие иммунизаторы, как и блокировщики, практически не используются в настоящее время.

Второй тип иммунизации защищает систему от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные (пример - печально известная строка "MsDos", предохраняющая от ископаемого вируса "Jerusalem"). Для защиты от резидентного вируса в память компьютера заносится программа, имитирующая копию вируса. При запуске вирус натывается на нее и считает, что система уже заражена.

Такой тип иммунизации не может быть универсальным, поскольку нельзя иммунизировать файлы от всех известных вирусов: одни вирусы считают уже зараженными файлы, если время создания файла содержит метку 62 секунды, а другие - 60 секунд. Однако несмотря на это, подобные иммунизаторы в качестве полумеры могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет определяться антивирусными сканерами.

Какой антивирус лучше?

Какой антивирус самый лучший? Ответ будет - "любой", если на вашем компьютере вирусы не водятся, и вы не пользуетесь вирусно-опасными источниками информации. Если же вы любитель новых программ, игрушек, ведете активную переписку по электронной почте и используете при этом Word или обмениваетесь таблицами Excel, то вам все-таки следует использовать какой-либо антивирус. Какой именно - решайте сами, однако есть несколько позиций, по которым различные антивирусы можно сравнить между собой.

Качество антивирусной программы определяется, на мой взгляд, по следующим позициям, приведенным в порядке убывания их важности:

Надежность и удобство работы - отсутствие "зависаний" антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.

Качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц (MS Word, Excel, Office97), упакованных и архивированных файлов. Отсутствие "ложных срабатываний". Возможность лечения зараженных объектов. Для сканеров (см. ниже), как следствие, важной является также периодичность появления новых версий (апдейтов), т.е. скорость настройки сканера на новые вирусы.

Существование версий антивируса под все популярные платформы (DOS, Windows, Windows95, Windows NT, Novell NetWare, OS/2, Alpha, Linux и т.д.), присутствие не только режима "сканирование по запросу", но и "сканирование на лету", существование серверных версий с возможностью администрирования сети.

Скорость работы и прочие полезные особенности, функции, "припарки" и "вкусности".

Надежность работы антивируса является наиболее важным критерием, поскольку даже "абсолютный антивирус" может оказаться бесполезным, если он будет не в состоянии довести процесс сканирования до конца - "повиснет" и не проверит часть дисков и файлов и, таким образом, оставит вирус незамеченным в системе. Если же антивирус требует от пользователя специальных знаний, то он также окажется бесполезным - большинство пользователей просто проигнорирует сообщения антивируса и нажмут [ОК] либо [Cancel] случайным образом, в зависимости от того, к какой кнопке ближе находится курсор мыши в данный момент. Ну а если антивирус будет чересчур часто задавать сложные вопросы рядовому пользователю, то, скорее всего, он (пользователь) перестанет запускать такой антивирус или даже удалит его с диска.

Качество детектирования вирусов стоит следующим пунктом по вполне естественной причине. Антивирусные программы потому и называются антивирусными, что их прямая обязанность - ловить и лечить вирусы. Любой самый "навороченный" по своим возможностям антивирус бесполезен, если он не в состоянии ловить вирусы или делает это не вполне качественно. Например, если антивирус не детектирует 100% какого-либо полиморфного вируса, то при заражении системы этим вирусом такой антивирус обнаружит только часть (допустим 99%) зараженных на диске файлов. Необнаруженными останется всего 1%, но когда вирус снова проникнет в компьютер, то антивирус опять обнаружит 99%, но уже не от всех файлов, а только от вновь зараженных. В результате заражено на диске будет уже 1.99%. И так далее, пока все файлы на диске не будут заражены при полном молчании антивируса.

Поэтому качество детектирования вирусов является вторым по важности критерием "лучшести" антивирусной программы, более важным, чем "многоплатформенность", наличие разнообразного сервиса и т.д. Однако если при этом антивирус с высоким качеством детектирования вирусов вызывает большое количество "ложных срабатываний", то его "уровень полезности" резко падает, поскольку пользователь вынужден либо уничтожать незараженные файлы, либо самостоятельно производить анализ подозрительных файлов, либо привыкает к частым "ложным срабатываниям", перестает обращать внимание на сообщения антивируса и в результате пропускает сообщение о реальном вирусе.

