ЧАСТЬ 4. ВРЕДОНОСТНЫЕ ПРОГРАММЫ

13. ВРЕДОНОСТНЫЕ ПРОГРАММЫ И КОМПЬЮТЕРНЫЕ ВИРУСЫ

13.1 Основные понятия

Для хранения информации на любом компьютере используются два вида памяти - постоянные запоминающие устройства (ПЗУ) и постоянные запоминающие устройства (ПЗУ). К первому типу относятся жесткие диски (винчестеры), дискеты, CD-ROM и другие мобильные носители информации, ко второму - оперативная память, то есть микросхема в системном блоке. Поэтому ПЗУ также называют внешней долговременной памятью, а ОЗУ - внутренней. Главное отличие оперативной памяти от внешней состоит в том, что информация, записанная на ОЗУ, может храниться только во время работы компьютера, при выключении или перезагрузке она теряется. Как следствие, большинство устройств ПЗУ предназначены для хранения значительно большего объема информации, чем оперативная память.

Для организации хранилища информации на ПЗУ используются файлы.

Файл *- это логический блок информации, хранимой на носителях информации.* Файл обязательно имеет имя и может содержать произвольный объем информации. Максимальная длина имени и максимальный объем файла определяются файловой системой.

Файловая система *- это совокупность правил, определяющих систему хранения информации*: различные атрибуты файлов, такие как максимальная длина имени, максимальный допустимый размер файла. Примеры файловых систем - FAT, FAT32, NTFS, EXT2, ISO9660.

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.

Передача программе пользовательских данных может осуществляться с помощью графического интерфейса, командной строки, конфигурационного файла или косвенно через другие программы.

Конфигурационный файл *представляет собой текстовый файл с последовательным перечнем данных и команд, которые необходимо передать программе.* При взаимодействии же двух программ между собой пользователь как правило явного участия не принимает.

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, то есть преобразовывающая машинный код, содержащийся в текстовом файле, в буквы, которые пользователь прочитает на экране.

Таким образом, практически все программы помимо основных функций, выполняют ряд дополнительных, служебных действий, не видимых обычному пользователю.

Вредоносная программа *- 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 как полное перезаписывание файлов (но в этом случае вредоносная программа обнаруживает себя при первом же запуске, поскольку ожидаемые действия полностью заменены), так и 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. Поскольку самая известная версия CIH срабатывала 26 апреля, то он получил второе имя - «Чернобыль».

13.2 Способы распространения вредоносных программ

В настоящее время имеется четыре основных способа передачи вредоносного ПО.

1. 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, перфокарты и перфоленты.

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

2. Локальная вычислительная сеть *(ЛВС)*[2)] *- это компьютерная сеть, покрывающая относительно небольшую территорию* (дом, школу, институт, микрорайон).

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.

3. 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.

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

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, не нужно его принуждать куда-либо обратиться и скопировать к себе вирус. Достаточно лишь прислать на его электронный адрес инфицированное письмо и заставить адресата его открыть. Часто для инфицирования даже не требуется запускать вложение - существуют методы, позволяющие заражать даже при обычном прочтении письма.

Пример 1. Horillka распространяется через Интернет в виде файлов, прикрепленных к зараженным письмам с такими параметрами: заголовок - «Внимание!», текст: «Выпущено новое vbs обновление для поиска вирусов в памяти ОС Windows! Оно помогает бороться с вирусами, рассылающимися по почте. Антивирусный модуль написан на скрипт-языке, что помогает перехватывать vb и js вирусы, прежде чем они начнут деструктивную деятельность. Достаточно открыть файл и программа по устранению вирусов проведет поиск вредоносных программ в памяти компьютера». Во вложении находится файл с именем «WinSys32dll.vbs», после его запуска происходит заражение компьютера. Как результат, 11 декабря каждого года на экран

выдается сообщение «COOOOOOOOL» и после следующей перезагрузки уничтожаются все данные на жестком диске C.

Пример 2. 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», «kindly check the attached LOVELETTER coming from me» и «LOVE-LETTER-FOR-YOU.TXT.vbs. После заражения происходила кража конфиденциальной информации и искажение содержимого некоторых файлов на жестком диске.

13.3 Операционная система. Уязвимости и заплаты

Все программы можно разделить на два типа - прикладные и системные.

Прикладное программное обеспечение *(прикладные программы) - это программы, предназначенные для выполнения определенных пользовательских задач и рассчитанные на непосредственное взаимодействие с пользователем.* Прикладные программы часто называют приложениями.

Системное программное обеспечение *используется для обеспечения работы компьютера самого по себе и выполнения прикладных программ.*

В персональном компьютере под прикладными программами понимаются различные текстовые редакторы, игры, почтовые программы, электронные словари. Роль базового системного программного обеспечения играет операционная система.

Операционная система *(ОС) - это комплекс программ, который обеспечивает управление физическими устройствами компьютера, доступ к файлам, ввод и вывод данных, выполнение и взаимодействие пользовательских программ.* 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. Уязвимости могут появляться как в системном, так и в прикладном программном обеспечении.*

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.*

Другими словами заплата - это дополнительная программа, которую следует запустить на выполнение, если в уже используемой программе обнаружилась ошибка или уязвимость. При этом часто можно устанавливать патч без удаления основной программы и даже без завершения ее работы - в первую очередь это касается операционных систем.

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 еще 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.

13.4 Последствия заражений вредоносной программой

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

***К неявным последствиям 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.*

Класс явных последствий постоянно увеличивается. К ним можно отнести:

***1. 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.*

Пример. Sircam рассылал себя с зараженных компьютеров в виде файлов, вложенных в письма электронной почты. Для этого случайным образом на жестком диске выбирался файл, к которому прикреплялся вирусный код (дописывался в конец файла). Таким образом отсылаемые письма содержали вложение, состоящее из двух частей: вирус и файл-приманку. Имя вложения формировалось на основе выбранного файла - например, если исходный файл назывался photos.zip, то имя вложения было - photos.zip.pif, photos.zip.lnk, photos.zip.bat или photos.zip.com. Адреса получателей выбирались из найденных на зараженном компьютере, а текст писем составлялся так, чтобы внушить как можно меньше подозрений и заставить адресата запустить полученный файл. Побочным эффектом такого способа распространения является утечка с зараженного компьютера конфиденциальных документов.

2. Кража конфиденциальной информации. *После инфицирования вирус ищет файлы, содержащие конфиденциальную информацию (номера кредитных карт, различные пароли, секретные документы), 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.

3. 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.

4. 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. Такие компьютеры часто называют машинами-зомби.

5. 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.

Пример. Bagle - вирус, распространяющийся в виде вложения в электронные письма. Адрес отправителя и имя вложения - произвольные, тема - «Hi», текст - «Test =)». 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. При этом злоумышленнику предоставляется возможность загружать на зараженный компьютер любые файлы и запускать их на выполнение. Первый вирус из этой серии, Bagle.a, был обнаружен 18 января 2004, однако по замыслу автора уже через 10 дней он перестал размножаться и вскоре появились новые, более совершенные

модификации Bagle. В результате автор получил огромную сеть подконтрольных ему компьютеров. Bagle-ботнет - одна из самых масштабных и известных сетей машин-зомби.

6. 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 вируса CodeRed.

7. Рассылка спама*. Под этим термином обычно понимается ненужная, нежелательная, не запрошенная получателем корреспонденция.* 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.

8. Фишинг. *Фактически фишинг - это метод кражи чужой информации, суть которого 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).

9. 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.

10. 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.

13.5 Классификация вредоностных программ

Все вредоносные программы в соответствии со способами распространения и вредоносной нагрузкой можно разделить на четыре основные типа:

- *компьютерные вирусы,*
- *черви,*
- *трояны*
- *другие программы.*

Рассмотрим основные особенности указанных типов подробнее.

13.5.1 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.

В соответствии с выбранным методом активации вирусы делятся на следующие виды:

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

Примеры. Вредоносная программа Virus.Boot.Snow.a записывает свой код в MBR жесткого диска или в загрузочные сектора дискет. При этом оригинальные загрузочные сектора шифруются вирусом. После получения управления вирус остается в памяти компьютера (резидентность) и перехватывает прерывания INT 10h, 1Ch и 13h. Иногда вирус проявляет себя визуальным эффектом - на экране компьютера начинает падать снег.

Другой загрузочный вирус Virus.Boot.DiskFiller также заражает MBR винчестера или загрузочные сектора дискет, остается в памяти и перехватывает прерывания - INT 13h, 1Ch и 21h. При этом, заражая дискеты, вирус форматирует дополнительную дорожку с номером 40 или 80 (в зависимости от объема дискеты он может иметь 40 либо 80 дорожек с номерами 0-39 или 0-79 соответственно). Именно на эту нестандартную дорожку вне поля обычной видимости вирус записывает свой код, добавляя в загрузочный сектор лишь небольшой фрагмент - головную часть вируса.

