

Откуда берутся вирусы

Глобальные сети - электронная почта

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word/Office97. Пользователь зараженного макро-вирусом редактора, сам того не подозревая, рассылает зараженные письма адресатам, которые в свою очередь отправляют новые зараженные письма и т.д.

Предположим, что пользователь ведет переписку с пятью адресатами, каждый из которых также переписывается с пятью адресатами. После отправки зараженного письма все пять компьютеров, получившие его, оказываются зараженными. Затем с каждого вновь зараженного компьютера отправляется еще пять писем. Одно уходит назад на уже зараженный компьютер, а четыре - новым адресатам.

Таким образом, на втором уровне рассылки заражено уже $1+5+20=26$ компьютеров. Если адресаты сети обмениваются письмами раз в день, то к концу рабочей недели (за 5 дней) зараженными окажутся как минимум $1+5+20+80+320=426$ компьютеров. Нетрудно подсчитать, что за 10 дней зараженными оказываются более ста тысяч компьютеров! Причем каждый день их количество будет учетверяться.

Описанный случай распространения вируса является наиболее часто регистрируемым антивирусными компаниями. Нередки случаи, когда зараженный файл-документ или таблица Excel по причине недосмотра попадает в списки рассылки коммерческой информации какой-либо крупной компании. В этом случае страдают не пять, а сотни или даже тысячи абонентов таких рассылок, которые затем разошлют зараженные файлы десяткам тысячам своих абонентов.

Электронные конференции, файл-серверы ftp и BBS

Файл-серверы "общего пользования" и электронные конференции также служат одним из основных источников распространения вирусов. Практически каждую неделю приходит сообщение о том, что какой-либо пользователь заразил свой компьютер вирусом, который был снят с BBS, ftp-сервера или из какой-либо электронной конференции.

При этом часто зараженные файлы "закладываются" автором вируса на несколько BBS/ftp или рассылаются по нескольким конференциям одновременно, и эти файлы маскируются под новые версии какого-либо программного обеспечения (иногда - под новые версии антивирусов).

В случае массовой рассылки вируса по файл-серверам ftp/BBS пораженными практически одновременно могут оказаться тысячи компьютеров, однако в большинстве случаев "закладываются" DOS- или Windows-вирусы, скорость распространения которых в современных условиях значительно ниже, чем макро-вирусов. По этой причине подобные инциденты практически никогда не кончаются массовыми эпидемиями, чего нельзя сказать про макро-вирусы.

Локальные сети

Третий путь "быстрого заражения" - локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере (в случае Novell NetWare - LOGIN.COM).

На следующий день пользователи при входе в сеть запускают зараженные файлы с сервера, и вирус таким образом получает доступ на компьютеры пользователей.

Вместо служебного файла LOGIN.COM может также выступать различное программное обеспечение, установленное на сервере, стандартные документы-шаблоны или Excel-таблицы, применяемые в фирме, и т.д.

Пиратское программное обеспечение

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных "зон риска". Часто пиратские копии на дискетах и даже на CD-дисках содержат файлы, зараженные самыми разнообразными типами вирусов.

Персональные компьютеры "общего пользования"

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из студентов принес на своих дискетах вирус и заразил какой-либо учебный компьютер, то очередную "заразу" получают и дискеты всех остальных студентов, работающих на этом компьютере.

То же относится и к домашним компьютерам, если на них работает более одного человека. Нередки ситуации, когда сын-студент (или дочь), работая на многопользовательском компьютере в институте, перетаскивают отсюда вирус на домашний компьютер, в результате чего вирус попадает в компьютерную сеть фирмы папы или мамы.

Ремонтные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники - тоже люди, и некоторым из них свойственно наплеватьское отношение к элементарным правилам компьютерной безопасности. Однажды забыв закрыть защиту от записи на одном из своих флоппи-дисков, такой "маэстро" довольно быстро разнесет заразу по машинам своей клиентуры и скорее всего потеряет ее (клиентуру).

Основные правила защиты

Правило первое

Крайне осторожно относитесь к программам и документам Word/Excel, которые получаете из глобальных сетей. Перед тем, как запустить файл на выполнение или открыть документ/таблицу, обязательно проверьте их на наличие вирусов.

Используйте специализированные антивирусы - для проверки "на-лету" всех файлов, приходящих по электронной почте (и по Internet в целом). К сожалению, на сегодняшний день мне неизвестны антивирусы, которые достаточно надежно ловят вирусы в приходящих из Internet файлах, но не исключено, что такие антивирусы появятся в ближайшем будущем.

