Антивирусная защита компьютерных систем

История компьютерных вирусов, классификация вирусов, признаки присутствия вирусов в компьютере, основы работы антивирусных программ.

Понятие вредоносной программы

- **Компьютерная программа**- *это последовательность инструкций (команд) для выполнения компьютером определенных действий. Программы записываются при помощи специальных языков программирования или машинного кода. Примеры компьютерных программ - программа чтения и записи данных на дискету, программа воспроизведения музыки с диска, записная книжка в мобильном телефоне, Microsoft Word.*

Вызов компьютерной программы, то есть запуск программы на выполнение, производится путем последовательной загрузки содержимого соответствующего ей файла в оперативную память, после чего компьютер начинает выполнять последовательность заложенных в эту программу действий.

Запустить программу можно также непрямым методом. Например, при доступе к любому файлу, содержащему текстовую информацию, должна запускаться программа, позволяющая его прочесть.

- **Вредоносная программа (код)** - *это программа, наносящая какой-либо вред компьютеру, на котором она запускается, или другим подключенным к нему компьютерам.*

Одним из способов для вредоносной программы оставаться незамеченной на компьютере является дописывание своего кода к файлу другой известной программы. При этом возможно: 1) полное перезаписывание файлов (в этом случае вредоносная программа обнаруживает себя при первом же запуске, поскольку ожидаемые действия полностью заменены), 2) внедрение в начало, середину или конец файла.

Пример. CIH - вирус, который в ходе заражения записывает свои копии во все запускаемые пользователем программные файлы (PE EXE). Внедрение может происходить как одним куском, так и путем деления вредоносного кода на блоки и записи их в разных частях заражаемого файла. При этом инфицированная программа может дальше выполнять свои основные функции и вирус в ней никак себя не обнаруживает. Однако в определенный момент времени происходит уничтожение всей информации на жестком диске.

Уголовная ответственность за распространение вирусов

Написание и распространение вирусов - уголовно наказуемые действия. Как и 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 146. Нарушение авторских и смежных прав.**
- **Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.**
- **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.**

Можно отметить, что кроме Уголовного Кодекса РФ существуют меры пресечения, предусмотренные внутренними правилами организаций. Часто встречаются ситуации, когда компьютер становится распространителем вредоносных программ без ведома его хозяина - как в примере с машинами-зомби. В этом случае, администратор локальной сети может применить к ним свои внутренние правила и отключить их от сети.

Пути распространения компьютерных вирусов

- **МОБИЛЬНЫЕ НОСИТЕЛИ**

К мобильным носителям можно отнести все виды энергонезависимых ПЗУ. То есть таких устройств, которые позволяют достаточно долго хранить информацию и при этом не требуют дополнительного питания от компьютера. Это дискеты, компакт диски, flash-накопители и др.

С помощью мобильных носителей распространение компьютерных вирусов происходит достаточно просто. Например, с компьютера А нужно перенести на компьютер Б файл. При этом компьютер А заражен вирусом. В процессе записи пользователь обращается к файлу и передает его программе, которая непосредственно производит запись на носитель. Даже если переносимый файл не был заражен ранее, инфицирование возможно на каждом из этапов копирования - при доступе, при чтении, при записи. Таким образом, на носитель записывается уже зараженный файл. После того, как файл будет скопирован на компьютер Б, компьютер окажется заражен. То есть в итоге вирусом будут инфицированы оба компьютера и носитель, который остается источником заражения для других компьютеров, на которых он будет прочтен.

Мобильные носители - достаточно распространенный способ для размножения компьютерных вирусов. Однако по скорости распространения этот путь существенно уступает компьютерным сетям.

- **КОМПЬЮТЕРНЫЕ СЕТИ**

Для удобства обмена информацией между компьютерами, их объединяют в компьютерные сети. Любые два компьютера, относящиеся к одной компьютерной сети, могут обмениваться данными без участия мобильных носителей - с помощью сетевых проводов, телефона, кабельного телевидения, радио или других технологий беспроводной связи. В большинстве случаев это существенно ускоряет и упрощает процедуру обмена файлами. Компьютерные сети могут быть локальными и глобальными.

