Александр Жадаев

Антивирусная защита ПК

от «чайника» к пользователю

Санкт-Петербург
«БХВ-Петербург»
2010

УДК 681.3.06
ББК 32.973.26-018.2
Ж15

Жадаев А. Г.

Ж15 Антивирусная защита ПК: от "чайника" к пользователю. — СПб.: БХВ-Петербург, 2010. — 224 с.: ил. — (Самоучитель)

ISBN 978-5-9775-0545-1

Описана настройка средств антивирусной защиты системы Windows 7, даны способы защиты компьютера с помощью бесплатных и наиболее популярных антивирусных программ. Рассмотрена организация защиты от проникновения вирусов из всех источников: Интернета, компакт-дисков, флэш-памяти и др. Рассказано, что такое компьютерные вирусы, черви, троянские программы, где они обитают и какую опасность предоставляют для компьютера. Представлен комплекс мер, включающий настройку операционной системы, установку и настройку антивирусных программ и входящих в них брандмауэров. Подробно рассмотрены бесплатные программы-антивирусы для компьютеров с ОС Windows XP/Vista/7 — Avira AntiVir Personal и Dr.Web CureIt!®. Детально, с помощью простых пошаговых инструкций описана работа с наиболее эффективным на сегодняшний день антивирусом Norton Internet Security, дающим профессиональную и комплексную защиту. Представлен обзор антивирусов фирм McAfee, ESET, Лаборатории Касперского, Panda Security.

Для широкого круга пользователей

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Юрий Рожко*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн обложки	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 29.01.10.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 18,06.
Тираж 2000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.60.953.Д.005770.05.09 от 26.05.2009 г. выдано Федеральной службой
по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0545-1

Оглавление

Введение

В данной книге описаны средства защиты компьютера от вирусов, а также и других опасностей, подстерегающих пользователя ПК при путешествиях в Интернете, работе с компакт-дисками, флэш-памятью и другими носителями информации. В настоящее время задача антивирусной защиты приобрела первостепенную важность, учитывая широкое распространение вирусов, шпионских программ и веб-сайтов с злонамеренным кодом, встроенным в странички сайта.

В книге рассмотрены все вопросы антивирусной защиты. В начале книги, в *главе 1*, описаны все виды вирусов, которые могут нарушить работу компьютера и привести к утере и раскрытию конфиденциальности хранимой на нем информации. Приводится классификация вирусов, рассмотрены способы их проникновения в компьютер. Также обсуждаются программы, нацеленные на похищение информации с компьютера — *троянские программы* или просто *трояны*, описаны разновидности такого рода злонамеренных программ, их классификация и методы проникновения в компьютеры. Все пользователи Интернета, наверное, слышали о компьютерных "*червях*", специальных программах, которые проникают на компьютер пользователя и начинают размножаться, проникая на другие компьютеры в сети или рассылая сами себя по почте. Читатель познакомится с разновидностями этих червей, способами проникновения червей в компьютер и различными примерами червей, наиболее "отличившимися" в нанесении вреда компьютерному сообществу. Наконец, описаны методы компьютерного "зловредства" под названием "*фишинг*" (fishing) и "*спам*" (spam), под которыми подразумевается создание подставных сайтов, имитирующих популярные сайты различного назначения, и рассылка писем рекламного характера по почтовым адресам, извлеченным из различных источников.

Познакомившись с характером вирусных и прочих угроз, подстерегающих всех беспечных пользователей компьютеров, читатель в *главе 2* познакомится

с методами защиты, призванными избавить его от всех опасностей. Описаны способы защиты от вирусов с помощью сканирования компьютера антивирусными программами, построения защитной стены, *брандмауэра* или иначе "файервола" (firewall), между компьютером и средой Интернета, а также использование почтовых фильтров для защиты от спама.

В *главе 3* читатель познакомится с методами настройки системы Window 7 для максимальной защиты компьютера от нежелательных воздействий. Вы узнаете, как следует настраивать файервол, встроенный в систему Windows 7, познакомитесь с методами защиты компьютера с помощью настройки своей учетной записи, техникой определения вредоносных программ с помощью Диспетчера Windows и определения характерных признаков работы злонамеренных программ на вашем компьютере. Общий вывод таков: система Windows 7 предоставляет некоторые важные инструменты защиты ПК от опасностей, подстерегающих пользователей при работе в Интернете и с различными носителями информации, но явно недостаточную. Все это делает важным использование специальных программ защиты, про которые и ведется речь в остальных главах книги.