Правило второе - защита локальных сетей

Для уменьшения риска заразить файл на сервере администраторам сетей следует активно использовать стандартные возможности защиты сети: ограничение прав пользователей; установку атрибутов "только на чтение" или даже "только на запуск" для всех выполняемых файлов (к сожалению, это не всегда оказывается возможным) и т.д.

Используйте специализированные антивирусы, проверяющие "на лету" файлы, к которым идет обращение. Если это по какой-либо причине невозможно, регулярно проверяйте сервер обычными антивирусными программами.

Значительно уменьшается риск заражения компьютерной сети при использовании бездисковых рабочих станций.

Желательно также перед тем, как запустить новое программное обеспечение, попробовать его на тестовом компьютере, не подключенном к общей сети.

Правило третье

Лучше покупать дистрибутивные копии программного обеспечения у официальных продавцов, чем бесплатно или почти бесплатно копировать их из других источников или

покупать пиратские копии. При этом значительно снижается вероятность заражения, хотя известны случаи покупки инфицированных дистрибутивов.

Как следствие из этого правила вытекает необходимость хранения дистрибутивных копий программного обеспечения (в том числе копий операционной системы), причем копии желательно хранить на защищенных от записи дискетах.

Пользуйтесь только хорошо зарекомендовавшими себя источниками программ и прочих файлов, хотя это не всегда спасает (например, на WWW-сервере Microsoft довольно долгое время находился документ, зараженный макро-вирусом "Wazzu"). По-видимому, единственными надежными с точки зрения защиты от вирусов являются BBS/ftp/WWW антивирусных фирм-разработчиков.

Правило четвертое

Старайтесь не запускать непроверенные файлы, в том числе полученные из компьютерной сети. Желательно использовать только программы, полученные из надежных источников. Перед запуском новых программ обязательно проверьте их одним или несколькими антивирусами.

Если даже ни один антивирус не среагировал на файл, который был снят с BBS или электронной конференции - не торопитесь его запускать. Подождите неделю, если этот файл вдруг окажется заражен новым неизвестным вирусом, то скорее всего кто-либо "наступит на грабли" раньше вас и своевременно сообщит об этом.

Желательно также, чтобы при работе с новым программным обеспечением в памяти резидентно находился какой-либо антивирусный монитор. Если запускаемая программа заражена вирусом, то такой монитор поможет обнаружить вирус и остановить его распространение.

Все это приводит к необходимости ограничения круга лиц, допущенных к работе на конкретном компьютере. Как правило, наиболее часто подвержены заражению "многопользовательские" персональные компьютеры.

Правило пятое

Пользуйтесь утилитами проверки целостности информации. Такие утилиты сохраняют в специальных базах данных информацию о системных областях дисков (или целиком системные области) и информацию о файлах (контрольные суммы, размеры, атрибуты, даты последней модификации файлов и т.д.). Периодически сравнивайте информацию, хранящуюся в подобной базе данных, с реальным содержимым винчестера, так как практически любое несоответствие может служить сигналом о появлении вируса или "троянской" программы.

Правило шестое

Периодически сохраняйте на внешнем носителе файлы, с которыми ведется работа. Такие резервные копии носят название backup-копий. Затраты на копирование файлов, содержащих исходные тексты программ, базы данных, документацию, значительно меньше затрат на восстановление этих файлов при проявлении вирусом агрессивных свойств или при сбое компьютера.

При наличии стримера или какого-либо другого внешнего носителя большого объема имеет смысл делать backup всего содержимого винчестера. Но поскольку времени на создание подобной копии требуется значительно больше, чем на сохранение только рабочих файлов, имеет смысл делать такие копии реже.

Прочие правила

Если нет нужды каждый день грузить систему с дискеты, поставьте в BIOS Setup порядок загрузки "сначала - С:, потом - А:". Это надежно защитит компьютер от загрузочных вирусов.

Не обольщайтесь встроенной в BIOS защитой от вирусов, многие вирусы "обходят" ее при помощи различных приемов.

То же верно для систем антивирусной защиты, встроенных в Word и Office97. Они также могут быть отключены вирусом (или самим пользователем, поскольку эти системы могут сильно мешать в работе).

Проблема защиты от макро-вирусов

Поскольку проблема макро-вирусов в последнее время перекрывает все остальные проблемы, связанные с прочими вирусами, на ней следует остановиться подробнее.