2. Файловые вирусы *- заражают файлы. Отдельно* ***по типу среды обитания в этой группе также выделяют следующие типы****.*

2.1 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.*

Пример. Самый известный файловый вирус всех времен и народов — Virus.Win9x.CIH, известный также как «Чернобыль». Имея небольшой размер - около 1 кб - вирус заражает PE-файлы (Portable Executable) на

компьютерах под управлением операционных систем Windows 95/98 таким образом, что размер зараженных файлов не меняется. Для достижения этого эффекта вирус ищет в файлах «пустые» участки, возникающие из-за выравнивания начала каждой секции файла под кратные значения байт. После получения управления вирус перехватывает IFS API, отслеживая вызовы функции обращения к файлам и заражая исполняемые файлы. 26 апреля срабатывает деструктивная функция вируса, которая заключается в стирании Flash BIOS и начальных секторов жестких дисков. Результатом является неспособность компьютера загружаться вообще (в случае успешной попытки стереть Flash BIOS) либо потеря данных на всех жестких дисках компьютера.

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

Пример. Одними из наиболее разрушительных макровирусов являются представители семейства Macro.Word97.Thus. Эти вирусы содержат три процедуры Document_Open, Document_Close и Document_New, которыми подменяет стандартные макросы, выполняющиеся при открытии, закрытии и создании документа, тем самым обеспечивая заражение других документов. 13 декабря срабатывает деструктивная функция вируса - он удаляет все файлы на диске C:, включая каталоги и подкаталоги.

***2.3 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).

Пример. Virus.VBS.Sling написан на языке VBScript (Visual Basic Script). При запуске он ищет файлы с расширениями .VBS или .VBE и заражает их. При наступлении 16-го июня или июля вирус при запуске удаляет все файлы с расширениями .VBS и .VBE, включая самого себя.

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 применяться такие технологии как:

- ***Шифрование** — вирус состоит из двух функциональных кусков: собственно вирус и шифратор.* Каждая копия вируса состоит из шифратора, случайного ключа и собственно вируса, зашифрованного этим ключом.

- ***Метаморфизм*** *— создание различных копий вируса путем замены блоков команд на эквивалентные, перестановки местами кусков кода,* вставки между значащими кусками кода «мусорных» команд, которые практически ничего не делают.

Сочетание этих двух технологий приводит к появлению следующих типов вирусов классифицируемых по технологии защиты от обнаружения:

1. ***Шифрованный вирус*** *— вирус, использующий простое шифрование со случайным ключом и неизменный шифратор.* Такие вирусы легко обнаруживаются по сигнатуре шифратора.
2. ***Метаморфный вирус*** *— вирус, применяющий метаморфизм ко всему своему телу для создания новых копий.*
3. ***Полиморфный вирус*** *— вирус, использующий метаморфный шифратор для шифрования основного тела вируса со случайным ключом.* При этом часть информации, используемой для получения новых копий шифратора также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм.

Пример. Одним из наиболее сложных и относительно поздних полиморфных вирусов является Virus.Win32.Etap. При заражении файла вирус перестраивает и шифрует собственный код, записывает его в одну из секций заражаемого файла, после чего ищет в коде файла вызов функции ExitProcess и заменяет его на вызов вирусного кода. Таким образом, вирус получает управление не перед выполнением исходного кода зараженного файла, а после него.

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.

13.5.2 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.

Пример. Классическими сетевыми червями являются представители семейства Net-Worm.Win32.Sasser. Эти черви используют уязвимость в службе LSASS Microsoft Windows. При размножении, червь запускает FTP-службу на TCP-порту 5554, после чего выбирает IP-адрес для атаки и отсылает запрос на порт 445 по этому адресу, проверяя, запущена ли служба LSASS. Если атакуемый компьютер отвечает на запрос, червь посылает на этот же порт эксплойт уязвимости в службе LSASS, в результате успешного выполнения которого на удаленном компьютере запускается командная оболочка на TCP-порту 9996. Через эту оболочку червь удаленно выполняет загрузку копии червя по протоколу FTP с запущенного ранее сервера и удаленно же запускает себя, завершая процесс проникновения и активации.

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.

1. ***Требующие активного участия пользователя.*** *Отличительная особенность таких является 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.*
2. ***Не требующие активного участия пользователя.*** *Активация сетевого червя без участия пользователя всегда означает, что червь использует бреши в безопасности программного обеспечении*

компьютера. Это приводит к очень быстрому распространению червя внутри корпоративной сети с большим числом станций, существенно увеличивает загрузку каналов связи и может полностью парализовать сеть. Именно этот метод активации использовали черви Lovesan и Sasser.

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).

13.5.3 Троянские программы

Трояны или программы класса троянский конь, в отличие от вирусов и червей, не обязаны уметь размножаться.

Троян (троянский конь) *- программа, основной целью которой является вредоносное воздействие по отношению к компьютерной системе путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.*

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.

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.

Пример. Trojan.SymbOS.Hobble.a является архивом для операционной системы Symbian (SIS-архивом). При этом он маскируется под антивирус Symantec и носит имя symantec.sis. После запуска на смартфоне троян подменяет оригинальный файл оболочки FExplorer.app на поврежденный

файл. В результате при следующей загрузке операционной системы большинство функций смартфона оказываются недоступными.

Для 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.

1. Клавиатурные шпионы, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору.

2. Похитители паролей предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат.

Пример. Trojan-PSW.Win32.LdPinch.kw собирает сведения о системе, а также логины и пароли для различных сервисов и прикладных программ - мессенджеров, почтовых клиентов, программ дозвона. Часто эти данные оказываются слабо защищены, что позволяет трояну их получить и отправить злоумышленнику по электронной почте.

3. 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.

Пример. Backdoor.Win32.Netbus.170 предоставляет полный контроль над компьютером пользователя, включая выполнение любых файловых операций, загрузку и запуск других программ, получение снимков экрана и т. д.

4. Люки (backdoor) *— трояны предоставляющие злоумышленнику ограниченный контроль над компьютером пользователя. От утилит удаленного управления отличаются более простым устройством и, как следствие, небольшим количеством доступных действий.* Тем не менее, обычно одними из действий являются возможность загрузки и запуска любых файлов по команде злоумышленника, что позволяет при необходимости превратить ограниченный контроль в полный.

Пример. Троян Backdoor.win32.Wootbot.gen использует IRC-канал для получения команд от «хозяина». По команде троян может загружать и запускать на выполнение другие программы, сканировать другие компьютеры на наличие уязвимостей и устанавливать себя на компьютеры через обнаруженные уязвимости.

5. Анонимные SMTP-сервера и прокси-сервера *- разновидность троянов, которые на зараженном компьютере организовывают несанкционированную отправку электронной почты, что часто используется для рассылки спама.*

Пример. Трояны из семейства Trojan-Proxy.Win32.Mitglieder распространяются с различными версиями червей Bagle. Троян запускается червем, открывает на компьютере порт и отправляет автору вируса информацию об IP-адресе зараженного компьютера. После этого компьютер может использоваться для рассылки спама.

6. Утилиты дозвона *- в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернет.*

7. 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.

8. 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.*

Пример. Virus.Win9x.CIH, Macro.Word97.Thus

Отдельно отметим, 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.

13.5.4 Другие вредоносные программы

Среди множества других вредоносных программ, для которых нельзя привести общий критерий, можно выделить следующие небольшие группы.

1. 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 условно опасным программам 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.
- ***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.

2. 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 использую*т хакеры для скрытного взятия под контроль взломанной системы (RootKit) и другие подобные утилиты. То есть такие специфические программы, которые обычно используют только хакеры.

3. 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.

13.6 Примеры угроз безопасности информации реализуемых вредоностными программами

Рассмотрим угрозы безопасности информации с точки зрения вирусов. Учитывая тот факт, что общее число вирусов по состоянию на сегодня превосходит 100000, проанализировать угрозы со стороны каждого из них является слишком трудоемкой и бесполезной задачей, поскольку ежедневно возрастает количество вирусов, а значит, необходимо ежедневно модифицировать полученный список. В этой работе мы будем считать, что вирус способен реализовать любую из угроз безопасности информации.

Существует множество способов классификации угроз безопасности информации, которая обрабатывается в автоматизированной системе. Наиболее часто используется классификация угроз по результату их влияния на информацию, а именно - нарушение конфиденциальности, целостности и доступности.

Для каждой угрозы существует несколько способов ее реализации со стороны вирусов.

Угроза нарушения конфиденциальности.

- Кража информации и ее распространение с помощью штатных средств связи либо скрытых каналов передачи: Email-Worm.Win32.Sircam - рассылал вместе с вирусными копиями произвольные документы, найденные на зараженном компьютере.
- Кража паролей доступа, ключей шифрования и пр.: любые трояны, крадущие пароли, Trojan-PSW.Win32.LdPinch.gen.
- Удаленное управление: Backdoor.Win32.NetBus, Email-Worm.Win32.Bagle (backdoor-функциональность).

Угроза нарушения целостности.

- Модификация без уничтожения (изменение информации): любой паразитирующий вирус.
- Модификация посредством уничтожения либо шифрации (удаление некоторых типов документов): Virus.DOS.OneHalf - шифрование содержимого диска, Virus.Win32.Gpcode.f - шифрует файлы с определенными расширениями, после чего самоуничтожается, оставляя рядом с зашифрованными файлами координаты для связи по вопросам расшифровки файлов.
- Модификация путем низкоуровневого уничтожения носителя (форматирование носителя, уничтожение таблиц распределения файлов): Virus.MSWord.Melissa.w - 25 декабря форматирует диск C:

Угроза нарушения доступности.