В *главе 4* мы рассмотрим работу с *бесплатными* программами антивирусной защиты, завоевавшими широкое распространение среди пользователей: Dr.Web CureIt!®, Dr.Web LiveCD, Dr.Web LinkChecker, Avira AntiVir Personal. Эти программы позволят вам решить практически все задачи защиты компьютера от вирусных угроз, не тратя при этом своих денег. Конечно, если ваш компьютер хранит достаточно важную информацию, то было бы разумнее приобрести пакет программ профессионального уровня. Но для многих пользователей использование таких бесплатных пакетов будет оптимальным решением.

Тем не менее, для защиты компьютера на профессиональном уровне настоятельно рекомендуется использование более функциональных программ, и в *главе 5* описана одна из наиболее популярных программ комплексной защиты компьютера — *Norton Internet Security 2010* от известной фирмы Symantec. Эта программа обеспечит домашнему компьютеру полную защиту компьютера практически от всех угроз, которые только существуют в настоящее время. С ее помощью вы сможете отсканировать свой компьютер на предмет заражения вирусами, получить предостережение от использования информации с любого ее носителя — лазерного диска, флэшки, построить надежный файервол от проникновения на компьютер вирусов, червей, троянов, закрыть вам доступ на злонамеренные сайты. Установив эту программу и освоив работу с ней с помощью данной книги, вы сможете превратить свой компьютер в неприступный бастион, которому не страшны никакие угрозы, приходящие из современного компьютерного мира.

Хотя Norton Internet Security 2010 — прекрасная программа, но список такого рода программ ею не исчерпывается. Поэтому в последней *главе 6* мы рассмотрим другие популярные программы, которые, возможно, покажутся вам более подходящими для вашего компьютера. Это набор программ той же фирмы Symantec, предназначенные для защиты офисных и корпоративных сетей, антивирусные решения Лаборатории Касперского, весьма популярные в РФ и странах СНГ, мощные пакеты антивирусной защиты фирмы ESET. Вкратце описана работа со знаменитым пакетом антивирусной защиты *ESET NOD32 Smart Security 4*, включающим в себя как модули антивирусной защиты, так и сетевого экрана. Не обойдены вниманием и пакеты антивирусной защиты фирм Panda Security и McAfee, также предлагающие средства для комплексной защиты домашнего компьютера, небольшой офисной и крупной корпоративной сети.

Прочитав эту книгу, вы овладеете всеми тонкостями антивирусной защиты компьютеров, как домашних, так и офисных, работающих в единой сетевой среде. Чтение ее не предполагает начальной подготовки, от вас требуются только общие знания по работе с системой Windows. Начав с нулевого уровня познаний в области антивирусной защиты, вы, освоив материал этой книги, станете настоящим профессионалом, которому по плечу любые задачи настройки системы информационной безопасности на вашем компьютере.

ГЛАВА 1

Представление о вирусных угрозах

Всем нам, как пользователям компьютеров, так и людям, непосвященным в таинства компьютерной технологии, постоянно приходилось слышать о слове "вирус". Естественно, это слово известно нам давно, еще из медицины. Значение слова "вирус" несло за собой нечто неприятное, губительное, заразное, несущее с собой проблемы. И вот, наступил век информационных технологий, компьютер перестал быть редкостью и находится почти в каждом доме, а ценность информации многократно увеличилась — и что же? Понятие "вирус" пришло и в эту область, в мир компьютерных технологий, который, казалось бы, совершенно далек от мира физического. Оказалось, что компьютеры и информация, находящаяся в них, нуждаются в защите от вирусов. Только речь тут идет не о "обычных" вирусах, а о *компьютерных*, о программах, которые своим поведением очень напоминают вирусы биологической природы.

История компьютерных вирусов очень интересна. Их появление и развитие было неожиданным — специалисты-компьютерщики в те далекие времена считали, что создание такого рода программ просто не имеет смысла. Первыми вирусами можно было назвать шуточные программы, которые не наносили никакого ущерба, а занимались отображением всякого рода картинок и сообщений на терминалах пользователей компьютера. Но время шло, и проблема защиты компьютеров от вирусов стала достаточно актуальной, когда последние стали уничтожать ценную информацию или воровать эту информацию, останавливать работу оборудования и технологические процессы, а иногда даже блокировать работу компьютерных сетей предприятий, ведомств и даже целых стран.

На сегодняшний день создано великое множество самых разнообразных вирусов. Поэтому данная глава книги поможет вам разобраться со всеми видами вирусных угроз. Ведь чтобы бороться с врагом, его нужно знать — эта

аксиома справедлива для компьютерного мира ничуть не меньше, чем для того, в котором мы живем.

