- **Несанкционированная рассылка электронных писем.** Ряд вирусов после заражения компьютера ищут на жестком диске файлы, содержащие электронные адреса (адресная книга) и без ведома пользователя начинают рассылку по ним инфицированных писем.
- **Кража конфиденциальной информации.** Очень часто главной целью вирусной атаки является кража конфиденциальной информации - такой как номера кредитных карт, различные пароли, секретные документы. То есть после инфицирования вирус ищет файлы, содержащие информацию, для кражи которой он предназначен, и передает ее хозяину. Это может происходить путем отправки выбранных данных в электронном сообщении на определенный адрес или прямой пересылки их на удаленный сервер.
- **Несанкционированное использование сетевых ресурсов.** Существуют вирусы, которые после заражения без ведома пользователя подключаются к различным платным службам с использованием личных данных, найденных на компьютере. Впоследствии жертве приходится оплачивать не заказанные ею услуги, а злоумышленник обычно получает процент от этого счета.
- **Удаленное управление компьютером.** После того, как произошло заражение, некоторые вирусы передают своему хозяину инструменты для удаленного управления инфицированным компьютером - открывают бекдоры (от англ. backdoor - черный ход). Обычно это выражается в возможности удаленно запускать размещенные на нем программы, а также загружать из Интернет по желанию злоумышленника любые файлы. Пользователь, чей компьютер заражен вирусом удаленного управления, может ничего и не подозревать. Свое присутствие такие программы обычно выражают только в использовании части ресурсов зараженного компьютера для своих нужд - в основном процессора и оперативной памяти.

- **Ботнеты.** Группа компьютеров, которыми централизованно управляет один злоумышленник, называется ботнетом. Число таких компьютеров в Интернет на сегодняшний день достигает нескольких миллионов и продолжает увеличиваться каждый день.
- **Несанкционированная атака на чужой сервер.** Последнее время вирусописатели используют ботнеты для организации так называемых DoS-атак. DoS (от англ. Denial of Service) - это построенное на принципе отказа в обслуживании нападение на удаленный сайт. Это означает, что каждый инфицированный компьютер периодически (с интервалом обычно порядка 1 секунды) посылает произвольный запрос на получение информации с заданного злоумышленником сайта. Все веб-сайты рассчитаны на определенное число запросов в единицу времени, поэтому резкое увеличение нагрузки практически всегда выводит сервер из строя. Атака, которая производится одновременно с большого количества компьютеров, называется распределенной DoS-атакой или DDoS (от англ. Distributed Denial of Service).
- **Рассылка спама**. Под этим термином обычно понимается ненужная, нежелательная, не запрошенная получателем корреспонденция. Обычно это рассылки рекламного характера. Спам может приходить как по электронной почте, так и в виде других сообщений, например на мобильный телефон в виде SMS. Поскольку электронных адресов в Интернет очень много, рассылка спама занимает много ресурсов. Поэтому злоумышленники часто используют для этих целей ботнеты.

• **Фишинг.** Фактически фишинг - это метод кражи чужой информации. Суть его заключается в подделке известного сайта и рассылке электронных писем-приглашений зайти на него и ввести свою конфиденциальную информацию. Например, создается точная копия сайта какого-либо банка и с помощью спам-технологий рассылается письмо, максимально похожее на настоящее, с уведомлением о сбое в программном обеспечении и просьбой зайти на сайт и заново ввести свои данные. Тут же, в письме приводится адрес сайта - естественно, поддельный, но также максимально похожий на правду.

Существует международная организация, ведущая учет фишинговым инцидентам - Anti-Phishing Working Group (www.antiphishing.org).

• **Уничтожение информации.** Большинство современных вредоносных программ если и несут в себе процедуры уничтожения информации на компьютере-жертве, то только в качестве дополнительной, неосновной функции. Однако для многих пользователей это наиболее явное и болезненное последствие - удаленным и не подлежащим восстановлению может оказаться любой файл на жестком диске, как детские фотографии, так и только что законченная курсовая работа или книга.

• **Мистификации.** Иногда на электронную почту или по другим каналам приходят так называемые предупреждения о новых вирусах. Обычно они содержат призывы не ходить по приведенным ссылкам, проверить свой компьютер на наличие на нем вируса указанным в сообщении методом или предостережение не принимать почту с определенными параметрами. Чаще всего это просто мистификация. Вреда, если не предпринимать указанные действия и не пересылать всем друзьям и знакомым, нет.

Уголовный ко

Написание и распространение вирусов - уголовно наказуемые действия. Как для других преступлений, меры их пресечения регулирует Уголовный Кодекс Российской Федерации. В нем к вирусописателям и распространителям вирусов можно применить ряд статей из главы 28 "Преступления в сфере компьютерной информации":

- Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.
- Статья 146. Нарушение авторских и смежных прав.
- Статья 272. Неправомерный доступ к компьютерной информации.
- Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.
- Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Отдельно стоит отметить, что кроме Уголовного Кодекса РФ существуют меры пресечения, предусмотренные внутренними правилами организации, услуги которой использует пользователь - школы, института, домашней компьютерной сети. Часто встречаются ситуации, когда компьютер становится распространителем вредоносных программ без ведома его хозяина - как например в случае машин-зомби. Однако это не мешает администраторам локальных сетей применять к ним свои внутренние правила и отключать их от сети.

Вирусы

Основная черта компьютерного вируса - это способность к саморазмножению.

Компьютерный вирус- это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Условно жизненный цикл любого компьютерного вируса можно разделить на пять стадий:

- Проникновение на чужой компьютер
- Активация
- Поиск объектов для заражения
- Подготовка копий
- Внедрение копий

Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения - фактически, все каналы, по которым можно скопировать файл. Однако в отличие от червей, вирусы не используют сетевые ресурсы - заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал. Например, скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.

После проникновения следует активация вируса. Это может происходить несколькими путями и в соответствии с выбранным методом вирусы делятся на такие виды:

• **Загрузочные вирусы** заражают загрузочные сектора жестких дисков и мобильных носителей.

• **Файловые вирусы** - заражают файлы. Отдельно по типу среды обитания в этой группе также выделяют:

– **Классические файловые вирусы** - они различными способами внедряются в исполняемые файлы (внедряют свой вредоносный код или полностью их перезаписывают), создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы

– **Макровирусы**, которые написаны на внутреннем языке, так называемых макросах какого-либо приложения. Подавляющее большинство макровирусов используют макросы текстового редактора Microsoft Word

– **Скрипт-вирусы**, написанные в виде скриптов для определенной командной оболочки - например, bat-файлы для DOS или VBS и JS - скрипты для Windows Scripting Host (WSH)

Дополнительным отличием вирусов от других вредоносных программ служит их жесткая привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Это означает, что вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например Unix. Точно также макровирус для Microsoft Word 2003 скорее всего не будет работать в приложении Microsoft Excel 97.

При подготовке своих вирусных копий для маскировки от антивирусов могут применять такие технологии как:

Шифрование - в этом случае вирус состоит из двух частей: сам вирус и шифратор.

Метаморфизм - при применении этого метода вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, обычно ничего не делающих команд.

Соответственно в зависимости от используемых методов вирусы можно делить на шифрованные, метаморфные и полиморфные, использующие комбинацию двух типов маскировки.

Основные цели любого компьютерного вируса - это распространение на другие ресурсы компьютера и выполнение специальных действий при определенных событиях или действиях пользователя (например, 26 числа каждого четного месяца или при перезагрузке компьютера). Специальные действия нередко оказываются вредоносными.

Черви

В отличие от вирусов черви - это вполне самостоятельные программы. Главной их особенностью также является способность к саморазмножению, однако при этом они способны к самостоятельному распространению с использованием сетевых каналов. Для подчеркивания этого свойства иногда используют термин "сетевой червь".

Червь (сетевой червь) - это вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом.