- Загрузка каналов передачи данных большим числом пакетов: Net-Worm.Win32.Slammer - непрерывная рассылка инфицированных пакетов в бесконечном цикле.
- Любая деятельность, результатом которой является невозможность доступа к информации; различные звуковые и визуальные эффекты: Email-Worm.Win32.Bagle.p - блокирование доступа к сайтам антивирусных компаний.
- Вывод компьютера из строя путем уничтожения либо порчи критических составляющих (уничтожение Flash BIOS): Virus.Win9x.CIH - порча Flash BIOS.

Как несложно было убедиться, для каждого из приведенных выше способов реализации угроз можно привести конкретный пример вируса, реализующего один или одновременно несколько способов.

13.7 История компьютерных вирусов

Теоретические основы создания компьютерных вирусов были заложены в 40-х годах XX столетия американским ученым Джоном фон Нейманом (John von Neumann), который также известен как автор базовых принципов работы современного компьютера. Впервые же термин вирус в отношении компьютерных программ применил Фред Коэн (Fred Cohen). Это случилось 3 ноября 1983 года на еженедельном семинаре по компьютерной безопасности в Университете Южной Калифорнии (США), где был предложен проект по созданию самораспространяющейся программы, которую тут же окрестили вирусом. Для ее отладки потребовалось 8 часов компьютерного времени на машине VAX 11/750 под управлением операционной системы Unix и ровно через неделю, 10 ноября состоялась первая демонстрация. Фредом Коэном по результатам этих исследований была опубликована работа «Computer Viruses: theory and experiments» с подробным описанием проблемы.

Поскольку рассматриваемые вирусы - это по сути компьютерные программы, то об их истории можно говорить только начиная с появления компьютеров, то есть с 1946 года, когда в США была выпущена первая электронно-вычислительная машина (ЭВМ) - ENIAC (Electronic Numerical Integrator And Computer). Однако до появления в 1960 году коммерческих компьютеров, доступ к ЭВМ был сильно ограничен и вирусных инцидентов зафиксировано не было.

Первый известный вирус был написан для компьютера Univac 1108 (конец 1960-х - начало 1970-х годов). Он назывался Pervading Animal и фактически представлял собой игру, написанную с ошибкой - с помощью наводящих вопросов программа пыталась определить имя животного, задуманного играющим. Ошибка заключалась в том, что при добавлении новых вопросов модифицированная игра записывалась поверх старой версии

плюс копировалась в другие директории. Следовательно через некоторое время диск становился переполненным. Поскольку Pervading Animal не был настоящим вирусом, он не содержал процедуры самораспространения и передавался исключительно через пользователей, желающих по собственной воле переписать программу.

В 1969 году в США была создана первая глобальная компьютерная сеть, прародитель современной Интернет, ARPANET (Advanced Research Projects Agency Network). Она объединяла четыре ведущие научные центра США и служила для быстрого обмена научной информацией. Не удивительно, что уже в начале 1970-х в ARPANET появился первый вирус, умеющий распространяться по сети. Он назывался Creeper и был способен самостоятельно выйти в сеть через модем и сохранить свою копию на удаленной машине. На зараженных компьютерах вирус обнаруживал себя сообщением «I'M THE CREEPER: CATCH ME IF YOU CAN». Для удаления назойливого, но в целом безобидного вируса неизвестным была создана программа Reaper. По сути это был вирус, выполнявший некоторые функции, свойственные антивирусу: он распространялся по компьютерной сети и в случае обнаружения на машине вируса Creeper, уничтожал его.

В это время компьютеры использовались исключительно в промышленных целях - они были очень дороги и сложны в эксплуатации, время работы на них было расписано по минутам. Выпуск персональных компьютеров, то есть таких, которые могли быть приобретены отдельными людьми и использованы в личных целях, был налажен в конце 70-х - начале 80-х годов прошлого века. Это были персональные компьютеры Apple и IBM Personal Computer. Однако с развитием компьютерной техники прогрессировали и компьютерные вирусы. В 1981 году были зафиксированы случаи заражения Elk Cloner, который распространялся через пиратские копии компьютерных игр. Поскольку жестких дисков тогда еще не было, он записывался в загрузочные сектора дискет и проявлял себя переворачиванием изображения на экране.

В 1984 году вышли в свет первые антивирусные программы - CHK4BOMB и BOMBSQAD. Их автором был Энди Хопкинс (Andy Hopkins). Программы анализировали загрузочные модули и позволяли перехватывать запись и форматирование, выполняемые через BIOS. На то время они были очень эффективны и быстро завоевали популярность.

Первую настоящую глобальную эпидемию вызвал в 1986 году вирус Brain. Он был написан двумя братьями-программистами Баситом Фарук и Амжадом Алви (Basit Farooq Alvi и Amjad Alvi) из Пакистана с целью определения уровня компьютерного пиратства у себя в стране: вирус заражал загрузочные сектора, менял метку диска на «(c) Brain» и оставлял сообщение с именами, адресом и телефоном авторов. Отличительная черта Brain - умение подставлять незараженный оригинал вместо реальных данных при попытке просмотра пользователем инфицированного загрузочного сектора (так называемая стелс-технология). В течение нескольких месяцев программа

вышла за пределы Пакистана и к лету 1987 года эпидемия достигла глобальных масштабов. Ничего деструктивного вирус не делал.

В этом же году произошло еще одно знаменательное событие. Немецкий программист Ральф Бюргер (Ralf Burger) открыл возможность создания программой своих копий путем добавления своего кода к выполняемым DOS-файлам формата COM. Опытный образец программы, получившей название Virdem, был продемонстрирован на форуме компьютерного андеграунда - Chaos Computer Club (декабрь 1986 года, Гамбург, ФРГ). По результатами исследований Бюргер выпустил книгу «Computer Viruses. The Disease of High Technologies», послужившую толчком к написанию тысяч компьютерных вирусов, частично или полностью использовавших описанные автором идеи.

В следующем 1987 году был написан первый по-настоящему вредоносный вирус - Lehigh. Он вызвал эпидемию в Лехайском университете (США). Lehigh заражал только системные файлы COMMAND.COM и был запрограммирован на удаление всей информации на инфицированном диске. В течение нескольких дней было уничтожено содержимое сотен дискет из библиотеки университета и личных дискет студентов. Всего за время эпидемии было заражено около четырех тысяч компьютеров. Однако за пределы университета Lehigh не вышел.

Mike RoChenle - псевдоним автора первой известной вирусной мистификации. В октябре 1988 года он разослал на станции BBS большое количество сообщений о вирусе, который передается от модема к модему со скоростью 2400 бит/с. В качестве панацеи предлагалось перейти на использование модемов со скоростью 1200 бит/с. Как это ни смешно, многие пользователи действительно последовали этому совету.

В ноябре 1988 года случилась глобальная эпидемия червя Морриса. Небольшая программа, написанная 23-летним студентом Корнельского университета (США) Робертом Моррисом, использовала ошибки в системе безопасности операционной системы Unix для платформ VAX и Sun Microsystems. С целью незаметного проникновения в вычислительные системы, связанные с сетью ARPANET, использовался подбор паролей (из списка, содержащего 481 вариант). Это позволяло маскироваться под задачу легальных пользователей системы. Однако из-за ошибок в коде безвредная по замыслу программа неограниченно рассылала свои копии по другим компьютерам сети, запускала их на выполнение и таким образом забирала под себя все сетевые ресурсы. Червь Морриса заразил по разным оценкам от 6000 до 9000 компьютеров в США (включая Исследовательский центр NASA) и практически парализовал их работу на срок до пяти суток. Общие убытки были оценены в минимум 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на восстановление работоспособности систем. Общая стоимость этих затрат оценивается в 96 миллионов долларов. Ущерб был бы гораздо больше, если бы червь изначально создавался с разрушительными целями. Роберт Моррис также стал первым человеком,

осужденным за написание и распространение компьютерных вирусов - 4 мая 1990 года состоялся суд, который приговорил его к 3 годам условно, 400 часам общественных работ и штрафу в 10 тысяч долларов США.

Примечательно, что в том же году, когда случилась эпидемия червя Морриса, известный программист Питер Нортон (Peter Norton) высказался резко против существования вирусов. Он официально объявил их несуществующим мифом и сравнил со сказками о крокодилах, живущих в канализации Нью-Йорка. Это показывает сколь низка была культура антивирусной безопасности в то время.

Тогда же, в 1988, вышла первая широко известная антивирусная программа английским программистом Аланом Соломоном (Alan Solomon) и называлась Dr. Solomon's Anti-Virus Toolkit. Она завоевала огромную популярность и просуществовала вплоть до 1998 года, когда компания Dr. Solomon была поглощена другим производителем антивирусов - американской Network Associates (NAI).

В декабре 1989 года разразилась первая эпидемия троянской программы - Aids Information Diskette. Ее автор разослал около 20000 дискет с вирусом по почтовым адресам в Европе, Африке и Австралии, похищенным из баз данных Организации всемирного здравоохранения и журнала PC Business World. После запуска вредоносная программа автоматически внедрялась в систему, создавала свои собственные скрытые файлы и директории и модифицировала системные файлы. Через 90 загрузок операционной системы все файлы на диске становились недоступными, кроме одного - с сообщением, предлагавшим прислать $189 на указанный адрес. Автор троянца, Джозеф Попп (Joseph Popp), признанный позднее невменяемым, был задержан в момент обналичивания чека и осужден за вымогательство. Фактически, Aids Information Diskette - это первый и единственный вирус, для массовой рассылки, использовавший настоящую почту.