- **Локальная вычислительная сеть** (ЛВС) - *это компьютерная сеть, покрывающая относительно небольшую территорию - дом, школу, предприятие, микрорайон.*

На входящих в компьютерную сеть компьютерах часто организовывается открытый доступ к отдельным или даже всем хранимым на них файлам. Это означает, что пользователь, работающий на одном компьютере, входящем в ЛВС, может открывать, читать, изменять и запускать файлы, физически расположенные на другом компьютере. Нередко выделяется специальный компьютер, выполняющий функцию хранилища файлов - файловый сервер. Главная его задача - обеспечивать доступ к хранимым на нем данным для всех компьютеров этой сети.

Вредоносные программы в полной мере используют преимущества ЛВС - фактически, почти все современные вирусы имеют встроенные процедуры инфицирования по локальным сетям и как следствие высокие темпы распространения.

Инфицирование обычно происходит в такой последовательности. Зараженный компьютер с заданным интервалом инициирует соединение поочередно со всеми другими компьютерами сети и проверяет наличие на них открытых для общего доступа файлов. Если такие есть, происходит инфицирование.

- **Глобальная вычислительная сеть** (ГВС) - *это компьютерная сеть, покрывающая большие территории - города, страны, континенты.*

Самая большая и самая известная на сегодняшний день глобальная вычислительная сеть - это всемирная сеть Интернет.

Наличие сети такого масштаба делает возможным всемирные эпидемии компьютерных вирусов.

Пример. 30 апреля 2004 года были обнаружены первые экземпляры вируса Sasser - в течение дня им было атаковано около 4 тысяч компьютеров, что вызвало серьезные сбои в работе таких компаний как Postbank, Delta Air Lines, Goldman Sachs. Впоследствии было поражено более 8 млн. компьютеров, а убытки от Sasser были оценены в 979 млн. долларов США.

- **Электронная почта** - *это способ передачи информации в компьютерных сетях, основанный на пересылке пакетов данных, называемых электронными письмами.*

Электронное письмо представляет собой файл с набором обязательных параметров: электронные адреса отправителя и получателя, заголовок, тело письма и некоторые другие служебные данные. Заголовок письма иногда также называют темой - обычно это фраза, отражающая общий смысл письма, например "С Новым годом!". Основной текст сообщения указывается в его теле и если кроме него необходимо переслать файлы, их прикрепляют к письму - совокупность таких файлов называется вложением.

На сегодняшний день электронная почта выступает основным путем распространения вирусов. Это происходит потому, что время доставки письма очень мало (обычно исчисляется минутами) и практически все пользователи Интернет имеют как минимум один почтовый ящик. При этом для того, чтобы доставить пользователю на компьютер зараженный файл, достаточно прислать на его электронный адрес инфицированное письмо и заставить адресата его открыть.

Создатели вирусов для ослабления бдительности нередко в параметрах письма в качестве отправителя указывают адрес, очень похожий на настоящий, или завлекающий текст в теме.

Пример. LoveLetter в мае 2000 года в течение всего нескольких часов заразил миллионы компьютеров по всему миру. Такому успеху способствовала удачно выбранная тема, интригующий текст и имя вложенного файла - "ILOVEYOU", и "LOVE-LETTER-FOR-YOU.TXT.vbs. После заражения происходила кража конфиденциальной информации и искажение содержимого некоторых файлов на жестком диске.

Уязвимости и заплаты операционной системы

В большинстве операционных систем существует возможность указать прикладные программы, которые необходимо всегда запускать после завершения загрузки операционной системы. Это удобно в таких случаях как запуск почтовых, антивирусных и др. программ, которые пользователь использует очень часто.

Однако наличие автозагрузки дает возможность вредоносным вирусам практически незаметно выполнять свои функции. Для этого во время заражения в список автозагрузки добавляется ссылка на программу, которая загружает вирус в оперативную память при каждой загрузке операционной системы. То есть фактически активация вируса происходит без участия пользователя при каждом включении компьютера.

- **Уязвимость** *(или брешь в системе безопасности) - это место в программном коде, которое теоретически или реально может быть использовано для несанкционированного доступа к управлению программой.*

Любая программа представляет собой написанную программистом последовательность действий, переведенную в машинный код. Как любой человек, программист может допустить ошибку или могут появиться новые технологии, и старая программа в ряде ситуаций будет вести себя не так как планировалось.