Жизненный цикл червей состоит из таких стадий:

- Проникновение в систему
- Активация
- Поиск объектов для заражения
- Подготовка копий
- Распространение копий

В зависимости от способа проникновения в систему черви делятся на типы:

- **Сетевые черви** используют для распространения локальные сети и Интернет
- **Почтовые черви** - распространяются с помощью почтовых программ
- **IM-черви** используют системы мгновенного обмена сообщениями
- **IRC-черви** распространяются по каналам IRC
- **P2P-черви** - при помощи пиринговых файлообменных сетей

После проникновения на компьютер, червь должен активироваться - иными словами запуститься. По методу активации все черви можно разделить на две большие группы - на тех, которые требуют активного участия пользователя и тех, кто его не требует. На практике это означает, что бывают черви, которым необходимо, чтобы владелец компьютера обратил на них внимание и запустил зараженный файл, но встречаются и такие, которые делают это сами, например, используя ошибки в настройке или бреши в системе безопасности операционной системы. Отличительная особенность червей из первой группы - это использование обманных методов. Это проявляется, например, когда получатель инфицированного файла вводится в заблуждение текстом письма и добровольно открывает вложение с почтовым червем, тем самым его активируя. В последнее время наметилась тенденция к совмещению этих двух технологий - такие черви наиболее опасны и часто вызывают глобальные эпидемии.

Сетевые черви могут кооперироваться с вирусами - такая пара способна самостоятельно распространяться по сети (благодаря червю) и в то же время заражать ресурсы компьютера (функции вируса).

Трояны

Трояны или программы класса троянский конь, в отличие от вирусов и червей, не обязаны уметь размножаться. Это программы, написанные только с одной целью - нанести ущерб целевому компьютеру путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

Троян (троянский конь) - программа, основной целью которой является вредоносное воздействие по отношению к компьютерной системе.

Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы, с целью проникновения в нее. Однако в большинстве случаев они проникают на компьютеры вместе с вирусом либо червем - то есть такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу. Нередко пользователи сами загружают троянские программы из Интернет.

Следовательно, жизненный цикл троянов состоит всего из трех стадий:

- Проникновение в систему
- Активация
- Выполнение вредоносных действий

Как уже говорилось выше, проникать в систему трояны могут двумя путями - самостоятельно и в кооперации с вирусом или сетевым червем. В первом случае обычно используется маскировка, когда троян выдает себя за полезное приложение, которое пользователь самостоятельно копирует себе на диск (например, загружает из Интернет) и запускает. При этом программа действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные трояну.

После проникновения на компьютер, трояну необходима активация и здесь он похож на червя - либо требует активных действий от пользователя или же через уязвимости в программном обеспечении самостоятельно заражает систему.

Поскольку главная цель написания троянов - это производство несанкционированных действий, они классифицируются по типу вредоносной нагрузки:

- **Клавиатурные шпионы**, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору.
- **Похитители паролей** предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат.
- **Утилиты скрытого удаленного управления** - это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Перечень действий, которые позволяет выполнять тот или иной троян, определяется его функциональностью, заложенной автором. Обычно это возможность скрыто загружать, отсылать, запускать или уничтожать файлы. Такие трояны могут быть использованы как для получения конфиденциальной информации, так и для запуска вирусов, уничтожения данных.
- **Анонимные SMTP-сервера и прокси-сервера** - такие трояны на зараженном компьютере организовывают несанкционированную отправку электронной почты, что часто используется для рассылки спама.

- **Утилиты дозвона** в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернет.
- **Модификаторы настроек браузера** меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т. п.
- **Логические бомбы** характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов.

Отдельно стоит отметить, что существуют программы из класса троянов, которые наносят вред другим, удаленным компьютерам и сетям, при этом не нарушая работоспособности инфицированного компьютера. Яркие представители этой группы - организаторы DDoS-атак.

Другие вредоносные программы

Кроме вирусов, червей и троянов существует еще множество других вредоносных программ, для которых нельзя привести общий критерий. Однако среди них можно выделить небольшие группы. Это в первую очередь:

❑ **Условно опасные программы**, то есть такие, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя. К ним относятся:

- **Riskware** - вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями. К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы больших сетей, клиенты IRC, программы для загрузки файлов из Интернет, утилиты восстановления забытых паролей и другие.

• **Рекламные утилиты** (adware) - условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается и программы начинают работать в обычном режиме. Проблема adware кроется в механизмах, которые используются для загрузки рекламы на компьютер. Кроме того, что для этих целей часто используются программы сторонних и не всегда проверенных производителей, даже после регистрации такие модули могут автоматически не удаляться и продолжать свою работу в скрытом режиме. Однако среди adware-программ есть и вполне заслуживающие доверия - например, клиент ICQ.

• **Pornware** - к этому классу относятся утилиты, так или иначе связанные с показом пользователям информации порнографического характера. На сегодняшний день это программы, которые самостоятельно дозваниваются до порнографических телефонных служб, загружают из Интернет порнографические материалы или утилиты, предлагающие услуги по поиску и показу такой информации. Отметим, что к вредоносным программам относятся только те утилиты класса pornware, которые устанавливаются на компьютер пользователя несанкционированно - через уязвимость в операционной системы или браузера или при помощи троянов. Обычно это делается с целью насильственного показа рекламы платных порнографических сайтов или служб.

- **Хакерские утилиты** - К этому виду программ относятся программы скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов), наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit) и другие подобные утилиты. То есть такие специфические программы, которые обычно используют только хакеры.
- **Злые шутки** - программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений о, например, форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений целиком и полностью отражает фантазию автора.

Антивирусы. Общие сведения

В общем случае за обнаружение присутствия вирусов на компьютере должны отвечать антивирусы - специальные программы, способные быстро и эффективно не только обнаруживать, но и обезвреживать вредоносные программы. Однако известно, и тому есть объективные причины, что ни один антивирус не обеспечивает полную защиту от всех вредоносных программ. Следовательно, хоть и маловероятно, но возможно заражение компьютера, даже если на нем установлен антивирус. При отсутствии антивируса, вероятность проникновения на компьютер вредоносных программ многократно возрастает.

Если компьютер заражен неизвестным вирусом, обычной практикой является самостоятельное обнаружение подозрительных файлов и отправка их на исследование в одну или несколько антивирусных компаний, как правило в ту, антивирус которой установлен на компьютере. Там эти файлы анализируют и при выявлении действительно неизвестного вируса или модификации вируса, выпускается обновление антивирусных баз, позволяющее обнаруживать и удалять этот вирус.

Но чтобы отправить подозрительные файлы на анализ, нужно сначала эти файлы найти. А чтобы всерьез заняться поиском, нужно иметь основания для подозрений в том, что компьютер заражен. Для этого нужно знать, какие особенности функционирования компьютера могут быть проявлениями вредоносных программ.

Виды проявлений

Не все вредоносные программы стремятся скрыть свое присутствие на компьютере. Некоторые ведут себя весьма активно: выводят на экран сообщения, открывают страницы веб-сайтов и т. п. Такие проявления логично назвать **явными**.

Другие вредоносные программы специальных сообщений не выводят, но могут провоцировать разного рода сбои в работе компьютера или прикладных программ. Например, одним из признаков попытки проникновения червя Sasser является появление на экране сообщения о сбое в процессе lsass.exe, в результате чего система будет перезагружена (см. рисунок 1).

Рис. 1. Признак заражения червем Sasser

Многие вредоносные программы пытаются отключить или полностью удалить антивирус, другие блокируют доступ к веб-серверам антивирусных компаний, чтобы сделать невозможным обновление антивирусных баз. Соответственно, если антивирус вдруг ни с того, ни с сего перестал запускаться, либо перестали открываться сайты антивирусных компаний при том, что в целом доступ в Интернет работает нормально, это могут быть проявления вирусов. Такого рода проявления будут называться **косвенными**.