Существует несколько приемов и встроенных в Word/Excel функций, направленных на предотвращение запуска вируса. Наиболее действенной из них является защита от вирусов, встроенная в Word и Excel (начиная с версий 7.0a). Эта защита при открытии файла, содержащего любой макрос, сообщает о его присутствии и предлагает запретить этот макрос. В результате макрос не только не выполняется, но и не виден средствами Word/Excel.

Такая защита является достаточно надежной, однако абсолютно бесполезна, если пользователь работает с макросами (любыми): она не отличает макросы вируса от не-вируса и выводит предупреждающее сообщение при открытии практически любого файла. По этой причине защита в большинстве случаев оказывается отключенной, что дает возможность вирусу проникнуть в систему. К тому же включение защиты от вирусов в уже зараженной системе не во всех случаях помогает - некоторые вирусы, однажды получив управление, при каждом запуске отключают защиту от вирусов и таким образом полностью блокируют ее.

Существуют другие методы противодействия вирусам, например функция DisableAutoMacros, однако она не запрещает выполнение прочих макросов и блокирует только те вирусы, которые для своего распространения используют один из авто-макросов.

Запуск Word с опцией /M (или с нажатой клавишей Shift) отключает только один макрос AutoExec и таким образом также не может служить надежной защитой от вируса.

Восстановление пораженных объектов

В большинстве случаев заражения вирусом процедура восстановления зараженных файлов и дисков сводится к запуску подходящего антивируса, способного обезвредить систему. Если же вирус неизвестен ни одному антивирусу, то достаточно отослать зараженный файл фирмам-производителям антивирусов и через некоторое время (обычно - несколько дней или недель) получить лекарство-"апдейт" против вируса. Если же время не ждет, то обезвреживание вируса придется произвести самостоятельно.

Восстановление файлов-документов и таблиц

Для обезвреживания Word и Excel достаточно сохранить всю необходимую информацию в формате не-документов и не-таблиц - наиболее подходящим является текстовый RTF-формат, содержащий практически всю информацию из первоначальных документов и не содержащий макросов. Затем следует выйти из Word/Excel, уничтожить все зараженные Word-документы, Excel-таблицы, NORMAL.DOT у Word и все документы/таблицы в StartUp-каталогах Word/Excel. После этого следует запустить Word/Excel и восстановить документы/таблицы из RTF-файлов.

В результате этой процедуры вирус будет удален из системы, а практически вся информация останется без изменений. Однако этот метод имеет ряд недостатков. Основной из них - трудоемкость конвертирования документов и таблиц в RTF-формат, если их число велико. К тому же в случае Excel необходимо отдельно конвертировать все Листы (Sheets) в каждом Excel-файле. Второй недостаток - потеря невирусных макросов, используемых при работе. Поэтому перед запуском описанной процедуры следует

сохранить их исходный текст, а после обезвреживания вируса - восстановить необходимые макросы в первоначальном виде.

Восстановление загрузочных секторов

Восстановление секторов в большинстве случаев является довольно простой операцией и прodelывается при помощи DOS'овской команды SYS (загрузочные сектора дискет и логических дисков винчестера) или командой FDISK/MBR (Master Boot Record винчестера). Можно, конечно же, воспользоваться утилитой FORMAT, однако практически во всех случаях команды SYS вполне достаточно.

Следует иметь в виду, что лечение секторов необходимо производить только при условии отсутствия вируса в оперативной памяти. Если копия вируса в памяти не обезврежена, то вполне вероятно, что вирус повторно заразит дискету или винчестер после того, как код вируса будет удален (даже если воспользоваться утилитой FORMAT).

Будьте также крайне осторожны при использовании FDISK/MBR. Эта команда заново переписывает код программы-загрузчика системы и не изменяет таблицу разбиения диска (Disk Partition Table). FDISK/MBR является 100% лекарством для большинства загрузочных вирусов, однако, если вирус шифрует Disk Partition Table или использует нестандартные способы заражения, FDISK/MBR может привести к полной потере информации на диске. Поэтому перед запуском FDISK/MBR убедитесь в корректности Disk Partition Table. Для этого требуется загрузиться с незараженной DOS-дискеты и проверить корректность этой таблицы (наиболее удобная программа для этой цели - Norton Disk Editor).

Если же восстановление секторов при помощи SYS/FDISK невозможно, то следует разобраться в алгоритме работы вируса, обнаружить на диске первоначальный boot/MBR-сектор и перенести его на законное место (для этого подходят Norton Disk Editor или AVPUTIL). При этом надо постоянно иметь в виду, что при перезаписи системных загрузчиков необходимо соблюдать особую осторожность, поскольку результатом неправильного исправления сектора MBR или boot-сектора может быть потеря всей информации на диске (дисках).