"Многоплатформенность" антивируса является следующим пунктом в списке, поскольку только программа, рассчитанная на конкретную операционную систему, может полностью использовать функции этой системы. "Неродные" же антивирусы часто оказываются неработоспособными, а иногда даже разрушительными. Например, вирус "OneHalf" поразил компьютер с установленными на нем Windows95 или WindowsNT. Если для расшифровки диска (данный вирус шифрует сектора диска) воспользоваться DOS-антивирусом, то результат может оказаться плачевным: информация на диске окажется безнадежно испорченной, поскольку Windows 95/NT не позволит антивирусу пользоваться прямыми

вызовами чтения/записи секторов при расшифровке секторов. Антивирус же, являющийся Windows-программой, справляется с этой задачей без проблем. Возможность проверки файлов "на лету" также является достаточно важной чертой антивируса. Моментальная и принудительная проверка приходящих на компьютер файлов и вставляемых дискет является практически 100%-й гарантией от заражения вирусом, если, конечно, антивирус в состоянии детектировать этот вирус. Очень полезными являются антивирусы, способные постоянно следить за "здоровьем" серверов - Novell NetWare, Windows NT, а в последнее время, после массового распространения макро-вирусов, и за почтовыми серверами, сканируя входящую/исходящую почту. Если же в серверном варианте антивируса присутствуют возможность антивирусного администрирования сети, то его ценность еще более возрастает.

Следующим по важности критерием является скорость работы. Если на полную проверку компьютера требуется несколько часов, то вряд ли большинство пользователей будут запускать его достаточно часто. При этом медленность антивируса совсем не говорит о том, что он ловит вирусов больше и делает это лучше, чем более быстрый антивирус. В разных антивирусах используются различные алгоритмы поиска вирусов, один алгоритм может оказаться более быстрым и качественным, другой - медленным и менее качественным. Все зависит от способностей и профессионализма разработчиков конкретного антивируса.

Наличие всяческих дополнительных функций и возможностей стоит в списке качеств антивируса на последнем месте, поскольку очень часто эти функции никак не сказываются на уровне "полезности" антивируса. Однако эти дополнительные функции значительно упрощают жизнь пользователя и, может быть, даже подталкивают его запускать антивирус почаще.

Методика использования антивирусных программ

Следите за тем, чтобы антивирусные программы, используемые для проверки, были самых последних версий. Если к программам поставляются апдейты, то проверьте их на "свежесть". Обычно выход новых версий антивирусов анонсируется, поэтому достаточно посетить соответствующие WWW/ftp/BBS.

"Национальность" антивирусов в большинстве случаев не имеет значения, поскольку на сегодняшний день процесс эмиграции вируса в другие страны и иммиграции антивирусных программ ограничивается только скоростью Internet, поэтому как вирусы, так и антивирусы не признают границ.

Если на компьютере обнаружен вирус, то самое главное - не паниковать (тем, для кого "встреча" с вирусом - вполне обыденное явление, такая рекомендация может показаться смешной). Паника никогда не доводила до добра: непродуманные действия могут привести к печальным последствиям.

Если вирус обнаружен в каком-то из новых файлов и еще не проник в систему, то нет причин для беспокойства: убейте этот файл (или удалите вирус любимой антивирусной программой) и спокойно работайте дальше. В случае обнаружения вируса сразу в нескольких файлах на диске или в

загрузочном секторе, то проблема становится более сложной, но все равно разрешимой - антивирусники не зря едят свой хлеб.

Следует еще раз обратить внимание на термин "ложное срабатывание". Если в каком-либо ОДНОМ файле, который достаточно долго "живет" на компьютере, какой-либо один антивирус обнаружил вирус, то это скорее всего ложное срабатывание. Если такой файл запускался несколько раз, а вирус так и не переполз в другие файлы, то это крайне странно. Попробуйте проверить файл другими антивирусами. Если они хранят молчание, отправьте этот файл в лабораторию фирмы-производителя антивируса, обнаружившего в нем вирус.

Если же на компьютере действительно найден вирус, то надо сделать следующее:

1. В случае обнаружения файлового вируса, если компьютер подключен к сети, необходимо отключить его от сети и проинформировать системного администратора. Если вирус еще не проник в сеть, это защитит сервер и другие рабочие станции от проникновения вируса. Если же вирус уже поразил сервер, то отключение от сети не позволит ему вновь проникнуть на компьютер после его лечения. Подключение к сети возможно лишь после того, как будут вылечены все сервера и рабочие станции.

При обнаружении загрузочного вируса отключать компьютер от сети не следует: вирусы этого типа по сети не распространяются (естественно, кроме файлово-загрузочных вирусов).

Если произошло заражение макро-вирусом вместо, отключения от сети достаточно на период лечения убедиться в том, что соответствующий редактор (Word/Excel) неактивен ни на одном компьютере.