В том же году был обнаружен вирус Cascade, вызывающий характерный видеоэффект - осыпание букв на экране. Примечателен тем, что послужил толчком для профессиональной переориентации Евгения Касперского на создание программ-антивирусов, будучи обнаруженным на его рабочем компьютере. Уже через месяц второй инцидент (вирус Vacsina) был закрыт при помощи первой версии антивируса -V, который несколькими годами позже был переименован в AVP - AntiViral Toolkit Pro.

Вскоре после этого, в конце 1990, несмотря на громкое заявление Питера Нортона, прозвучавшее двумя годами ранее и где он авторитетно заявлял о надуманности проблемы вирусов, вышла первая версия антивирусной программы Norton AntiVirus.

Первый общедоступный конструктор вирусов VCL (Virus Creation Laboratory), представляющий собой графическую среду для разработки вирусов для операционной системы MS DOS, появился в июле 1992 года. Начиная с этого момента, любой человек мог легко сформировать и написать

вирус. Этот год также положил начало эпохи вирусов для Windows - был создан первый вирус, поражающий исполняемые файлы Microsoft Windows 3.1. Однако поскольку Win.Vir эпидемии не вызвал, его появление осталось практически незаметным.

OneHalf, очень сложный вирус, обнаруженный в июне 1994 года, вызвал глобальную эпидемию во всем мире, в том числе в России. Он заражал загрузочные сектора дисков и COM/EXE-файлы, увеличивая их размер на 3544, 3577 или 3518 байта, в зависимости от модификации. При каждой перезагрузке зараженного компьютера зашифровывались два последних незашифрованных ранее цилиндра жесткого диска. Это продолжалось до тех пор, пока весь винчестер не оказывался зашифрованным. Встроенная стелс-процедура позволяла вирусу при запросе зашифрованной информации производить расшифровку на лету - следовательно, пользователь долгое время пребывал в неведении. Единственным визуальным проявлением вируса было сообщение «Dis is one half. Press any key to continue...», выводившееся в момент достижения количеством зашифрованных цилиндров диска половины от их общего числа. Однако при первой же попытке лечения, после вылечивания загрузочных секторов диска, вся информация на винчестере становилась недоступной, без возможности восстановления. Популярности этого вируса в России поспособствовала компания Доктор Веб, которая выпустила новую версию своего антивируса, анонсировав его как средство от OneHalf. Однако на практике после лечения загрузочных секторов от этого вируса, Dr.Web забывал расшифровать информацию на диске и восстановить ее было уже невозможно.

Следующий год запомнился инцидентом в корпорации Microsoft. В феврале 1995 года, в преддверии выпуска новой операционной системы Windows 95, была разослана демонстрационная дискета, зараженная загрузочным вирусом Form. Копии этого диска получили 160 бета-тестеров, один из которых не поленился провести антивирусную проверку. Вслед за Microsoft отличились журналы PC Magazine (английская редакция) и Computer Life, которые разослали своим подписчикам дискеты, зараженные загрузочными вирусами Sampo и Parity_Boot соответственно.

В августе 1995 появился Concept - первый вирус, поражавший документы Microsoft Word.

В том же 1995 году, в бесплатном приложении полуподпольного издания известного специалиста в области компьютерных вирусов Марка Людвига (Mark Ludwig) «Underground Technology Review», был приведен исходный код вируса Green Stripe, который заражал документы AmiPro, популярного в то время текстового редактора.

До февраля 1997 года считалось, что операционная систем Linux неуязвима перед вирусами, пока не появился Linux.Bliss. В марте того же года были зафиксированы первые случаи использования возможностей

электронной почты - ShareFun, по совместительству первый макро-вирус для MS Word 6/7, распространялся с помощью почтовой программы MS Mail.

Первая утилита удаленного администрирования - BackOrifice, Backdoor.BO - была обнаружена в августе 1998 года. Единственное ее отличие от обычных программ для удаленного управления - это несанкционированная установка и запуск. Действие утилиты сводилось к скрытому слежению за системой: ссылка на BackOrifice отсутствовала в списке активных приложений, но при этом зараженный компьютер был открыт для удаленного доступа. Фактически, на зараженные компьютеры предоставлялся свободный вход для других вредоносных программ. Впоследствии возник целый класс вирусов - червей, размножение которых базировалось на оставленных BackOrifice дырах.

26 марта 1999 года началась глобальная эпидемия Melissa - первого вируса для MS Word, сочетавшего в себе также и функциональность интернет-червя. Сразу же после заражения системы он считывал адресную книгу почтовой программы MS Outlook и рассылал по первым 50 найденным адресам свои копии. Причем это делалось абсолютно незаметно для пользователя и, что самое страшное, от его имени. Такие компании как Microsoft, Intel, Lockheed Martin были вынуждены временно отключить свои корпоративные службы электронной почты. По разным оценкам совокупный ущерб от вируса варьировался от нескольких миллионов до десятков миллионов долларов США.

Через некоторое время был обнаружен и арестован автор вируса Melissa, Дэвид Л. Смит (David L. Smith). 9 декабря он был признан виновным и осужден на 10 лет тюремного заключения и к штрафу в размере 400 000 долларов США.

В декабре 1999 года был впервые обнаружен вирус-червь с заложенными в нем функциями удаленного самообновления - Babylonia. Он ежеминутно пытался соединиться с сервером, находящемся в Японии и загрузить оттуда список вирусных модулей.

LoveLetter - это скрипт-вирус, 5 мая 2000 года побивший рекорд вируса Melissa по скорости распространения. Всего в течение нескольких часов были поражены миллионы компьютеров - LoveLetter попал в Книгу Рекордов Гиннеса. Успех гарантировали методы социальной инженерии: электронное сообщение имело тему «I love you» и интригующий текст, призывающий открыть вложенный файл с вирусом.

Август 2000 года ознаменовался завоеванием вирусами мобильных устройств - вирус Liberty заражал карманные компьютеры Palm Pilot с операционной системой PalmOS.

На тот момент все известные вирусы для хранения собственных копий использовали файлы, то есть ПЗУ компьютера. Обнаруженный 12 июля 2001 года CodeRed стал первым представителем нового типа вредоносных программ, способных активно распространяться и работать на зараженных компьютерах без использования файлов. В процессе работы такие вирусы

существуют исключительно в системной памяти, а при передаче на другие компьютеры - в виде специальных пакетов данных. Для проникновения на удаленные компьютеры CodeRed использовал брешь в системе безопасности IIS (Internet Information Services), которая позволяет злоумышленникам запускать на удаленных серверах посторонний программный код. 18 июня 2001 года Microsoft выпустила соответствующую заплатку, однако подавляющее большинство пользователей не успело вовремя обновить свое программное обеспечение. CodeRed вызвал эпидемию, заразив около 12000 (по другим данным - до 200000) серверов по всему миру и провел крупномасштабную DDoS атаку на веб-сервер Белого дома, вызвав нарушение его нормальной работы. Через неделю, 19 июля появилась новая модификация CodeRed, показавшая чудеса распространения - более 350000 машин за 14 часов (до 2000 компьютеров в минуту).

В это же время был обнаружен почтовый червь Sircam (12 июля 2001 года). Этот вирус отличала необычная процедура выбора имени зараженного вложения. Для этого случайным образом на диске инфицированного компьютера выбирался документ, к имени которого добавлялось расширение .pif, .lnk, .bat или .com. Полученная конструкция вида mydiary.doc.com служила темой рассылаемых писем и именем новой копии программы: к отобранному файлу дописывался код червя - таким образом Sircam мог привести к утечке конфиденциальной информации. При рассылке в поле от указывался один из адресов, найденных на зараженном компьютере, а сообщение содержало текст вида «Hi! How are you? I send you this file in order to have your advice. See you later. Thanks». Кроме этого, в определенный момент времени (в зависимости от системного времени и модификации вируса) на зараженном компьютере удалялись все файлы на системном жестком диске.

18 сентября 2001 года началась эпидемия Nimda - этот вирус-червь в течение всего 12 часов поразил до 450000 компьютеров. Для распространения были задействованы пять методов: электронная почта (брешь в системе безопасности Internet Explorer, позволяющая автоматически выполнять вложенный исполняемый файл), по локальной сети, внедрение на IIS-сервера, заражение браузеров, а также с помощью бекдор-процедур, оставленных предыдущими вирусами. После заражения Nimda открывал локальные диски на полный доступ для всех желающих.

Вскоре после Nimda появился Klez - почтовый червь, различные модификации которого на протяжении следующих нескольких лет занимали первые строки в рейтингах популярности. Программа проникала на компьютер по сети или через электронную почту, используя брешь в защите IFrame браузера Internet Explorer, которая допускала автоматический запуск вложенного файла. Также вирус имел встроенную функцию поиска и подавления антивирусного программного обеспечения. Klez дописывал свой код к одному из документов на зараженной машине и начинал массовую рассылку. В поле «От» подставлялся любой адрес, найденный на компьютере

или же случайно сгенерированный. При этом список всех обнаруженных на зараженном компьютере адресов электронной почты также присоединялся к вложению. Кроме рассылки своих копий, червь обнаруживал себя по 13-м числам четных месяцев или шестым нечетных, в зависимости от модификации: в такой день все файлы на зараженных компьютерах заполнялись случайным содержимым.