После обнаружения уязвимости, производители программ обычно стараются как можно скорее выпустить дополнения, которые бы исправляли исходный код и закрывали брешь.

- **Заплата** *или* **патч** *(от англ. patch - латать, ставить заплаты) - это программный код, используемый для модификации используемой программы.*

Если фирмой-производителем используемой программы был выпущен пакет обновлений к ней, настоятельно рекомендуется его установить.

Пример. В январе 2003 года началась эпидемия Slammer, заражающего сервера под управлением операционной системы Microsoft SQL Server 2000. Вирус использовал брешь в системе безопасности SQL Server, заплата к которой вышла в июле 2002. После проникновения Slammer начинал в бесконечном цикле посылать свой код на случайно выбранные адреса в сети - только за первые 10 минут было поражено около 90% (120 000 единиц) всех уязвимых серверов, при этом пять из тринадцати главных серверов Интернет вышли из строя.

Последствия заражений компьютерными вирусами

Последствия инфицирования компьютера вредоносной программой могут быть как явными, так и неявными.

К неявным обычно относят заражения программами, которые по своей сути являются вирусами, однако из-за ошибок в своем коде или нестандартному программному обеспечению целевого компьютера, вредоносную нагрузку выполнить не могут. При этом свое присутствие в системе они никак не выражают.

Разнообразие явных последствий с ростом числа вирусов постоянно увеличивается. Можно выделить следующие основные:

- **Несанкционированная рассылка электронных писем.** Ряд вирусов после заражения компьютера ищут на жестком диске файлы, содержащие электронные адреса 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. В этом случае 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.

Пример. Dialer - после попадания на компьютер, этот вирус начинал дозвон на международные телефонные номера для подключения к платным сервисам. Через некоторое время пользователю приходил огромный телефонный счет и доказать в подавляющем большинстве случаев что он никуда не звонил не представлялось возможным.

- **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. Свое присутствие такие программы обычно выражают только в использовании части ресурсов зараженного компьютера для своих нужд - в основном процессора и оперативной памяти. Пользователь, чей компьютер заражен вирусом удаленного управления, может ничего и не подозревать. Такие компьютеры часто называют машинами-зомби.
- **Ботнеты.** Группа компьютеров, которыми централизованно управляет один злоумышленник. Число таких компьютеров в Интернет на сегодняшний день достигает нескольких миллионов и продолжает увеличиваться каждый день.

Пример. Bagle - вирус, распространяющийся в виде вложения в электронные письма. После заражения он копирует себя на жесткий диск под именем *bbeagle.exe* и регистрирует этот файл в автозапуске операционной системы. Далее происходят попытки соединиться с несколькими удаленными серверами. В результате автор получил огромную сеть подконтрольных ему компьютеров. Bagle-ботнет - одна из самых масштабных и известных сетей машин-зомби.

- **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).

Пример.Одна из самых известных DDoS-атак была предпринята в июле 2001 года. Объектом нападения стал веб-сайт Белого дома в США (*www.whitehouse.gov*). В атаке участвовало около 12000 (по другим данным - до 200000) компьютеров, зараженных во время прошедшей незадолго до этого эпидемии вирусом CodeRed.

- **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.
- **Уничтожение информации.** Большинство современных вредоносных программ если и несут в себе процедуры уничтожения информации на компьютере-жертве, то только в качестве дополнительной, не основной 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.

Пример. В апреле 2004 года произошла массовая рассылка предупреждения о якобы опасном вирусе, основным признаком присутствия которого на компьютерах под управлением операционной системы Microsoft Windows заявлялось наличие файла jdbgmgr.exe, который и содержит саму вредоносную программу. В действительности же этот файл является стандартной программой, входящей в большинство версий Microsoft Windows. Удаление или изменение содержимого *jdbgmgr.exe* влечет непредсказуемые последствия в работоспособности операционной системы.

Классификация вирусов

Все вредоносные программы в соответствии со способами распространения и вредоносной нагрузкой можно разделить на четыре основные типа - компьютерные вирусы, черви, трояны и другие программы.