Наконец, есть вирусы, которые никак не выдают своего присутствия на компьютере, не выводят сообщений и не конфликтуют с другими приложениями. Их проявления незаметны на первый взгляд и могут состоять в наличии дополнительных процессов в памяти, в сетевой активности, в характерных изменениях системного реестра Windows. Такие проявления будут называться **скрытыми**.

Таким образом проявления вредоносных программ можно условно разбить на три группы по тому, насколько легко их обнаружить:

- **Явные** - вредоносная программа самостоятельно проявляет заметную активность
- **Косвенные** - другие программы начинают выводить сообщения об ошибках или вести себя нестандартно из-за присутствия на компьютере вируса
- **Скрытые** - ни явных ни косвенных проявлений вредоносная программа не имеет

Где искать

Всегда существует вероятность, что наблюдаемый эффект не является результатом действий вируса, а вызван обычными ошибками в используемых программах или же вредоносными скриптами, которые не оставили никаких файлов на компьютере.

Для того чтобы подозрения переросли в уверенность нужно произвести дополнительный поиск скрытых проявлений вредоносных программ, имея конечной целью обнаружение файлов вредоносной программы.

Скрытые проявления включают:

- Наличие в памяти подозрительных процессов
- Наличие на компьютере подозрительных файлов
- Наличие подозрительных ключей в системном реестре Windows
- Подозрительная сетевая активность

Подозрительные процессы

Процесс - это фактически запущенный исполняемый файл. Часть процессов относится к операционной системе, часть к запущенным программам.

Чтобы получить список процессов, нужно вызвать диспетчер задач - стандартное средство Windows для управления процессами. В операционных системах семейства Windows для вызова диспетчера задач нужно нажать комбинацию клавиш **Ctrl + Shift + Esc** или вызвать контекстное меню в системной панели (внизу экрана) и выбрать пункт Диспетчер задач.

На закладке **Процессы** в колонке **Имя образа** содержатся имена файлов, которым соответствуют запущенные процессы. Например, процесс **svchost.exe** отвечает за запуск служб в Windows.

Найти информацию о неизвестном процессе можно в сети Интернет.

Автозапуск

Отличительным признаком большинства червей и многих троянских программ является изменение параметров системы таким образом, чтобы файл вредоносной программы выполнялся автоматически при каждом запуске компьютера. Поэтому наличие незнакомых файлов в списке файлов автозапуска также является поводом для пристального изучения этих файлов.

Наиболее известный источник файлов автозапуска - это папка **Автозагрузка** в меню **Программы**, доступном при нажатии кнопки **Пуск**. Ярлыки, находящиеся в этой папке соответствуют запускаемым программам. Собственно имя запускаемого файла, можно определить через свойства ярлыка.

Однако в связи с тем, что папка **Автозагрузка** известна большинству пользователей, вредоносные программы редко используют ее для автозапуска, предпочитая менее заметные способы.

Системный реестр Windows

Для настройки автозапуска в реестре Windows предназначено несколько ключей:

Первая группа находится в ключе **HKCU\Software\Microsoft\Windows\CurrentVersion**, все ключи, относящиеся к автозагрузке, начинаются с **Run**. Эти программы запускаются только при входе в систему текущего пользователя. В зависимости от операционной системы это могут быть ключи:

- **Run** - основной ключ автозапуска
- **RunOnce** - служебный ключ для программ, которым требуется запуститься только один раз

Другая группа находится в ключе **HKLM\Software\Microsoft\Windows\CurrentVersion**, т. е. в аналогичном ключе, но в настройках, относящихся к компьютеру в целом, а значит, ко всем пользователям. Имена ключей такие же: RunServicesOnce - служебный ключ для служб, которым требуется однократный запуск

- **Run**
- **RunOnce**
- **RunServices**
- **RunServicesOnce**

Стандартными для Windows являются следующие строки запуска:

Имя	Значение
KernelFaultCheck	%systemroot%\system32\dumprep 0 -k
Synchronization Manager	mobsync.exe /logon
LoadPowerProfile	Rundll32.exe powrprof.dll,LoadCurrentPwrScheme
ScanRegistry	C:\WINDOWS\scanregw.exe /autorun
SystemTray	SysTray.Exe
TaskMonitor	C:\WINDOWS\taskmon.exe
CTFMON.EXE	C:\WINDOWS\system32\ctfmon.exe

В зависимости от настроек Windows и установленных программ ключи автозапуска могут содержать множество различных строк для запуска различных программ. Поэтому все на первый взгляд подозрительные файлы нужно перепроверять - они могут оказаться вполне обычными программами.

Ни в коем случае не следует изменять настройки системного реестра наугад - это может привести к полной неработоспособности компьютера и необходимости переустанавливать операционную систему. Вносить изменения в реестр можно только будучи абсолютно уверенным в своих действиях и полностью осознавая характер и последствия производимых модификаций.

Конфигурационные файлы win.ini и system.ini

Настроить автозапуск программ можно и в системных файлах Windows - system.ini и win.ini. Эти файлы используются (преимущественно, использовались) в Windows 3.x, 9x, Me для хранения системных настроек. В Windows NT, 2000, XP аналогичные настройки перенесены в системный реестр, но старые конфигурационные файлы сохранены в целях обеспечения совместимости со старыми же программами.

Конфигурационные файлы win.ini и system.ini разбиты на секции. Название каждой секции заключено в квадратные скобки, например, **[boot]** или **[windows]**.

В файле win.ini строки запуска программ выглядят так:

Load=<строка запуска>

Run=<строка запуска>

Анализируя такие строки можно понять, какие файлы запускаются при старте компьютера.

В файле system.ini есть ровно одна строка, через которую чаще всего запускаются вирусы, расположена в секции [boot]:

shell=<имя программной оболочки Windows>

Во всех версиях Windows стандартной программной оболочкой является explorer.exe. Если в строке **shell=** указано что-то отличное от explorer.exe, это с большой вероятностью вредоносная программа. Справедливости ради, нужно отметить, что существуют легальные программы, являющиеся альтернативными программными оболочками Windows. Такие программы могут изменять значение параметра shell в файле system.ini.

В Windows NT, 2000, XP и 2003 параметры стандартной оболочки задаются в реестре, в ключе HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon в параметре Shell. Значение этого параметра также в подавляющем большинстве случаев должно быть Explorer.exe.

Сетевая активность

Вредоносные программы могут проявляться не только в виде подозрительных процессов или файлов автозапуска, но и в виде сетевой активности. Черви используют сеть для распространения, троянские программы - для загрузки дополнительных компонентов и отсылки информации злоумышленнику.

Некоторые типы троянских программ специально предназначены для обеспечения удаленного управления зараженным компьютером. Для обеспечения доступа к компьютеру по сети со стороны злоумышленника они открывают определенный порт.

Вредоносные программы для приема команд или данных от злоумышленника используют определенный порт, постоянно ожидая сигналов на этот порт. В таких случаях принято говорить, что программа слушает порт.

Определить, какие порты слушаются на компьютере можно при помощи команды **netstat -n**. Для ее выполнения сперва нужно запустить командную оболочку. В случае Windows NT, 2000, XP и 2003 она запускается командой cmd.exe. Для запуска используются команды Выполнить в меню Пуск.

После выполнения в командной [redacted]tat -a в том же окне отображаются данные об установленных соединениях и открытых портах (тех, которые слушаются). Выглядит это как на рисунке 2.