Стоит также отметить Tanatos/Bugbear (впервые обнаружен в октябре 2001 года) - почтовый червь, устанавливающий бекдор-процедуру (Backdoor) и троян - клавиатурный шпион. Процедура распространения практически полностью была списана с Klez - копирование по сети, массовая рассылка с зараженным документом во вложении, использование уязвимости IFrame в Internet Explorer, подавление антивирусных программ. Кроме увеличения трафика, вирус проявлял себя спонтанной печатью разнообразного мусора на сетевых принтерах.

В январе 2003 года грянула эпидемия интернет-червя Slammer, заражающего сервера под управлением Microsoft SQL Server 2000. Вирус использовал брешь в системе безопасности SQL Server, заплата к которой вышла шестью месяцами ранее. После проникновения на компьютер 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 DNS-серверов сети Интернет вышли из строя. Slammer имел крайне небольшой размер - всего 376 байт (CodeRed - 4 КБ, Nimda - 60 КБ) и присутствовал только в памяти зараженных компьютеров. Более того, при работе червя никакие файлы не создавались, и червь никак не проявлял себя (помимо сетевой активности зараженного компьютера). Это означает, что лечение заключалось только в перезагрузке сервера, а антивирусы в данной ситуации бессильны.

В августе 2003 года около 8 миллионов компьютеров во всем мире оказались заражены интернет-червем Lovesan/Blaster. Для размножения использовалась очередная брешь - на этот раз в службе DCOM RPC Microsoft Windows. Кроме того, Lovesan/Blaster включал в себя функцию DDoS-атаки на сервер с обновлениями для Windows.

Неделей позже новый вирус, Sobig.f, установил новый рекорд по скорости - доля зараженных им писем доходила до 10 % от всей корреспонденции. Это достигалось использованием спамерских технологий. Sobig.f также инициировал цепную реакцию: каждый новый вариант червя создавал сеть инфицированных компьютеров, которая позднее использовалась в качестве платформы для новой эпидемии. Однако конец эпидемии запрограммировал сам автор - 10 сентября 2003 года Sobig.f прекратил размножение.

В феврале 2004 года появился Bizex (также известный как Exploit) - первый ICQ-червь. Для распространения использовалась массовая несанкционированная рассылка по ICQ сообщения

«http://www.jokeworld.biz/index.html :)) LOL». Получив от знакомого человека такую ссылку, ничего не подозревающая жертва открывала указанную страницу и в случае, если использовался браузер Internet Explorer с незакрытой уязвимостью, на компьютер загружались файлы вируса. После установки в систему, Bizex закрывал запущенный ICQ-клиент и подключившись к серверу ICQ с данными зараженного пользователя начинал рассылку по найденным на компьютере спискам контактов. Одновременно происходила кража конфиденциальной информации - банковские данные, различные логины и пароли.

В этом же 2004 году разразилась так называемая война вирусописателей. Несколько преступных группировок, известных по вирусам Bagle, Mydoom и Netsky выпускали новые модификации своих программ буквально каждый час. Каждая новая программа несла в себе очередное послание к противостоящей группировке, изобилующее нецензурными выражениями, а Netsky даже удалял любые обнаруженные экземпляры вирусов Mydoom и Bagle.

Mydoom известен также массированной 12-дневной DDoS-атакой на веб-сайт компании SCO, начавшейся 1 февраля 2004 года. За пару часов работа сервера была полностью парализована и вернуться в нормальный режим www.sco.com смог только 5 марта. В ответ руководители SCO объявили награду в размере 250 тысяч долларов США за информацию об авторе червя.

Нельзя не упомянуть червя Sasser, который в мае 2004 года поразил более 8 млн. компьютеров, а убытки от него оцениваются в 979 млн. долларов США. Для проникновения Sasser использовал уязвимость в службе LSASS Microsoft Windows.

Вскоре после того, как начали активно использоваться смартфоны (от англ. smartphone) - устройства, сочетающие в себе функции карманного компьютера и телефона, появился и первый вирус для них - Cabir (июнь 2004 года). Он распространялся через протокол Bluetooth и заражал мобильные телефоны, работающие под управлением OS Symbian. При каждом включении инфицированного телефона вирус получал управление и начинал сканировать список активных Bluetooth-соединений, выбирал первое доступное и пытался передать туда свой основной файл caribe.sis. Ничего деструктивного Cabir не делал - только снижал стабильность работы телефона за счет постоянных попыток сканирования активных Bluetooth-устройств.

Вредоносные программы - это не только вирусы, черви и трояны. К этому классу в полной мере можно отнести и adware - программы, которые отображают на экране рекламу без ведома и согласия пользователя, и pornware - программы, самостоятельно инициирующие соединения с платными порнографическими сайтами. Начиная с 2004 отмечается широкое распространение использования вирусных технологий для установки adware/pornware на целевые компьютеры. Этот год также запомнился

масштабными арестами вирусописателей - было осуждено около 100 хакеров, причем трое из них находились в двадцатке самых разыскиваемых ФБР преступников.

В следующем, 2005 году глобальных эпидемий зафиксировано не было. Это не означает уменьшение числа вирусов - наоборот, с каждым днем их появляется все больше. Но при этом можно отметить увеличение избирательности вредоносных программ - становятся популярны черви, главной целью которых является похищение определенной информации. Кроме уже ставших привычными краж номеров кредитных карт, участились случаи воровства персональных данных игроков различных онлайновых. Развитие получили и вирусные технологии для мобильных устройств. В качестве пути проникновения используются не только Bluetooth-устройства, но и обычные MMS-сообщения (червь ComWar).

В современном Интернет в среднем каждое тридцатое письмо заражено почтовым червем, около 70% всей корреспонденции - нежелательна. С ростом сети Интернет увеличивается количество потенциальных жертв вирусописателей, выход новых операционных систем влечет за собой расширение спектра возможных путей проникновения в систему и вариантов возможной вредоносной нагрузки для вирусов.

13.8 Ответственность за написание и распространение вредоносных программ

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. Незаконное использование объектов авторского права или смежных прав, а равно присвоение авторства, если эти деяния причинили крупный ущерб, - наказываются штрафом в размере от двухсот до четырехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до четырех месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, - наказываются штрафом в размере от четырехсот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от четырех до восьми месяцев, либо арестом на срок от четырех до шести месяцев, либо *лишением свободы на срок до пяти лет*.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Нарушение

тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан - наказывается штрафом в размере от пятидесяти до ста минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного месяца, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, - наказывается штрафом в размере от ста до трехсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до трех месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от двух до четырех месяцев. Незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации, - наказываются штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо ограничением свободы на срок до трех лет, либо *лишением свободы на срок до трех лет с лишением права занимать определенные должности* или заниматься определенной деятельностью на срок до трех лет.

Статья 272. Неправомерный доступ к компьютерной информации. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет. То же деяние, совершенное, группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо *лишением свободы на срок до пяти лет*

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо

копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются *лишением свободы на срок от трех до семи лет*.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо свободы на срок до двух лет. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается *лишением свободы на срок до четырех лет*.

14. ОСНОВЫ БОРЬБЫ С ВРЕДОНОСТНЫМИ ПРОГРАММАМИ

14.1 Самостоятельная диагностика заражения вредоносными программами

14.1.1 Признаки и диагностика заражений через браузер

Явные проявления обычно заражений через Браузер выражаются в неожиданно появляющихся рекламных сообщениях и баннерах - обычно это следствие проникновения на компьютер рекламной утилиты. Поскольку их главная цель - это привлечь внимание пользователя к рекламируемой услуге или товару, то им сложно оставаться незаметными. Также явные проявления могут вызывать ряд троянских программ, например утилиты несанкционированного дозвона к платным сервисам. Они вынуждены быть явными, поскольку используемые ими приложения сложно использовать незаметно от пользователя.

14.1.2 Подозрительные процессы

Одним из основных проявлений вредоносных программ является наличие в списке запущенных процессов (в ОС семейства Windows вызывается через CTRL+ALT+DEL, рис 14.1) подозрительных программ. Исследуя этот список и особенно сравнивая его с перечнем процессов, которые были запущены на компьютере сразу после установки системы, то есть до начала работы, можно сделать достаточно достоверные выводы об инфицировании. Это часто помогает при обнаружении вредоносных программ, имеющих лишь только скрытые или косвенные проявления.

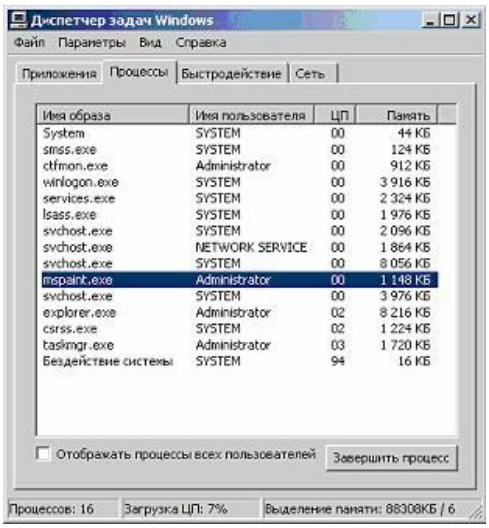

Рис. 14.1 – Просмотр запущенных в системе Windows процессов

14.1.3 Сетевая активность

Неожиданно возросшая сетевая активность может служить ярким свидетельством работы на компьютере подозрительный программы. Но при этом нужно не забывать, что ряд вполне легальных приложений также имеют свойство иногда связываться с сайтом фирмы-производителя, например для проверки наличия обновлений или более новых версий. Поэтому, прежде чем отключать сеть необходимо уметь определять какие программы и приложения вызвали эту подозрительную активность.