- **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.*

Основная черта компьютерного вируса - это способность к саморазмножению, поэтому условно жизненный цикл любого компьютерного вируса можно разделить на пять стадий:

1. Проникновение на чужой компьютер
2. Активация
3. Поиск объектов для заражения
4. Подготовка копий
5. Внедрение копий

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.

В соответствии с выбранным методом активации 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

При подготовке своих вирусных копий для маскировки от антивирусов могут применяться 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.

- **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 стадий, подобных вирусам, но в отличие от вирусов черви - это вполне самостоятельные программы. Стадии жизненного цикла червя:

1. Проникновение в систему
2. Активация
3. Поиск объектов для заражения
4. Подготовка копий
5. Распространение копий

После проникновения на компьютер, червь должен активироваться, т.е. быть запущенным к исполнению. 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).

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

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.

Жизненный цикл троянов состоит из трех стадий:

1. Проникновение в систему
2. Активация
3. Выполнение вредоносных действий

Способы проникновения в компьютер троянов следующие:

- некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы, с целью проникновения в нее;
- в большинстве случаев троянские программы проникают на компьютеры вместе с вирусом либо червем, такие трояны можно рассматривать как дополнительную вредоносную нагрузку;
- маскировка, когда троян выдает себя за полезное приложение, которое пользователь самостоятельно копирует себе на диск (например, загружает из Интернет) и запускает. При этом сама программа действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные трояну.

Можно отдельно 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.

Классификация троянов 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.

- **Другие вредоносные программы**

Кроме вирусов, червей и троянов существует еще множество других вредоносных программ, для которых нельзя привести общий критерий. Их можно объединить в следующие небольшие группы:

- **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 ним относятся утилиты удаленного управления, 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 в том, что для рекламных 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.
  - **Pornware** - к этому классу относятся утилиты, так или иначе связанные с показом пользователям информации порнографического характера, которые самостоятельно дозваниваются до порнографических телефонных служб, загружают из Интернет порнографические материалы или утилиты, предлагающие услуги по поиску и показу такой информации. К вредоносным программам относятся 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.
- **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.

Признаки присутствия на компьютере вредоносных программ

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

- **Явные** - вредоносная программа самостоятельно проявляет заметную активность;

Некоторые вирусы ведут себя весьма активно: выводят на экран сообщения, открывают страницы веб-сайтов и т. п. Изменение стартовой страницы браузера, изменение стандартной страницы поиска, несанкционированное открытие новых окон, ведущих на определенные сайты - все это может быть следствием выполнение вредоносного скрипта на одном из посещенных сайтов. В таком случае новые программы на компьютер не проникают, а настройки браузера можно восстановить. Если же после восстановления настроек они снова меняются при следующем запуске браузера или после перезагрузки компьютера, значит причина изменений - наличие на компьютере вредоносной программы.

После установки в системе троянская или рекламная программа выводит на экран сообщения о том, что на компьютере обнаружены вредоносные или рекламные программы. В силу того, что эти сообщения замаскированы под стандартные служебные сообщения Windows, пользователь не всегда догадывается, что это результат работы вредоносных программ и в результате попадает на те же рекламные или вредоносные сайты

Не так давно получили распространения особые вредоносные программы - утилиты дозвона. Эти утилиты без санкции пользователя и игнорируя настройки пытаются установить модемное соединение с Интернетом через дорогую телефонную линию или дорогого провайдера. Признаком заражения может быть несанкционированные попытки компьютера соединиться с Интернетом по модему.

- **Косвенные** - другие программы начинают выводить сообщения об ошибках или вести себя нестандартно из-за присутствия на компьютере вируса;

Многие вредоносные программы небезуспешно пытаются выгрузить антивирус из памяти или даже удалить файлы антивируса с дисков компьютера. Поэтому внезапное завершение работы антивируса вполне может являться поводом для беспокойства.

Некоторые вредоносные программы нейтрализуют возможность обновления антивирусных средств. В среднем, пользователи не часто заходят на сайты антивирусных компаний, а сообщения антивируса о невозможности обновиться могут списывать на проблемы у провайдера или на самих серверах обновления. Таким образом вирус может длительное время оставаться незамеченным.