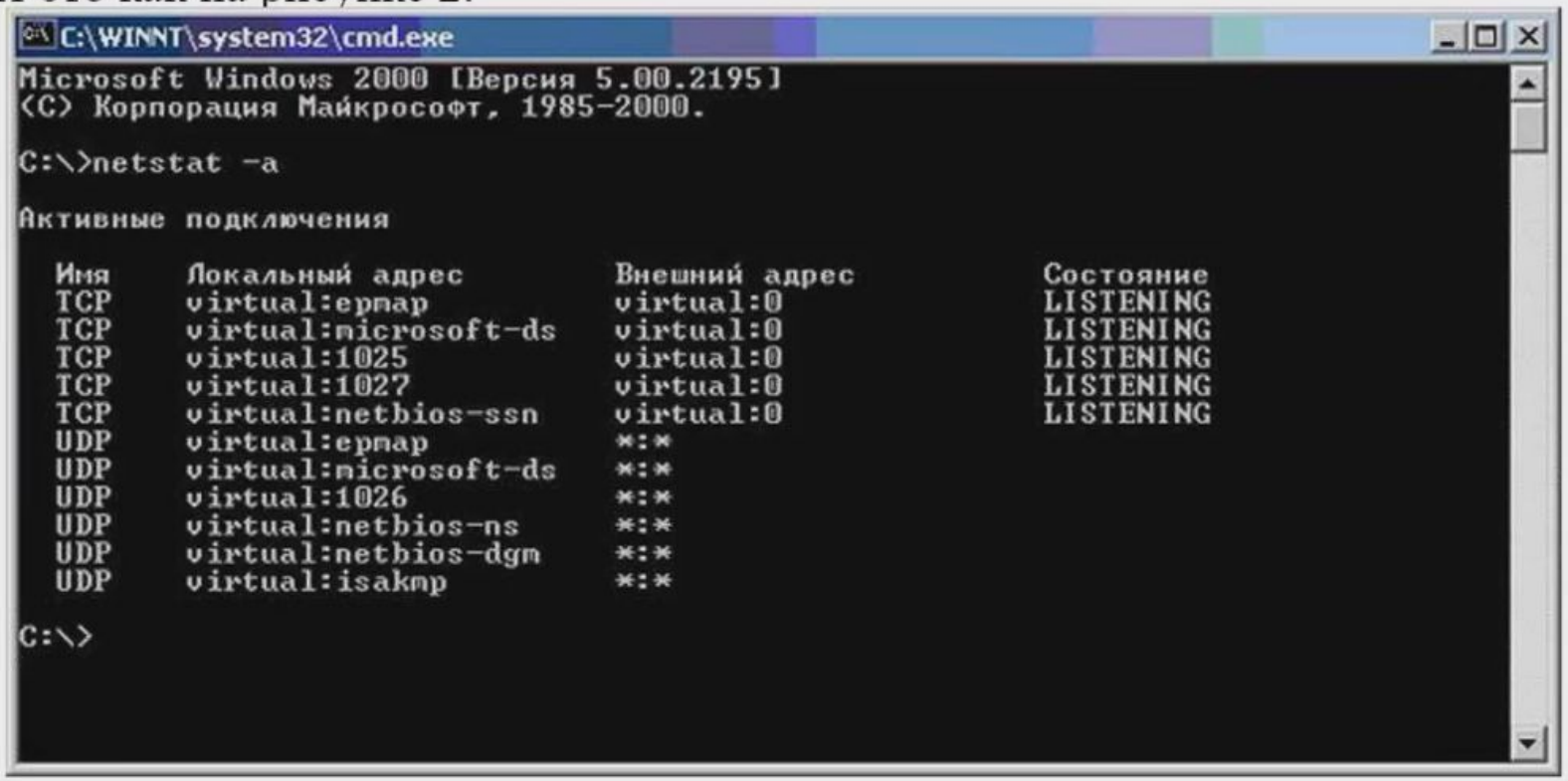

Рис. 2. Команда netstat -a

Результатом выполнения команды является список активных подключений, в который входят установленные соединения и открытые порты. Открытые TCP-порты обозначаются строкой LISTENING в колонке состояние. Часть портов связана с системными службами Windows и отображается не по номеру, а по названию - epmap, microsoft-ds, netbios-ssn. Порты, не относящиеся к стандартным службам, отображаются по номерам.

UDP-порты обозначаются строкой UDP в колонке Имя. Они не могут находиться в разных состояниях, поэтому специальная пометка LISTENING в их отношении не используется. Как и TCP-порты они могут отображаться по именам или по номерам.

Порты, используемые вредоносными программами, чаще всего являются нестандартными и поэтому отображаются согласно их номерам. Впрочем, могут встречаться троянские программы, использующие для маскировки стандартные для других приложений порты, например 80, 21, 443 - порты, используемые на файловых и веб-серверах.

Просто обнаружить неизвестные системе (и пользователю) порты мало. Нужно еще узнать, какие программы используют эти порты. Команда netstat не позволяет этого сделать, поэтому потребуется воспользоваться сторонними утилитами, например, утилитой tcpview.exe. Эта утилита отображает более полную информацию о подключениях, включая данные о процессах, слушающих порты. Характерный вид окна утилиты представлен на рисунке 3.

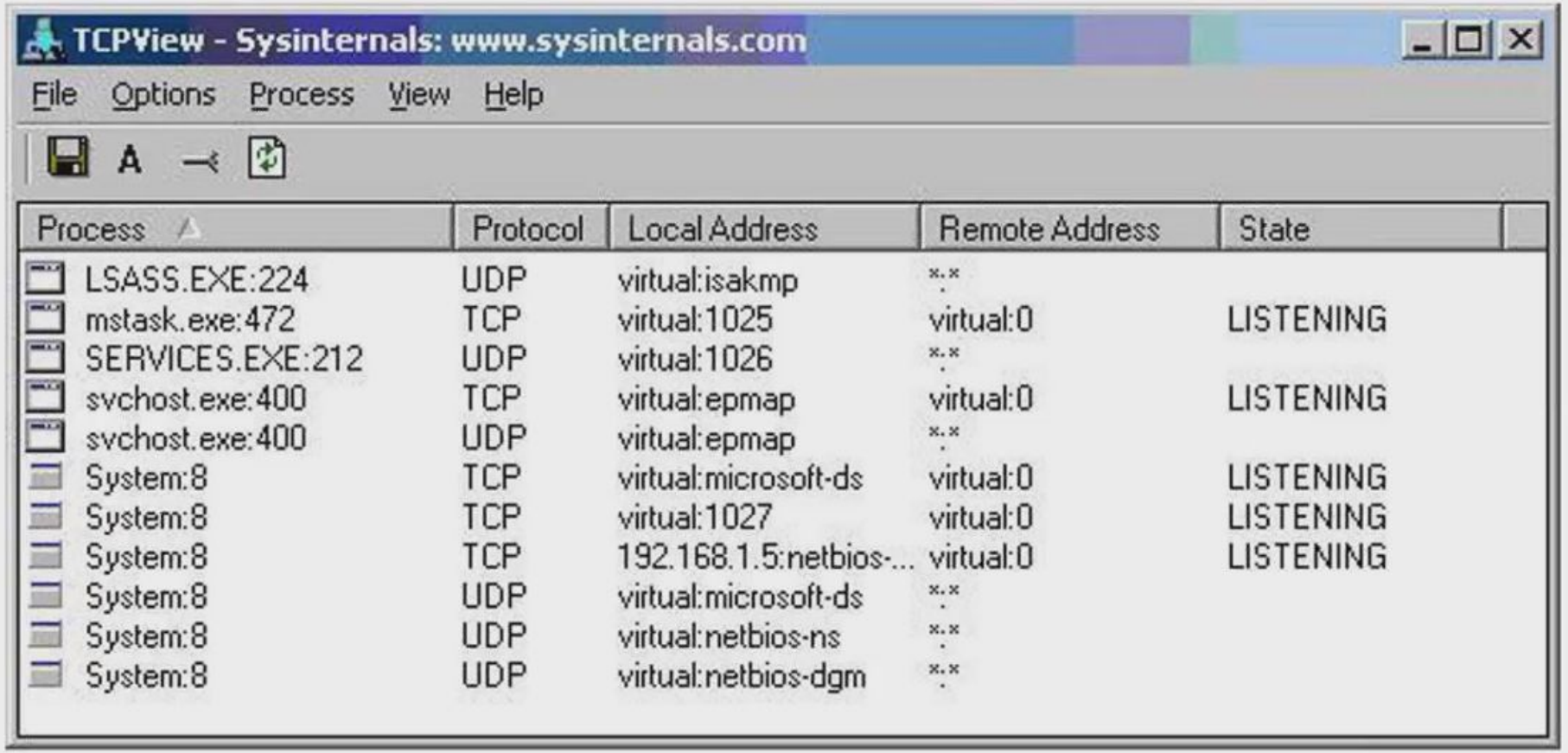

Рис. 3. Утилита tcpview.exe

Методы защиты от вредоносных программ

Для защиты от вредоносных программ нужно использовать антивир Выступающий
Основные причины, по которым антивирус не справился со своей задачей:

- Антивирус был отключен пользователем
- Антивирусные базы были слишком старые
- Были установлены слабые настройки защиты
- Вирус использовал технологию заражения, против которой у антивируса не было средств защиты
- Вирус попал на компьютер раньше, чем был установлен антивирус, и смог обезвредить антивирусное средство
- Это был новый вирус, для которого еще не были выпущены антивирусные базы

В целом можно сделать вывод, что просто наличия установленного антивируса может оказаться недостаточно для полноценной защиты, и что нужно использовать дополнительные методы. Ну а если антивирус на компьютере не установлен, то без дополнительных методов защиты и вовсе не обойтись.

Если взглянуть, на приведенные для примера причины пропуска вируса антивирусом, можно увидеть, что первые три причины связаны с неправильным использованием антивируса, следующие три - с недостатками самого антивируса и работой производителя антивируса. Соответственно и методы защиты делятся на два типа - **организационные и технические**

Организационные м[redacted]ны в первую очередь на пользователя компьютера. Их цель состоит в том, чтобы изменить поведение пользователя, ведь не секрет, что часто вредоносные программы попадают на компьютер из-за необдуманных действий пользователя. Простейший пример организационного метода - разработка правил работы за компьютером, которые должны соблюдать все пользователи.

Технические методы, наоборот, направлены на изменения в компьютерной системе. Большинство технических методов состоит в использовании дополнительных средств защиты, которые расширяют и дополняют возможности антивирусных программ. Такими средствами защиты могут быть:

- Программы, защищающие от атак по сети
- Средства борьбы со спамом
- Исправления, устраняющие "дыры" в операционной системе, через которые могут проникать вирусы

Все вышеперечисленные средства, так или иначе, могут помочь в борьбе с вирусами, но ни одно из них полностью проблему не решает. Далеко не все вирусы распространяются путем атак на сетевые службы и могут быть заблокированы брандмауэрами. Многие вредоносные программы не имеют никакого отношения к электронной почте, а значит антиспамовые фильтры против них бессильны. Какими бы ни были организационные меры, люди их применяющие могут ошибаться.

Поэтому самыми эффективными средствами защиты от вирусов были и остаются специальные программы, способные распознавать и обезвреживать вирусы в файлах, письмах и других объектах. Такие программы называются антивирусами и для того, чтобы построить действительно надежную антивирусную защиту, использовать их нужно обязательно.

Антивирусные программы - это программы, основной задачей которых является защита именно от вирусов, или точнее, от вредоносных программ.

Методы и принципы защиты теоретически не имеют особого значения, главное чтобы они были направлены на борьбу с вредоносными программами. Но на практике дело обстоит несколько иначе: практически любая антивирусная программа объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню.

Из всех методов антивирусной защиты можно выделить две основные группы:

Сигнатурные методы - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов

Эвристические методы - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен

Поиск вирусов, похожих на известные

Если сигнатурный метод основан на выделении характерных признаков вируса и поиске этих признаков в проверяемых файлах, то эвристический анализ основывается на (весьма правдоподобном) предположении, что новые вирусы часто оказываются похожи на какие-либо из уже известных. Постфактум такое предположение оправдывается наличием в антивирусных базах сигнатур для определения не одного, а сразу нескольких вирусов. Основанный на таком предположении эвристический метод заключается в поиске файлов, которые не полностью, но очень близко соответствуют сигнатурам известных вирусов.

Положительным эффектом от использования этого метода является возможность обнаружить новые вирусы еще до того, как для них будут выделены сигнатуры.

Отрицательные стороны:

- Вероятность ошибочно определить наличие в файле вируса, когда на самом деле файл чист - такие события называются ложными срабатываниями
- Невозможность лечения - и в силу возможных ложных срабатываний, и в силу возможного неточного определения типа вируса, попытка лечения может привести к большим потерям информации, чем сам вирус, а это недопустимо
- Низкая эффективность - против действительно новаторских вирусов, вызывающих наиболее масштабные эпидемии, этот вид эвристического анализа малопригоден

Поиск вирусов, выполняющих подозрительные действия

Другой метод, основанный на эвристике, исходит из предположения, что вредоносные программы так или иначе стремятся нанести вред компьютеру. Метод основан на выделении основных вредоносных действий, таких как, например:

- Удаление файла
- Запись в файл
- Запись в определенные области системного реестра
- Открытие порта на прослушивание
- Перехват данных вводимых с клавиатуры
- Рассылка писем
- И др.

Понятно, что выполнение каждого такого действия по отдельности не является поводом считать программу вредоносной. Но если программа последовательно выполняет несколько таких действий, например, записывает запуск себя же в ключ автозапуска системного реестра, перехватывает данные вводимые с клавиатуры и с определенной частотой пересылает эти данные на какой-то адрес в Интернет, значит эта программа по меньшей мере подозрительна. Основанный на этом принципе эвристический анализатор должен постоянно следить за действиями, которые выполняют программы.

Преимуществом описанного метода является возможность обнаруживать неизвестные ранее вредоносные программы, даже если они не очень похожи на уже известные. Например, новая вредоносная программа может использовать для проникновения на компьютер новую уязвимость, но после этого начинает выполнять уже привычные вредоносные действия. Такую программу может пропустить эвристический анализатор первого типа, но вполне может обнаружить анализатор второго типа.

Отрицательные черты те же, что и раньше:

- Ложные срабатывания
- Невозможность лечения
- Невысокая эффективность

Дополнительные [redacted]

Практически любой антивирус сегодня использует все известные методы обнаружения вирусов. Но одних средств обнаружения мало для успешной работы антивируса, для того, чтобы чисто антивирусные средства были эффективными, нужны дополнительные модули, выполняющие вспомогательные функции.

Модуль обновления

В первую очередь, каждый антивирус должен содержать модуль обновления. Это связано с тем, что основным методом обнаружения вирусов сегодня является сигнатурный анализ, который полагается на использование антивирусной базы. Для того чтобы сигнатурный анализ эффективно справлялся с самыми последними вирусами, антивирусные эксперты постоянно анализируют образцы новых вирусов и выпускают для них сигнатуры. После этого главной проблемой становится доставка сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу.

Именно эту задачу и решает модуль обновления. После того, как эксперты создают новые сигнатуры, файлы с сигнатурами размещаются на серверах компании - производителя антивируса и становятся доступными для загрузки. Модуль обновления обращается к этим серверам, определяет наличие новых файлов, загружает их на компьютер пользователя и дает команду антивирусным модулям использовать новые файлы сигнатур.

Модули обновления разных антивирусов весьма похожи друг на друга и отличаются типами серверов, с которых они могут загружать файлы обновлений, а точнее, типами протоколов, которые они могут использовать при загрузке - HTTP, FTP, протоколы локальных Windows-сетей. Некоторые антивирусные компании создают специальные протоколы для загрузки своих обновлений антивирусной базы. В таком случае модуль обновления может использовать и этот специальный протокол.