Восстановление файлов

В подавляющем большинстве случаев восстановление зараженных файлов является достаточно сложной процедурой, которую невозможно произвести "руками" без необходимых знаний - форматов выполняемых файлов, языка ассемблера и т.д. К тому же обычно зараженными на диске оказываются сразу несколько десятков или сотен файлов и для их обезвреживания необходимо разработать собственную программу-антивирус (можно также воспользоваться возможностями редактора антивирусных баз из комплекта AVP версий 2.x).

При лечении файлов следует учитывать следующие правила:

необходимо протестировать и вылечить все выполняемые файлы (COM, EXE, SYS, OVL) во всех каталогах всех дисков вне зависимости от атрибутов файлов (т.е. файлы read-only, системные и скрытые);

желательно сохранить неизменными атрибуты и дату последней модификации файла;

необходимо учесть возможность многократного поражения файла вирусом ("бутерброд" из вирусов).

Само лечение файла производится в большинстве случаев одним из нескольких стандартных способов, зависящих от алгоритма размножения вируса. В большинстве случаев это сводится к восстановлению заголовка файла и уменьшению его длины.

Деактивация оперативной памяти

Процедура деактивации памяти, как и лечение зараженных файлов, требует некоторых знаний об операционной системе и обязательного знания азыка Ассемблер.

При решении этих задач не обойтись без дизассемблера или отладчика (например, отладчиков AFD, AVPUTIL, SoftICE, TurboDebugger, дизассемблеров Sourcer или IDA).

И отладчики, и дизассемблеры имеют и положительные и отрицательные черты - каждый выбирает то, что он считает более удобным. Несложные короткие вирусы быстро "вскрываются" стандартным отладчиком DEBUG, при анализе объемных и высокосложных полиморфик-стелс-вирусов не обойтись без дизассемблера. Если необходимо быстро обнаружить метод восстановления пораженных файлов, достаточно пройтись отладчиком по началу вируса до того места, где он восстанавливает загруженную программу перед тем, как передать ей управление (фактически именно этот алгоритм чаще всего используется при лечении вируса). Если же требуется получить детальную картину работы вируса или хорошо документированный листинг, то кроме дизассемблеров Sourcer или IDA с их возможностями восстанавливать перекрестные ссылки, здесь вряд ли что поможет. К тому же следует учитывать, что, во-первых, некоторые вирусы достаточно успешно блокируют попытки протрассировать их коды, а во-вторых, при работе с отладчиком существует ненулевая вероятность того, что вирус вырвется из-под контроля.

При анализе файлового вируса необходимо выяснить, какие файлы (COM, EXE, SYS) поражаются вирусом, в какое место (места) в файле записывается код вируса - в начало, конец или середину файла, в каком объеме возможно восстановление файла (полностью или частично), в каком месте вирус хранит восстанавливаемую информацию.

При анализе загрузочного вируса основной задачей является выяснение адреса (адресов) сектора, в котором вирус сохраняет первоначальный загрузочный сектор (если, конечно, вирус сохраняет его).

Для резидентного вируса требуется также выделить участок кода, создающий резидентную копию вируса и вычислить возможные адреса точек входа в перехватываемые вирусом прерывания. Необходимо также определить, каким образом и где в оперативной памяти вирус выделяет место для своей резидентной копии: записывается ли вирус по фиксированным адресам в системные области DOS и BIOS, уменьшает ли размер памяти, выделенной под DOS (слово по адресу [0000:0413]), создает ли для себя специальный MCB-блок либо использует какой-то другой способ.

Существуют особые случаи, когда анализ вируса может оказаться очень сложной для пользователя задачей, например при анализе полиморфик-вируса. В этом случае лучше обратиться к специалисту по анализу кодов программ.

Для анализа макро-вирусов необходимо получить текст их макросов. Для нешифрованных не-стелс вирусов это достигается при помощи меню Tools/Macro. Если же вирус шифрует свои макросы или использует стелс-приемы, то необходимо воспользоваться специальными утилитами просмотра макросов. Такие специализированные утилиты есть практически у каждой фирмы-производителя антивирусов, однако они являются утилитами "внутреннего пользования" и не распространяются за пределы фирм.

На сегодняшний день известна единственная shareware-программа для просмотра макросов - Perforin. Однако эта утилита пока не поддерживает файлы Office97.