2. Если обнаружен файловый или загрузочный вирус, следует убедиться в том, что вирус либо нерезидентный, либо резидентная часть вируса обезврежена: при запуске некоторые (но не все) антивирусы автоматически обезвреживают резидентные вирусы в памяти. Удаление вируса из памяти необходимо для того, чтобы остановить его распространение. При сканировании файлов антивирусы открывают их, многие из резидентных вирусов перехватывают это событие и заражают открываемые файлы. В результате большая часть файлов окажется зараженной, поскольку вирус не удален из памяти. То же может произойти и в случае загрузочных вирусов - все проверяемые дискеты могут оказаться зараженными.

Если используемый антивирус не удаляет вирусы из памяти, следует перезагрузить компьютер с заведомо незараженной и защищенной от записи системной дискеты. Перезагрузка должна быть "холодной" (клавиша Reset или выключение/включение компьютера), так как некоторые вирусы "выживают" при теплой перезагрузке. Некоторые вирусы используют приемы, позволяющие им "выжить" и при холодной перезагрузке (см., например, вирус "[Ugly](#)"), поэтому также следует проверить в настройках BIOS пункт "последовательность загрузки A: C:", чтобы гарантировать загрузку DOS с системной дискеты, а не с зараженного винчестера.

Помимо резидентности/нерезидентности полезно ознакомиться и с другими характеристиками вируса: типами заражаемых вирусом файлов, проявлениями и прочее. Единственный известный мне источник подробной информации данного рода практически обо всех известных вирусах - "Энциклопедия вирусов AVP".

3. При помощи антивирусной программы нужно восстановить зараженные файлы и затем проверить их работоспособность. Перед лечением или одновременно с ним - создать резервные копии зараженных файлов и распечатать или сохранить где-либо список зараженных файлов (log-файл антивируса). Это необходимо для того, чтобы восстановить файлы, если лечение окажется неуспешным из-за ошибки в лечащем модуле антивируса либо по причине неспособности антивируса лечить данный вирус. В этом случае придется прибегнуть к помощи какого-либо другого антивируса.

Гораздо надежнее, конечно, восстановить зараженные файлы из backup-копии (если она есть), однако все равно потребуются услуги антивируса - вдруг не все копии вируса окажутся уничтожены, или если файлы в backup-копии также заражены.

Следует отметить, что качество восстановления файлов многими антивирусными программами оставляет желать лучшего. Многие популярные антивирусы частенько необратимо портят файлы вместо их лечения. Поэтому если потеря файлов нежелательна, то выполнять перечисленные выше пункты следует в полном объеме.

В случае загрузочного вируса необходимо проверить все дискеты независимо от того, загрузочные они (т.е. содержат файлы DOS) или нет. Даже совершенно пустая дискета может стать источником распространения вируса - достаточно забыть ее в дисковом диске и перезагрузить компьютер (если, конечно же, в BIOS Setup загрузочным диском отмечен флоппи-диск)

Помимо перечисленных выше пунктов необходимо обращать особое внимание на чистоту модулей, сжатых утилитами типа LZEXE, PKLITE или DIET, файлов в архивах (ZIP, ARC, ICE, ARJ и т.д.) и данных в самораспаковывающихся файлах, созданных утилитами типа ZIP2EXE. Если случайно упаковать файл, зараженный вирусом, то обнаружение и удаление такого вируса без распаковки файла практически невозможно. В данном случае типичной будет ситуация, при которой все антивирусные программы, неспособные сканировать внутри упакованных файлов, сообщат о том, что от вирусов очищены все диски, но через некоторое время вирус появится опять.

Штаммы вируса могут проникнуть и в backup-копии программного обеспечения при обновлении этих копий. Причем архивы и backup-копии являются основными поставщиками давно известных вирусов. Вирус может годами "сидеть" в дистрибутивной копии какого-либо программного продукта и неожиданно проявиться при установке программ на новом компьютере.

Никто не гарантирует полного уничтожения всех копий компьютерного вируса, так как файловый вирус может поразить не только выполняемые файлы, но и оверлейные модули с расширениями имени, отличающимися от

COM или EXE. Загрузочный вирус может остаться на какой-либо дискете и внезапно проявиться при случайной попытке перезагрузиться с нее. Поэтому целесообразно некоторое время после удаления вируса постоянно пользоваться резидентным антивирусным сканером (не говоря уже о том, что желательно пользоваться им постоянно)

Профилактика заражения компьютера

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которое позволяет значительно снизить вероятность заражения вирусом и потери каких-либо данных.

Для того чтобы определить основные правила компьютерной гигиены, необходимо выяснить основные пути проникновения вируса в компьютер и компьютерные сети.