Второе, в чем могут отличаться модули обновления - это настройка действий, на случай, если источник обновлений недоступен. Например, в некоторых модулях обновления можно указать не один адрес сервера с обновлениями, а адреса нескольких серверов, и модуль обновления будет обращаться к ним по очереди, пока не обнаружит работающий сервер. Или же в модуле обновления может быть настройка - повторять попытки обновления с заданным интервалом определенное количество раз или же до тех пор, пока сервер не станет доступным. Эти две настройки могут присутствовать и одновременно.

Модуль планирования

Второй важный вспомогательный модуль - это модуль планирования. Существует ряд действий, которые антивирус должен выполнять регулярно: в частности, проверять весь компьютер на наличие вирусов и обновлять антивирусную базу. Модуль планирования как раз и позволяет настроить периодичность выполнения этих действий.

Для обновления антивирусной базы рекомендуется использовать небольшой интервал - один час или три часа, в зависимости от возможностей канала доступа в Интернет. В настоящее время новые модификации вредоносных программ обнаруживаются постоянно, что вынуждает антивирусные компании выпускать новые файлы сигнатур буквально каждый час. Если пользователь компьютера много времени проводит в Интернете, он подвергает свой компьютер большому риску и поэтому должен обновлять антивирусную базу как можно чаще.

Полную проверку компьютера нужно проводить хотя бы потому, что сначала появляются новые вредоносные программы, а только потом сигнатуры к ним, а значит всегда есть возможность загрузить на компьютер вредоносную программу раньше, чем обновление антивирусных баз. Чтобы обнаружить эти вредоносные программы, компьютер нужно периодически перепроверять. Разумным расписанием для проверки компьютера можно считать раз в неделю.

Исходя из сказанного, основная задача модуля планирования - давать возможность выбрать для каждого действия расписание, которое больше всего подходит именно для этого типа действия. Следовательно модуль обновления должен поддерживать много различных вариантов расписания из которых можно было бы выбирать.

Модуль управления

По мере увеличения количества модулей в антивирусе возникает необходимость в дополнительном модуле для управления и настройки. В простейшем случае - это общий интерфейсный модуль, при помощи которого можно в удобной форме получить доступ к наиболее важным функциям:

- Настройке параметров антивирусных модулей
- Настройке обновлений
- Настройке периодического запуска обновления и проверки
- Запуску модулей вручную, по требованию пользователя
- Отчетам о проверке
- Другим функциям, в зависимости от конкретного антивируса

Основные требования к такому модулю - удобный доступ к настройкам, интуитивная понятность, подробная справочная система, описывающая каждую настройку, возможность защитить настройки от изменений, если за компьютером работает несколько человек. Подобным модулем управления обладают все антивирусы для домашнего использования. Антивирусы для защиты компьютеров в крупных сетях должны обладать несколько иными свойствами.

В большой организации за настройку и правильное функционирование антивирусов отвечают не пользователи компьютеров, а специальные сотрудники. Если компьютеров в организации много, то каждому ответственному за безопасность сотруднику придется постоянно бегать от одного компьютера к другому, проверяя правильность настройки и просматривая историю обнаруженных заражений. Это очень неэффективный подход к обслуживанию системы безопасности.

Поэтому, чтобы упростить работу администраторов антивирусной безопасности, антивирусы, которые используются для защиты больших сетей, оборудованы специальным модулем управления. Основные свойства этого модуля управления:

Поддержка удаленного управления и настройки - администратор безопасности может запускать и останавливать антивирусные модули, а также менять их настройки по сети, не вставая со своего места

Защита настроек от изменений - модуль управления не позволяет локальному пользователю изменять настройки или останавливать антивирус, чтобы пользователь не мог ослабить антивирусную защиту организации

Это далеко не все требования к управлению антивирусной защитой в крупной организации, а только основные принципы.

Карантин

Среди прочих вспомогательных средств во многих антивирусах есть специальные технологии, которые защищают от возможной потери данных в результате действий антивируса.

Например, легко представить ситуацию, при которой файл детектируется как возможно зараженный эвристическим анализатором и удаляется согласно настройкам антивируса. Однако эвристический анализатор никогда не дает стопроцентной гарантии того, что файл действительно заражен, а значит с определенной вероятностью антивирус мог удалить незараженный файл.

Или же антивирус обнаруживает важный документ зараженный вирусом и пытается согласно настройкам выполнить лечение, но по каким-то причинам происходит сбой и вместе с вылеченным вирусом теряется важная информация.

Разумеется, от таких случаев желательно застраховаться. Проще всего это сделать, если перед лечением или удалением файлов сохранить их резервные копии, тогда если окажется, что файл был удален ошибочно или была потеряна важная информация, всегда можно будет выполнить восстановление из резервной копии.

Тестирование работы антивируса

После того как антивирус установлен и настроен, каждый пользователь хочет убедиться, что он все сделал правильно и антивирусная защита работает. Но как это проверить? Первое, что приходит в голову: взять где-нибудь зараженный файл и посмотреть поймает ли его антивирус. Но, как и у многих простых решений, у этого есть ряд очевидных недостатков:

Зараженный файл не так-то просто найти. Даже если воспользоваться поиском в Интернете и найти какие-то файлы, нет никакой гарантии, что они действительно заражены. Т. е. если антивирус обнаружит в них вирусы, значит они заражены, а антивирус работает, но если не обнаружит, то неизвестно - антивирус не работает, или файлы не заражены

Использовать для тестирования настоящие вирусы крайне опасно. Если пользователь все же ошибся и неправильно выполнил установку или настройку антивируса, в процессе тестирования он может на самом деле заразить свой компьютер, в результате чего потерять данные или стать источником заражения для других компьютеров.

Значит нужен такой способ тестирования антивирусов, который был бы безопасным, но давал четкий ответ на вопрос, корректно ли работает антивирус. Понимая важность проблемы, организация EICAR при участии антивирусных компаний создала специальный тестовый файл, который был назван по имени организации - eicar.com.

Eicar.com - это исполняемый файл в COM-формате, который не выполняет никаких вредоносных действий, а просто выводит на экран строку "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!". Тем не менее, все антивирусные компании договорились включить этот файл в свои антивирусные базы и детектировать его как вирус, специально чтобы пользователи могли без риска протестировать свою антивирусную защиту.

Получить eicar.com можно на сайте организации EICAR по адресу http://www.eicar.org/anti_virus_test_file.htm, но проще создать этот файл самому. Дело в том, что машинный код файла eicar.com состоит из печатных символов и его можно создать при помощи любого текстового редактора. Например, можно воспользоваться стандартным для операционных систем Windows редактором Notepad. В окне Notepad нужно набрать строку

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* сохранить файл под именем **eicar.com**, и все - тестовый файл готов.

Созданный описанным способом файл eicar.com ничем не отличается от доступного на сайте организации EICAR, можно загрузить и убедиться самому. Его можно пытаться скопировать на защищенную машину, запускать на ней или же просто проверять, чтобы проверить работу антивируса в разных режимах.

Тестирование антивируса при помощи eicar.com тоже не идеально. Концепция тестового файла и сам тестовый файл, разрабатывались в начале 90-х годов, когда едва ли не единственным типом вредоносных программ были файловые вирусы. Поэтому eicar.com в первую очередь позволяет протестировать, как антивирус справляется с файловыми вирусами и близкими по структуре вредоносными программами - большинством троянов, некоторыми червями.

Однако сейчас разнообразие вредоносных программ гораздо больше. И соответственно больше антивирусных модулей, предназначенных для защиты от различных угроз. Например, во многих антивирусах имеется специальный модуль защиты от скрипт-вирусов, а поскольку eicar.com скрипт-вирусом не является, он непригоден для тестирования таких модулей. Точно так же eicar.com непригоден для тестирования специальных модулей для защиты от макровирусов. К сожалению, на сегодняшний день новых способов тестирования антивирусных средств, которые поддерживались бы всеми производителями антивирусов нет, и приходится полагаться на старые способы.