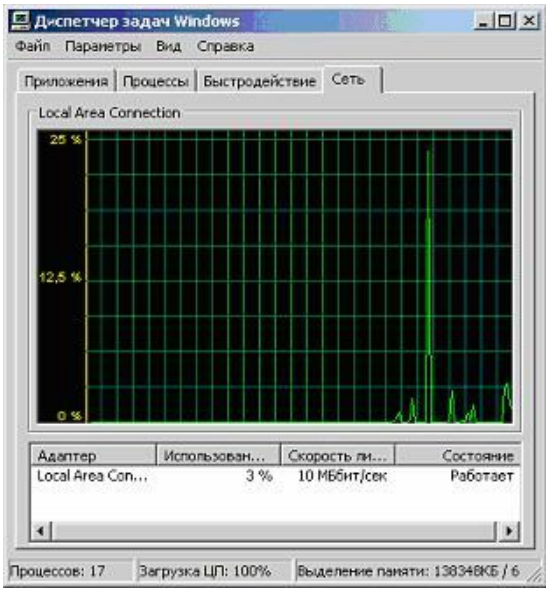

Рис. 14.2

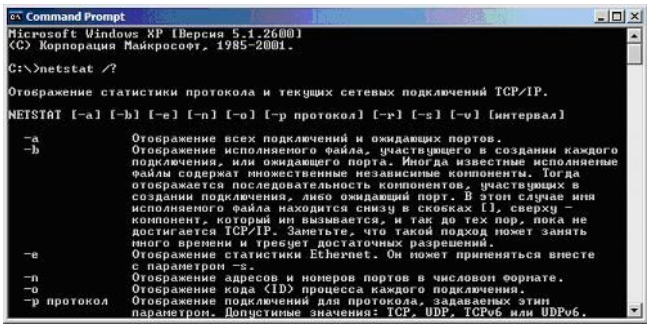

Рис. 14.3

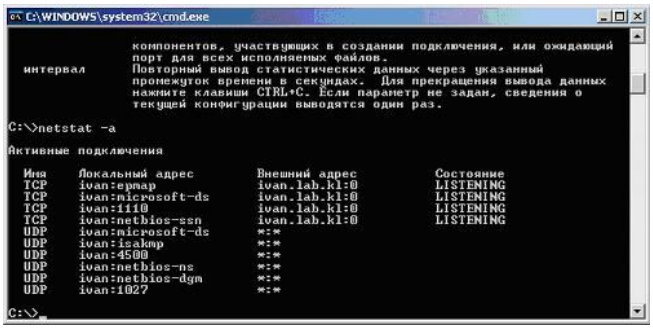

Рис. 14.4

Изучить и проанализировать сетевую активность можно с помощью встроенных в операционную систему инструментов или же воспользовавшись специальными отдельно устанавливаемыми приложениями. В этом задании это предлагается сделать с помощью **Диспетчера задач Windows** (рис. 14.2) и встроенной утилиты netstat (рис. 14.3, 14.4), которая выводит на экран мгновенную статистику сетевых соединений.

14.1.4 Элементы автозапуска

Для того, чтобы прикладная программа начала выполняться, ее нужно запустить. Следовательно, и вирус нуждается в том, чтобы его запустили.

Оптимальным с точки зрения вируса вариантом служит запуск одновременно с операционной системой - в этом случае запуск практически гарантирован.

Вредоносная программа может вносить изменения в системные файлы win.ini и system.ini.

Следует также отметить, что в файле system.ini кроме секции [boot] вредоносные программы могут использовать секцию [Drivers].

Вредоносные программы могут вносить изменения в следующие ветки реестра:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion в ключи Run, RunOnce, RunOnceEx, RunServices, RunServicesOnce - для того чтобы система запускала созданные червем файлы
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion в ключ Run.

Кроме выше перечисленных ветвей и ключей реестра вредоносные программы могут вносить изменения и в другие ветки и ключи реестра, например:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\WOW\boot
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Drivers32
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\ CurrentVersion\WinLogon
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\ Installed Components
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\AeDebug

Диагностика элементов автозапуска возможно путем изучения секций: SYSTEM.INI (рис. 14.5); WIN.INI (рис. 14.6); «Автозапуск» (рис. 14.7) и «Службы» (рис. 14.8), в утилите конфигурирования msconfig. Удаление запускаемого вируса из автозагрузке возможно путем использования утилиты regedit.

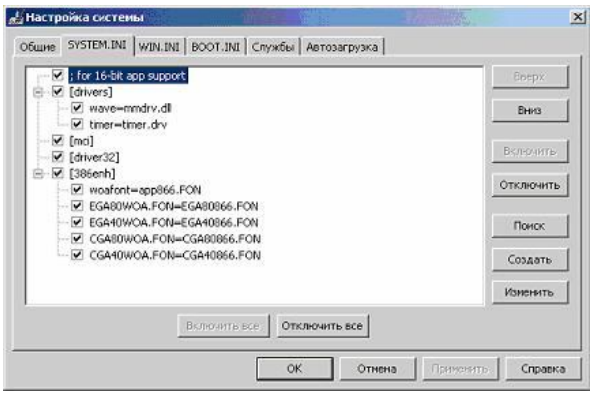

Рис. 14.5

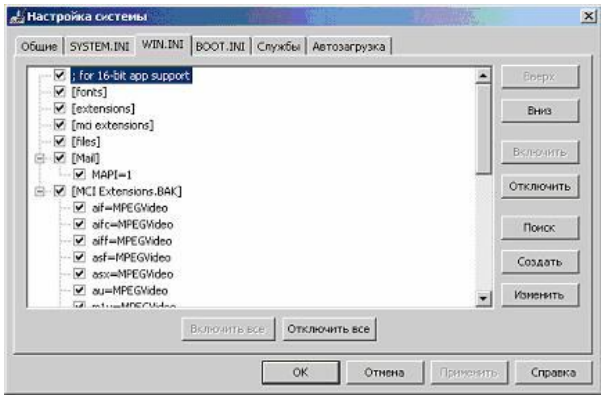

Рис. 14.6

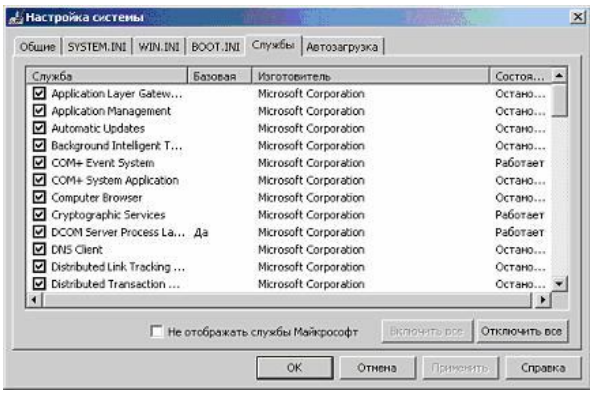

Рис. 14.7

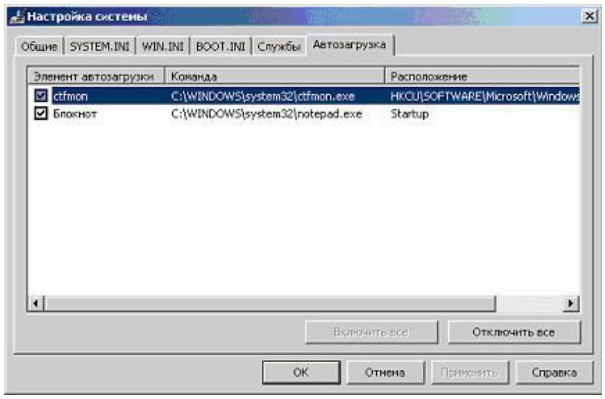

Рис. 14.8

14.2 Основы функционирования антивирусного программного обеспечения

Антивирус *- программное средство, предназначенное для борьбы с вирусами.*

Основными задачами антивируса является:

- *Препятствование проникновению вирусов в компьютерную систему.*
- *Обнаружение наличия вирусов в компьютерной системе.*
- *Устранение вирусов из компьютерной системы без нанесения повреждений другим объектам системы.*
- *Минимизация ущерба от действий вирусов.*

14.2.1 Технологии обнаружения вирусов

Технологии, применяемые в антивирусах, можно разбить на две группы

1. *Технологии сигнатурного анализа.*
2. *Технологии вероятностного анализа:*
   - *2.1. Эвристический анализ.*
   - *2.2. Поведенческий анализ.*
   - *2.3. Анализ контрольных сумм.*

Сигнатурный анализ *- метод обнаружения вирусов, заключающийся в проверке наличия в файлах сигнатур вирусов.* Сигнатурный анализ является наиболее известным методом обнаружения вирусов и используется практически во всех современных антивирусах. Для проведения проверки антивирусу необходим набор вирусных сигнатур, который хранится в антивирусной базе. Ввиду того, что сигнатурный анализ предполагает проверку файлов на наличие сигнатур вирусов, антивирусная база нуждается в периодическом обновлении для поддержания актуальности антивируса.