Вирусы могут быть причиной сбоев в работе 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.

Другой пример, троянская программа Backdoor.NTHack, результатом присутствия которой на компьютере может быть сообщение об ошибке, возникающее при загрузке компьютера:
STOP 0xC000021A {Fatal System Error} The Windows Logon Process terminated unexpectedly.

Если компьютер заражен и рассылает инфицированные почтовые сообщения, они могут быть обнаружены на одном из серверов в Интернете и антивирус на сервере может отправить уведомление отправителю зараженного сообщения. Следовательно, косвенным признаком присутствия вируса может быть получение почтового сообщения о том, что с почтового адреса пользователя компьютера был отправлен вирус.

Признак заражения червем Sasser

- **Скрытые** - ни явных ни косвенных проявлений вредоносная программа не имеет.

В отсутствие явных или косвенных проявлений о присутствии вируса можно судить, например, по необычной сетевой активности, когда ни одно сетевое приложение не запущено, а значок сетевого соединения сигнализирует об обмене данными. Другими признаками могут служить незнакомые процессы в памяти или файлы на диске.

Скрытые проявления включают:

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

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.

Системный реестр Windows - это основное хранилище большинства настроек операционной системы и многих приложений. Для доступа к системному реестру используется системная утилита regedit.exe, расположенная в папке операционной системы.

На верхнем уровне реестр делится на несколько веток (пять или шесть, в зависимости от версии Windows). С точки зрения автозапуска наиболее важны две ветки:

1. HKEY_CURRENT_USER - ветка ключей, относящихся к текущему пользователю, часто сокращенно обозначается как HKCU
2. HKEY_LOCAL_MACHINE - ветка ключей, относящихся к компьютеру в целом, сокращается до HKLM

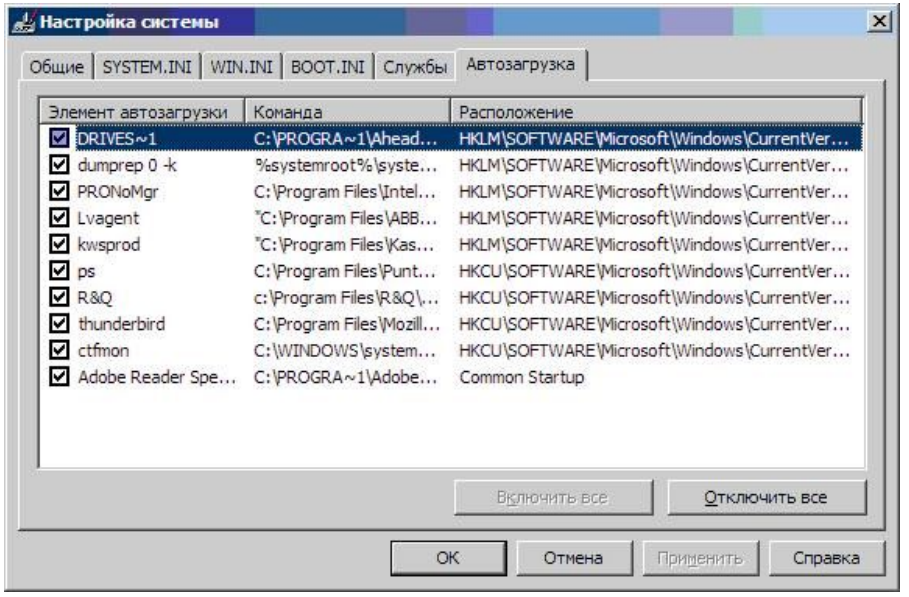
<u>Ни в коем случае не следует изменять настройки системного реестра наугад - это может привести к полной неработоспособности компьютера и необходимости переустанавливать операционную систему.</u>

Для настройки автозапуска в реестре Windows предназначено несколько ключей:

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

Настроить автозапуск программ можно и в системных файлах Windows - system.ini и win.ini. В файле win.ini строки запуска программ выглядят так: **Load**=<строка загрузки>; **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**=<explorer.exe>. Если в строке **shell=** указано что-то отличное от explorer.exe, это с большой вероятностью вредоносная программа.