Режимы работы антивирусов

Надежность антивирусной защиты обеспечивается не только способностью отражать любые вирусные атаки. Другое не менее важное свойство защиты - ее непрерывность. Это означает, что антивирус должен начинать работу по возможности до того, как вирусы смогут заразить только что включенный компьютер и выключаться только после завершения работы всех программ. Однако с другой стороны, пользователь должен иметь возможность в любой момент запросить максимум ресурсов компьютера для решения своей, прикладной задачи и антивирусная защита не должна ему помешать это сделать. Оптимальный выход в этой ситуации - это введение двух различных режимов работы антивирусных средств: один с небольшой функциональностью, но работающий постоянно, и второй - тщательная и более ресурсоемкая проверка на наличие вирусов по запросу пользователя. Такое разделение принято в большинстве современных антивирусов.

Проверка по требованию

В некоторых случаях наличия постоянно работающей проверки в режиме реального времени может быть недостаточно. Возможна ситуация, когда на компьютер был скопирован зараженный файл, исключенный из постоянной проверки ввиду больших размеров и, следовательно, вирус в нем обнаружен не был. Если этот файл на рассматриваемом компьютере запускаться не будет, то вирус может остаться незамеченным и проявить себя только после пересылки его на другой компьютер, что может сильно повредить репутации отправителя - распространителя вирусов. Для исключения подобных случаев используется второй режим работы антивируса - проверка по требованию.

Для такого режима обычно предполагается, что пользователь лично укажет какие файлы, каталоги или области диска необходимо проверить и время, когда нужно произвести такую проверку - в виде расписания или разового запуска вручную. Обычно рекомендуется проверять все чужие внешние носители информации, такие как дискеты, компакт диски, flash-накопители каждый раз перед чтением информации с них, а также весь свой жесткий диск не реже одного раза в неделю.

Проверка по требованию

В некоторых случаях наличия постоянно работающей проверки в режиме реального времени может быть недостаточно. Возможна ситуация, когда на компьютер был скопирован зараженный файл, исключенный из постоянной проверки ввиду больших размеров и, следовательно, вирус в нем обнаружен не был. Если этот файл на рассматриваемом компьютере запускаться не будет, то вирус может остаться незамеченным и проявить себя только после пересылки его на другой компьютер, что может сильно повредить репутации отправителя - распространителя вирусов. Для исключения подобных случаев используется второй режим работы антивируса - проверка по требованию.

Для такого режима обычно предполагается, что пользователь лично укажет какие файлы, каталоги или области диска необходимо проверить и время, когда нужно произвести такую проверку - в виде расписания или разового запуска вручную. Обычно рекомендуется проверять все чужие внешние носители информации, такие как дискеты, компакт диски, flash-накопители каждый раз перед чтением информации с них, а также весь свой жесткий диск не реже одного раза в неделю.

Антивирусные комплексы

Второй способ оптимизации работы антивируса - это создание различных его версий для компьютеров, служащих разным целям. Зачастую они отличаются лишь наличием тех или иных специфических модулей и различием в интерфейсе, в то время как непосредственно антивирусная проверка осуществляется одной и той же подпрограммой, называемой антивирусным ядром.

Антивирусный комплекс - набор антивирусов, использующих одинаковое антивирусное ядро или ядра, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем. В антивирусный комплекс также в обязательном порядке входят средства обновления антивирусных баз

Всякая локальная сеть, как правило, содержит компьютеры двух типов - рабочие станции, за которыми непосредственно сидят люди, и сетевые серверы, используемые для служебных целей.

Рабочие станции - это компьютеры локальной сети, за которыми непосредственно работают пользователи. Главной задачей комплекса для защиты рабочих станций является обеспечение безопасной работы на рассматриваемом компьютере - для этого необходима проверка в режиме реального времени, проверка по требованию и проверка локальной электронной почты.

Сетевые сервера- это компьютеры, специально выделенные для хранения или обработки информации. Они обычно не используются для непосредственной работы за ними и поэтому в отличие от рабочих станций проверка электронной почты на наличие вирусов тут не нужна. Следовательно, антивирусный комплекс для файловых серверов должен производить проверку в режиме реального времени и проверку по требованию.

Антивирусный комплекс для защиты почтовых систем предназначен для проверки всех проходящих электронных писем на наличие в них вирусов. То есть проверять другие файлы, размещенные на этом компьютере, он не обязан (для этого существует комплекс для защиты сетевых серверов). Поэтому к нему предъявляются требования по наличию собственно программы для проверки всей принимаемой и отправляемой почтовой корреспонденции в режиме реального времени, и дополнительно механизма проверки по требованию почтовых баз данных.

Аналогично в соответствии со своим назначением, антивирусный комплекс для шлюза осуществляет только проверку проходящих через шлюз данных.

Поскольку все вышеперечисленные комплексы используют сигнатурный анализ, то в обязательном порядке в них должно входить средство для поддержания антивирусных баз в актуальном состоянии, то есть механизм их обновления. Дополнительно часто оказывается полезным модуль для удаленного централизованного управления, который позволяет системному администратору со своего рабочего места настраивать параметры работы антивируса, запускать проверку по требованию и обновление антивирусных баз.

Уровни антивирусной защиты

Для инфицирования системы вирусом необходимо наличие каналов связи с другими компьютерами. Причем чем их больше и чем менее они защищены, тем выше вероятность заражения. Таким образом, архитектура системы антивирусной защиты сильно зависит от функции рассматриваемого компьютера, а именно от присутствующих у него каналов связи с окружающим миром. Поскольку именно по этим характеристикам выше было введено разделение сети на сегменты, то удобно выделить и соответствующие уровни антивирусной защиты:

- Уровень защиты рабочих станций и сетевых серверов
- Уровень защиты почтовых серверов
- Уровень защиты шлюзов

В этой классификации на каждый почтовый сервер могут быть установлены одновременно программы, реализующие уровень защиты рабочих станций и сетевых серверов и программы, относящиеся к уровню защиты почтовых серверов. Аналогично дело обстоит и со шлюзами - программное обеспечение уровня рабочих станций и сетевых серверов и уровня защиты шлюзов.

Уровень защиты рабочих станций и сетевых серверов

Уровень защиты рабочих станций и сетевых серверов - самый обширный. Он охватывает все компьютеры локальной сети и служит самым последним оплотом на пути проникновения вредоносных программ. Даже если где-то в системе антивирусной защиты случился прокол и одна машина все же оказалась заражена, установленные на остальных компьютерах антивирусные программы должны предотвратить дальнейшее распространение эпидемии по сети. На этом уровне используются антивирусные комплексы для защиты рабочих станций и сетевых серверов.

Защита рабочих станций и сетевых серверов ответственна в первую очередь за чистоту файловой системы каждого из компьютеров сети. Следовательно, она в обязательном порядке должна содержать постоянную проверку как механизм предотвращения заражения системы вирусами, проверку по требованию - процедуру для тщательной ревизии рассматриваемой машины и нейтрализации проникших на нее вредоносных программ, и модуль для поддержания вирусных сигнатур в актуальном состоянии. Дополнительно, для рабочих станций накладывается требование к наличию процедур проверки почтовых сообщений.

Рассматриваемые здесь рабочие станции в разрезе антивирусной защиты отличаются от домашних компьютеров в первую очередь политикой антивирусной безопасности, принятой в организации, которой принадлежит сеть, и обязательной для соблюдения всеми пользователями. Обычной практикой служит введение отдельной должности системного администратора, который обязан следить за состоянием компьютерной техники. При этом остальные пользователи часто не имеют прав на доступ к ряду критических для функционирования сети программ, пусть даже установленных на их компьютере. Программное обеспечение, ответственное за антивирусную безопасность, относится именно к таким.