Недостатки сигнатурного анализа *определяют границы его функциональности - возможность обнаруживать лишь уже известные вирусы - против новых вирусов сигнатурный сканер бессилен.*

Достоинством сигнатурного анализа *является то, что наличие сигнатур вирусов предполагает возможность лечения инфицированных файлов, обнаруженных при помощи сигнатурного анализа.* Однако, лечение допустимо не для всех вирусов - трояны и большинство червей не поддаются лечению по своим конструктивным особенностям, поскольку являются цельными модулями, созданными для нанесения ущерба. Грамотная реализация вирусной сигнатуры позволяет обнаруживать известные вирусы со стопроцентной вероятностью.

Эвристический анализ *- технология, основанная на вероятностных алгоритмах, результатом работы которых является выявление подозрительных объектов. В процессе эвристического анализа проверяется структура файла, его соответствие вирусным шаблонам.* Наиболее популярной эвристической технологией является проверка содержимого файла на предмет наличия модификаций уже известных сигнатур вирусов и их комбинаций. ***Достоинством эвристического анализа*** *является то, что он может определять гибриды и новые версии ранее известных вирусов без дополнительного обновления антивирусной базы.* ***Недостатком*** *– то, что эвристический анализ не предполагает лечения.* Данная технология не способна на 100% определить вирус перед ней или нет, и как любой вероятностный алгоритм грешит ложными срабатываниями.

Поведенческий анализ *- технология, в которой решение о характере проверяемого объекта принимается на основе анализа выполняемых им операций. Поведенческий анализ весьма узко применим на практике, так как большинство действий, характерных для вирусов, могут выполняться и обычными приложениями.* Наибольшую известность получили поведенческие анализаторы скриптов и макросов, поскольку соответствующие вирусы практически всегда выполняют ряд однотипных действий. Помимо этого поведенческие анализаторы могут отслеживать попытки прямого доступа к файлам, внесение изменений в загрузочную запись дискет, форматирование жестких дисков и т. д. Поведенческие анализаторы не используют для работы дополнительных объектов, подобных вирусным базам и, как следствие, неспособны различать известные и неизвестные вирусы - все подозрительные программы априори считаются неизвестными вирусами. Аналогично, особенности работы средств, реализующих технологии поведенческого анализа, не предполагают лечения.

Например, средства защиты, вшиваемые в BIOS, также можно отнести к поведенческим анализаторам. При попытке внести изменения в MBR компьютера, анализатор блокирует действие и выводит соответствующее уведомление пользователю.

Анализ контрольных сумм *- это способ отслеживания изменений в объектах компьютерной системы. На основании анализа характера изменений - одновременность, массовость, идентичные изменения длин файлов - можно делать вывод о заражении системы.* Анализаторы контрольных сумм (также используется название «ревизоры изменений») как и поведенческие анализаторы не используют в работе дополнительные объекты и выдают вердикт о наличии вируса в системе исключительно методом экспертной оценки. Чаще подобные технологии применяются в сканерах при доступе - при первой проверке с файла снимается контрольная сумма и помещается в кэше, перед следующей проверкой того же файла сумма снимается еще раз, сравнивается, и в случае отсутствия изменений файл считается незараженным.

14.2.2 Классификация антивирусного программного обеспечения

Помимо используемых технологий, антивирусы отличаются друг от друга условиями эксплуатации. Уже из анализа задач можно сделать вывод о том, что препятствование проникновению вредоносного кода должно осуществляться непрерывно, тогда как обнаружение вредоносного кода в существующей системе - скорее разовое мероприятие. Следовательно, средства, решающие эти две задачи должны функционировать по-разному.

Таким образом, антивирусы можно разделить на две большие категории:

- ***Предназначенные для непрерывной работы*** - к этой категории относятся средства проверки при доступе, почтовые фильтры, системы сканирования проходящего трафика Интернет, другие средства, сканирующие потоки данных.
- ***Предназначенные для периодического запуска*** - различного рода средства проверки по запросу, предназначенные для однократного сканирования определенных объектов. К таким средствам можно отнести сканер по требованию файловой системы в антивирусном комплексе для рабочей станции, сканер по требованию почтовых ящиков и общих папок в антивирусном комплексе для почтовой системы (в частности, для Microsoft Exchange).

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.

Антивирусное ядро *- реализация механизма сигнатурного сканирования и эвристического анализа на основе имеющихся сигнатур вирусов.*

Исходя из текущей необходимости в средствах защиты выделяют следующие типы антивирусных комплексов:

1. ***Антивирусный комплекс для защиты рабочих станций*** - *предназначен для обеспечения антивирусной защиты рабочей станции*, на которой он установлен. Состоит, как и указывалось ранее из средств непрерывной работы и предназначенных для периодического запуска, а также средств обновления антивирусных баз.
2. ***Антивирусный комплекс для защиты файловых серверов*** - *предназначен для обеспечения антивирусной защиты сервера, на котором установлен.* Указание на файловый сервер в названии является скорее данью истории, корректней будет звучать термин «сетевой». Определение того, насколько нуждается в антивирусной защите сервер, осуществляется не только исходя из его назначения (является сервер файловым, почтовым, либо выполняет другую функцию), а и из используемой на нем платформы.
3. ***Антивирусный комплекс для защиты почтовых систем****, назаначение комплекса назначение - препятствовать доставке зараженных сообщений пользователям сети, но он не предназначен для защиты почтовой системы от поражения вирусами*. Как уже указывалось ранее, сегодня одним из главных средств доставки вирусов в локальную сеть является именно электронная почта. Поэтому, при наличии в локальной сети специализированного узла, обрабатывающего входящую и исходящую из сети почтовую корреспонденцию (почтового сервера), логично будет использовать средство централизованной проверки всего почтового потока на наличие вирусов)
4. ***Антивирусный комплекс для защиты шлюзов*** - *предназначен для проверки на наличие вирусов данных, через этот шлюз передаваемых. Как правило в его состав входят:*
   - *4.1.* ***Сканер HTTP-потока*** *— предназначен для проверки данных, передаваемых через шлюз по протоколу HTTP.*
   - *4.2.* ***Сканер FTP-потока*** *— предназначен для проверки данных, передаваемых через шлюз по протоколу FTP. В случае использования FTP over HTTP FTP-запросы будут проверяться сканером HTTP-потока.*
   - *4.3.* ***Сканер SMTP-потока*** *— предназначен для проверки данных, передаваемых через шлюз по SMTP.*

14.3 Комплексые средства антивирусной зашиты

14.3.1 Комплексы антивирусной зашиты для сетевых шлюзов

Задача антивируса установленного на шлюзе *— не допустить проникновения вирусов вовнутрь сети через поток данных Интернет.*

Существующие реализации универсальных антивирусов для шлюзов позволяют проверять данные, поступающие по следующим протоколам:

- *HTTP;*
- *FTP;*
- *SMTP.*

Требования к антивирусам для шлюзов:

1. ***Основные требования*** - являющиеся по сути требованием, выполнения антивирусом свою основной задачи:
   1.1. *Проверка Интернет-потоков данных (HTTP, FTP и, возможно, SMTP)* на наличие вирусов и предотвращать проникновение вирусов в сеть.
   1.2. *Проверка составных объектов* - архивов, самораспаковывающиеся архивов, упакованных исполняемых файлоа, почтовых баз, файлов почтовых форматов.
   1.3. *Возможность настраивать действия, которые будут выполняться при обнаружении вредоносных программ в потоках данных*. Стандартными действиями при этом являются - пропустить, удалить, поместить на карантин.
   1.4. *Возможность лечениять зараженных объектов*.
2. ***Требования к управлению****:*
   2.1. *Масштабируемость* — настройки одного сервера должны легко распространяться на другие сервера или группу серверов, особенно если речь идет о массивах серверов Microsoft ISA Server или подобных решениях.
   2.2. *Удаленное управление* — администратор антивирусной безопасности должен иметь возможность управлять всеми антивирусными средствами непосредственно со своего рабочего места.

При проверке протоколов Интернет, сервер антивирусной проверки наиболее оптимально устанавливать перед прокси-сервером, но за брандмауэром, если смотреть со стороны защищаемой сети (рис. 14.9). Впрочем, брандмауэр может и отсутствовать. В этом случае антивирус получает на вход тот же поток, который до этого получал прокси-сервер, выполняет проверку поступающих данных на наличие вредоносного кода и передает уже проверенные данные на прокси-сервер.