Для получения обобщенной информации об автоматически запускаемых приложениях, можно воспользоваться системной утилитой msconfig.exe. Эта утилита входит в состав Windows 98, Me, XP и 2003 и предоставляет сводную информацию обо всех источниках объектов автозапуска.



На закладке Автозагрузка собраны данные о запускаемых программах из реестра и меню Пуск. В колонке Элемент автозагрузки приводится имя записи в реестре или имя ярлыка в меню Пуск. В колонке Команда – строка запуска программы, в колонке Расположение - ключ реестра, в котором расположена соответствующая запись, или Common Startup - для ярлыков меню Пуск. win.ini расположены на одноименных закладках. Кроме этого имеется закладка Службы, содержащая информацию о запускаемых службах в Windows XP. Службы отвечают, например, за вывод на печать, за обнаружение новых устройств, а обеспечение сетевого взаимодействия компьютеров и т. п. Но в качестве служб могут регистрироваться и некоторые вредоносные программы.

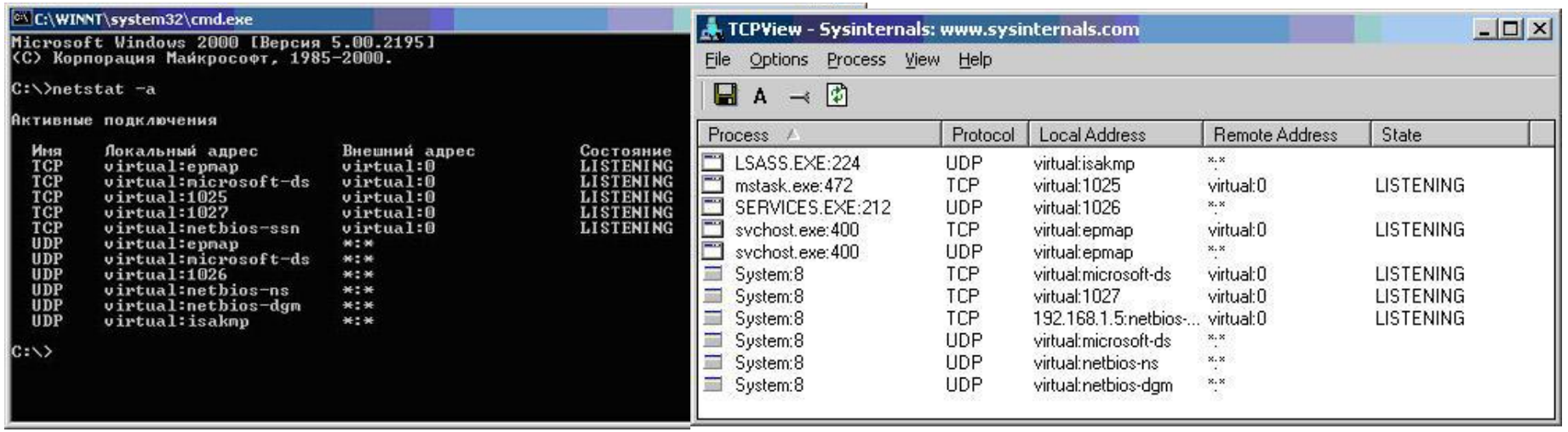
Сетевая активность

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. Для обеспечения доступа к компьютеру по сети со стороны злоумышленника они открывают определенный порт.

Обнаружить неизвестные системе (и пользователю) порты и узнать, какие программы используют эти порты можно воспользовавшись сторонними утилитами, например, утилитой tcpview.exe. Эта утилита отображает полную информацию о подключениях, включая данные о процессах, слушающих порты. Характерный вид окна утилиты показан на рисунке.

Определить, какие порты слушаются на компьютере можно при помощи команды netstat -a. Для запуска используется команда Выполнить в меню Пуск.

Результатом выполнения команды является список активных подключений, в который входят установленные соединения и открытые порты. Открытые TCP-порты обозначаются строкой LISTENING в колонке состояние. 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 (если они связаны с системными службами Windows) или по номерам.



Что делать с результатами поиска?