Наличие десятков, сотен, а иногда и тысяч компьютеров, объединенных в одну локальную сеть требует немалых затрат для администрирования каждого из них. Для того чтобы это было по силам сделать сравнительно малочисленной группе администраторов, применяются различные специальные программы и утилиты для централизованного удаленного управления. С их помощью администратор может не вставая из-за своего компьютера одновременно управлять и настраивать программы на удаленных компьютерах и подчиненных ему других элементах сети.

Следовательно, к антивирусному комплексу для защиты рабочих станций и сетевых серверов предъявляется дополнительное требование - наличие в его составе программного средства для удаленного централизованного управления локальными приложениями.

Уровень защиты почты

Защита почты - это вторая ступень в антивирусной защите сети. Она служит для уменьшения нагрузки и увеличения надежности системы защиты рабочих станций и сетевых серверов. Дополнительно антивирусная проверка почты, а именно исходящей корреспонденции, в случае одиночного вирусного инцидента внутри сети послужит преградой для распространения этого вируса на другие, внешние, компьютеры. В системе защиты этого уровня используется комплекс для защиты почтовых систем.

В общем случае почтовым сервером называется компьютер, на котором установлена и успешно функционирует программа по обработке почты. Почтовый сервер относится к серверной группе, а не к рабочим станциям. Это объясняется тем, что его главное предназначение состоит в обеспечении работы почтовой системы, а не в решении локальных прикладных задач. Таким образом, почтовый сервер фактически представляет собой хранилище информации (электронных писем) для других сетевых пользователей.

Почтовая программа осуществляет передачу электронных писем от одного компьютера к другому.

На почтовом сервере формируется очередь из еще не отосланных и еще неполученных писем, а также полностью или частично хранится входящая корреспонденция.

Следовательно, антивирусная проверка должна включать в себя как проверку всех проходящих через почтовую программу потоков, так и хранилища электронных писем.

Поэтому антивирусный комплекс для защиты почты должен содержать:

- Антивирусную проверку в режиме реального времени проходящей через почтовую систему корреспонденции
- Антивирусную проверку в режиме реального времени файлов, запрашиваемых пользователями из своих почтовых ящиков
- Антивирусную проверку по требованию для хранимых на сервере файлов почтового формата, а именно информации в ящиках пользователей
- Средство для обновления антивирусных баз

Уровень защиты шлюзов

В большинстве случаев антивирусная защита на уровне шлюза играет вспомогательную роль в общей системе антивирусной безопасности сети. Это происходит потому, что задача такого антивирусного комплекса - только проверка поступающей извне информации на наличие в ней вредоносных программ. Однако даже если вирус проникнет сквозь шлюз, заразить ни один компьютер ему не удастся: его перехватит антивирус на локальной машине, а в случае инфицированного почтового сообщения - он будет остановлен еще на почтовом сервере.

Однако такой сценарий реализуется только при исправно и бесперебойно работающей системе антивирусной защиты сети, в частности на уровне защиты рабочих станций и сетевых серверов. На практике же часто встречаются сбои. Причем чем больше локальная сеть, тем больше вероятность, что такой инцидент может случиться. Несмотря на то, что распределенная система защиты рабочих станций и сетевых серверов не даст в любом случае такому вирусу распространиться далее по сети и он будет локализован на одной инфицированной машине, это все равно не очень хорошо, потому что на ней тоже могут храниться очень важные документы и при отсутствии защиты шлюза вирус сможет, например, произвести несанкционированную рассылку или позволить злоумышленнику похитить конфиденциальную информацию.

Поэтому антивирусная защита шлюза позволяет существенно увеличить надежность антивирусной защиты в целом.

Дополнительно, в случае вирусной эпидемии в Интернет, именно система защиты шлюза прореагирует и уведомит администратора первой, что позволит ему оперативно принять меры по повышению уровня защиты, например, провести срочное внеочередное обновление антивирусных баз или даже отключить отдельные особо важные или секретные компьютеры от сети.

Аналогично защите почты, на уровне защиты шлюза используется антивирусный комплекс для защиты шлюзов. Он отвечает только за проверку проходящих через него данных, а за чистоту файловой системы ответственен комплекс по защите сетевых серверов. Поэтому программный комплекс для защиты шлюзов должен содержать только фильтры для проходящих через него потоков. Обычно это HTTP, FTP и SMTP.

Централизованное управление антивирусной защитой

Как уже упоминалось выше, для локальной сети, насчитывающей десятки или больше компьютеров, использование системы удаленного централизованного управления антивирусной защитой оказывается очень полезным. Она позволяет администратору не вставая из-за своего рабочего места обслуживать все входящие в его ведение рабочие станции и сетевые сервера: удаленно настраивать политики антивирусной безопасности, запускать проверку объектов на наличие в них вирусов, включать или выключать постоянную защиту, централизованно обновлять антивирусные базы, разрешать или запрещать пользователям самим менять какие-либо настройки, в том числе позволять или не позволять им видеть, что на компьютере вообще установлен и работает антивирус. Однако главное преимущество использования такой системы - это возможность тотального контроля за вирусной активностью и состоянием антивирусной защиты в сети, быстрого обнаружения и оперативного устранения всех вирусных инцидентов.

Логическая сеть

Ситуация, когда один администратор управляет антивирусной защитой всех без исключения входящих в локальную сеть компьютеров, встречается очень редко. Это происходит потому, что обычно есть ряд машин, содержащих особо конфиденциальную информацию и нуждающихся в индивидуальном подходе (например, личный компьютер директора) или целые отделы, не имеющими физической связи с остальной локальной сетью (обычно так устроены финансовые и другие департаменты, работающие с секретными данными).

Поэтому в отношении системы удаленного администрирования употребляется термин **логической сети**, под которым понимается **группа компьютеров, управление антивирусной защитой которых может вестись из одного источника**.

Таким образом, если в организации, которой принадлежит локальная сеть, есть несколько связанных только через Интернет филиалов, то управление антивирусной защитой может осуществляться полностью централизованно одним администратором или же может быть разбито на отдельные сегменты. Часто в больших компаниях можно встретить смешанный вариант - вся локальная сеть разбита на связанные между собой подсети разных масштабов и за каждой из них следит отдельный человек, но существует главный администратор, который может со своего рабочего места в любой момент вмешаться в работу своих подчиненных и взять управление на себя.

Компоненты

Система удаленного централизованного управления обычно состоит из таких отдельных программных компонентов:

- **Клиентской антивирусной программы**, то есть антивирусного комплекса для рабочих станций или сетевых серверов.
- **Сервера администрирования** - так называется программа, которая собирает, обрабатывает и хранит все настройки, информацию обо всех событиях и инцидентах, имевших место в сети, рассылает уведомления и отчеты. Для полноценного функционирования необходима база данных для хранения всей собранной информации. Сервер администрирования и база данных могут устанавливаться как на отдельном выделенном для этого компьютере, так и на рабочем месте администратора, на одной машине или на разных.
- **Агента администрирования**, который устанавливается на все компьютеры, входящие в логическую сеть системы антивирусной защиты. Его задача - обеспечить связь клиентской программы с сервером администрирования и оперативно передать ему информацию о состоянии антивирусной защиты на этой машине, получить новые антивирусные базы или другие указания и команды.
- **Консоли администрирования**, устанавливаемой на рабочем месте администратора. Это небольшая программа, которая позволяет в приятном и удобном виде вывести данные с сервера администрирования, на их основе построить графики и диаграммы, создать отчеты, произвести настройку клиентских компьютеров, удаленно запустить проверку или обновить антивирусные базы одновременно на нескольких машинах. Возможности той или иной консоли полностью зависят от заложенных в нее фирмой-производителем функций.