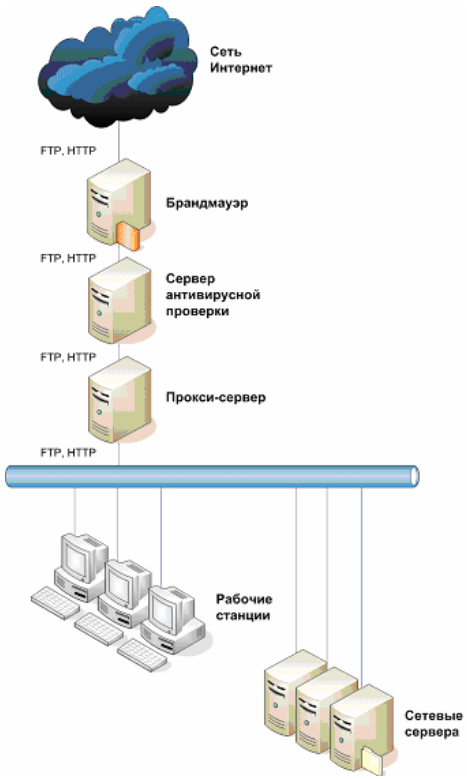

Рис. 14.9 - Установка сервера антивирусной проверки перед прокси-сервером

14.3.2 Комплексы антивирусной защиты почтовых систем

В силу того, что по разным оценкам от 80 до 95 процентов вирусов проникает в корпоративные сети через электронную почту, проверка почтового трафика является одной из важнейших задач обеспечения антивирусной безопасности организации. При этом под почтовым трафиком понимается SMTP-поток. Антивирусные комплексы для защиты почтовых систем не проверяют данные, передаваемые по протоколам IMAP и POP при обращении пользователей к своим персональным внешним по отношению к организации ящикам, поскольку это - задача антивирусного комплекса для защиты рабочих станций. Задачей антивирусного комплекса для почтовой системы является проверка и всего потока писем, поступающих и исходящих из почтовой системы организации.

К почтовому антивирусному комплексу, предьявляются требования, удовлетворение которых существенно упрощает задачу защиты организации от проникновения вирусов через почтовый поток:

1. **Карантин** — кроме удаления и доставки пользователю сообщения, возможна реализация карантинного хранилища - в этом случае пользователю доставляется уведомление со ссылкой на место в карантине, где хранится вложение к его письму.
2. **Добавление информации о проверке в письмо** — в конец проверенного письма, либо в служебный заголовок добавляется

информация о том, что письмо было проверено, а также статус проверки. Указание в таком сообщении версии использованных антивирусных баз, а также точного времени проверки позволит существенно упростить служебные расследования при поражении вирусами узлов сети.

3. **Генерация списка обнаруживаемых вирусов** — может пригодиться для точного определения состояния антивирусного комплекса во время проведения служебного расследования, при условии реализации предыдущего пункта
4. **Возможность выделения различных групп пользователей и задания различных настроек проверки для этих групп** — логичное продолжение требования к возможности исключения пользователей из проверки. Некоторые пользователи, наоборот, могут входить в группу риска, поскольку обрабатывают информацию, составляющую коммерческую либо государственную тайну. Требования к проверке корреспонденции таких пользователей должны быть более жесткими чем обычные.
5. **Возможность модификации уведомлений, в том числе и для различных групп пользователей** — может пригодиться для указания адресов и телефонов, по которым нужно обращаться с вопросами касательно антивирусной защиты.
6. **Возможность блокировки объектов, не прошедших проверку** — в некоторых случаях проверить вложение на наличие вирусов не представляется возможным — к примеру, если это часть многотомного архива либо архив, защищенный паролем. В этом случае антивирусный комплекс должен обладать возможностью блокировать сообщения, содержащие подобные вложения.
7. **Вирусная атака** — при обнаружении *N* вирусов в *M* минут иногда полезно уведомить администратора об этом факте. Подобное поведение продукта скорее всего будет свидетельствовать о вирусной эпидемии либо атаке на сервер. В обоих случаях администратор может попытаться внести изменения в настройки самого комплекса с тем, чтобы отсеивать зараженные письма на более раннем этапе, снижая, тем самым, нагрузку на сервер

Примером антивирусной защиты для почтовых систем может являться VS API 2.0 для Microsoft Exchange Server 2000. Общая схема работы VS API 2.0 приведена на рис. 14.10.

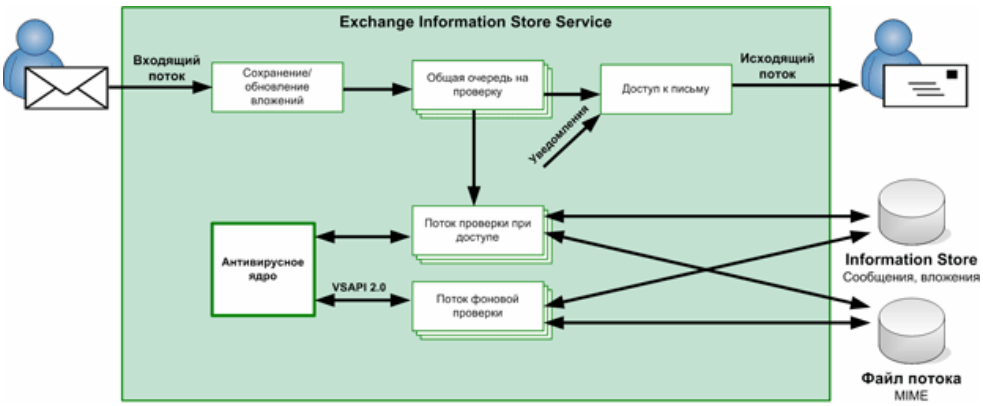

Рис. 14.10 - Схема работы VS API 2.0

14.3.4 Системы централизованного управления антивирусной защитой

Для локальной сети, больше количкство компьютеров, использование системы удаленного централизованного управления антивирусной защитой оказывается максимльно эффективным. Она позволяет администратору на своем рабочем месте обслуживать все рабочие станции и сервера сети:

1. возможность осуществлять полный контроль за вирусной активностью и состоянием антивирусной защиты в сети (основное преимущество),
2. быстро обнаруживать и оперативно устраненять все вирусные инцидентов,
3. удаленно настраивать политики антивирусной безопасности,
4. запускать проверку объектов на наличие в них вирусов,
5. включать или выключать постоянную защиту,
6. централизованно обновлять антивирусные базы,
7. 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.

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 ведется 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 вывести данные с сервера администрирования, на их основе 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.

На рис. 14.11 представлена схема взаимодействия перечисленных компонентов, а на рис. 14.12 - схема сбора и передачи на хранение серверу администрирования данных о состоянии антивирусной защиты.

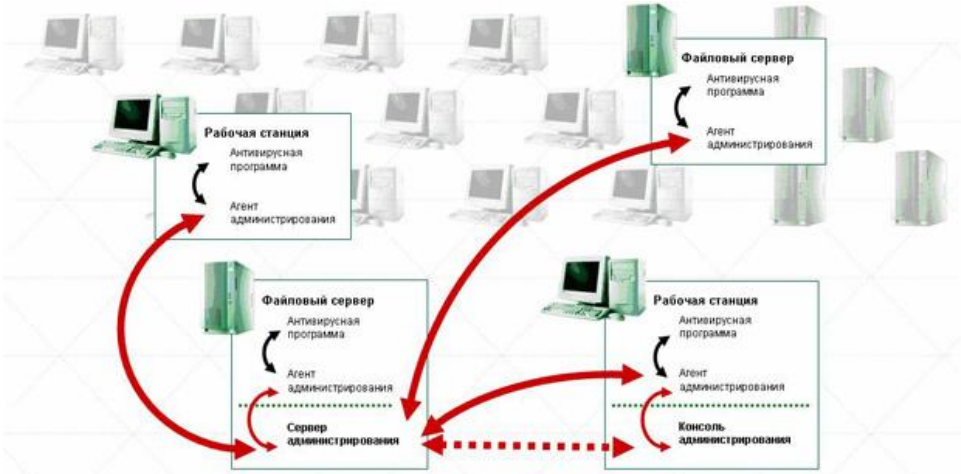

Рис. 14.11 - Схема взаимодействия компонентов централизованно управляемого комплекса антивирусной защиты в сети

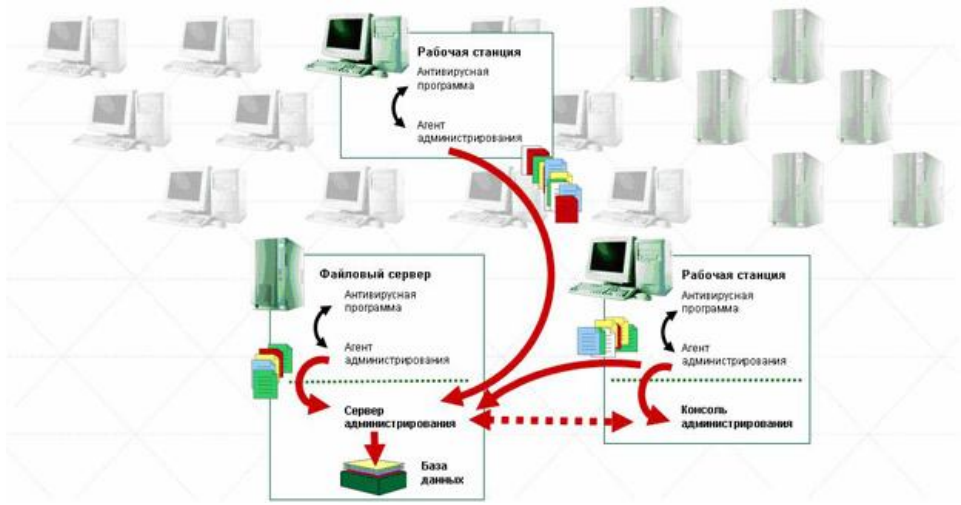

Рис. 14.12 - Схема сбора статистики в системе антивирусной защиты