Итак, по результатам анализа процессов, параметров автозагрузки и соединений получен список подозрительных с точки зрения пользователя процессов (имен файлов). Для неопытного пользователя неизвестных, а значит подозрительных имен файлов может оказаться слишком много, поэтому имеет смысл выделить наиболее подозрительные из них - те, которые были обнаружены в двух и более источниках. Например, файлы, которые присутствуют в списке процессов и в списке автозагрузки. Еще более подозрительными являются процессы, обнаруженные в автозагрузке и слушающие порты.

Для выяснения природы подозрительных процессов проще всего использовать Интернет. В глобальной сети имеются сайты, собирающие информацию о различных процессах. Данных по всем процессам вредоносных программ на таких сайтах может и не быть, но во всяком случае на них есть информация о большом количестве неопасных процессов и таким образом можно будет исключить из списка те процессы, которые относятся к операционной системе или известным не вредоносным программам. Одним из таких сайтов является http://www.processlibrary.com.

После того, как список подозрительных процессов максимально сужен и в нем остались только те, о которых нет исчерпывающей и достоверной информации, остается последний шаг, найти эти файлы на диске и отправить на исследование в одну из антивирусных компаний для анализа.

Методы защиты от вредоносных программ

- **Организационные методы**

Самым простым примером организационных методов защиты от вирусов является выработка и соблюдение определенных правил обработки информации.

- ***Правила обработки информации***
  - Не открывать почтовые сообщения от незнакомых отправителей
  - Проверять сменные накопители (дискеты, компакт-диски, flash-накопители) на наличие вирусов перед использованием
  - Проверять на наличие вирусов файлы, загружаемые из Интернет
  - Работая в Интернет, не соглашаться на непрошенные предложения загрузить файл или установить программу
- ***Правила использования программ***
  - Следить за тем, чтобы программы, обеспечивающие защиту, были постоянно запущены, и чтобы функции защиты были активированы
  - Регулярно обновлять антивирусные базы
  - Регулярно устанавливать исправления операционной системы и часто используемых программ. Не менять настройки по умолчанию программ, обеспечивающих защиту, без необходимости и полного понимания сути изменений

- **Технические методы**

- ***Обновления***

Для загрузки и установки обновлений в большинстве программ и систем есть встроенные средства. Например, в Windows XP имеется специальный компонент Автоматическое обновление, параметры работы которого настраиваются в окне Свойства системы, доступном через панель управления

- ***Брандмауэры***

Брандмауэр - это программа, которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил.

Из популярных операционных систем, встроенный брандмауэр имеется в Windows XP. Окно настройки его параметров можно вызвать из панели управления

Для более удобной работы, а также на тех операционных системах, где встроенного брандмауэра нет, используются программы-брандмауэры других производителей, например Kaspersky Anti-Hacker, Agnitum Outpost Firewall, ZoneAlarm и другие.

- ***Средства защиты от нежелательной корреспонденции***

Для фильтрации нежелательной почты в антиспамовых фильтрах применяется несколько методов:

- Черные и белые списки адресов.
- Базы данных образцов спама.
- Самообучение.
- Анализ служебных заголовков.

Основы работы антивирусных программ

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.

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**

  Основанный на предположении, что новые вирусы часто оказываются похожи на какие-либо из уже известных, эвристический метод заключается в поиске файлов, которые не полностью, но очень близко соответствуют сигнатурам известных вирусов.
  - **Поиск вирусов, выполняющих подозрительные действия**

  Метод основан на выделении основных вредоносных действий, таких как, удаление файла, запись в файл, запись в определенные области системного реестра, открытие порта на прослушивание, перехват данных вводимых с клавиатуры, рассылка писем и др.
  - **Карантин**

  Специальная технология, которая защищает от возможной потери данных в результате действий антивируса. Перед лечением или удалением файлов сохраняются их резервные копии, тогда в случае ошибочно удаления файла и потери важной информации, всегда можно выполнить восстановление из резервной копии.
- Тестирование работы антивируса

Тестирование антивирусов, должно быть безопасным, но при этом давать 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. В окне Notepad нужно набрать сл. строку и сохранить по именем eicar.com

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*