1.1. Все о компьютерных вирусах

Вы все прекрасно знаете, что на сегодняшний день информация является очень ценным продуктом. Ее хранение в компьютере нуждается в обеспечении защиты от различных угроз. *Компьютерные вирусы* — самая главная и известная угроза для информации.

Давайте разберемся, что же такое компьютерные вирусы. Если в медицине вирусом является некая инфекция, заражение которой происходит переносом некоего биологического организма (организмов) от одного живого существа к другому, то в компьютерной области вирус — это программа, и заражение ею происходит посредством переноса программ от компьютера к компьютеру. Эти вирусные программы, как и обычные программы, пишутся программистами. Но, в отличие от обычных программ, основной целью вирусных программ является быстрое распространение, т. е. заражение компьютеров, и последующее выживание на инфицированном компьютере. Плюс выполнение какого-либо злонамеренного действия, наподобие уничтожения информации.

Основными отличительными чертами вирусных программ являются:

- вирусные программы приносят только вред: удаляют или похищают данные, закрывают доступ к информации, затормаживают работу компьютера, выводят из строя обычные программы, изменяют настройки BIOS, форматируют диски и многое другое, на что способна фантазия и возможности разработчика этого вируса;
- вирусные программы могут устанавливаться автоматически;
- вирусные программы используют возможность обмана, выдавая содержимое за безопасное и скрывая все это за ложной оболочкой. В таком случае пользователь очень часто сам помогает вирусу заразить компьютер;
- вирусные программы способны к самокопированию.

Это общие черты компьютерных вирусов. Но число разновидностей вирусов велико, как и в живой природе, и каждый вид имеет свои особенности. Познакомимся с некоторыми из них поближе.

1.1.1. Классификация вирусов

Знакомство с вирусами начнем, разделив их на четыре вида:

- загрузочные вирусы;
- файловые;

- вирусы-сценарии;
- макровирусы.

Загрузочные вирусы

Загрузочные вирусы сегодня можно встретить очень редко. Как класс вирусов они постепенно исчезают, поэтому здесь мы их только упомянем. При включении компьютера происходит определение места, откуда загружать операционную систему, и в этот момент запускается загрузочный вирус. Причем загрузочному вирусу все равно, какой тип операционной системы стоит на вашем компьютере. В основном он проживает в загрузочном секторе (MBR — Master Boot Record) жесткого диска и флоппи-дискет.

Файловые вирусы

Файловые вирусы могут размножаться в файловой системе какой-нибудь операционной системы. Принцип заражения файлов и размножения вирусов довольно прост. Размножаются вирусы так: они создают свои копии, которые сохраняются на диске, заражая другие файлы или создавая новые файлы. Но когда вирусы создают новые файлы, это заметно для пользователей, даже если этого не заметил антивирус. Часто вирус создает скрытые файлы и папки, а лучше всего для вируса это заразить файл. Заражение файла происходит, когда вирус создает свою копию внутри какого-нибудь существующего файла. Тем самым, при запуске этого зараженного файла запускается сначала программа вируса, а потом программа файла. Хотя бывает и наоборот, когда запускается файл программы, а с наступлением какого-либо события в работе программы запускается вирус. Существует много различных вирусов:

- вирусы-компаньоны, которые переименовывают и скрывают оригинальный файл, а на его месте создают свою копию;
- вирусы, которые заменяют своим кодом содержимое других файлов, причем полностью;
- паразитические вирусы;
- link-вирусы и др.

Известно несколько способов заражения файла вирусом, рассматривать которые мы не будем, а только перечислим:

- внедрение вируса в начало файла (это когда код программы сдвигается);
- внедрение вируса в конец файла;
- внедрение вируса в середину файла;
- внедрение вируса в свободные места по всему файлу.

Эти способы заражения полезно знать тем, кто разрабатывает антивирусы. Поэтому более подробную информацию о способах вы сможете найти в соответствующей литературе.

Файловые вирусы — это самые распространенные вирусы. Их происхождение зависит от среды какой-либо операционной системы. Первым вирусом для операционной системы Linux можно считать появление в феврале 1997 году вируса Bliss. Что касается операционной системы Windows, то она является самой популярной на сегодняшний день, но это не значит, что самой безопасной. Скорее наоборот, именно эта операционная система в силу своей популярности подвергается нашествию наибольшего количества вирусов.

Первым вирусом, заражающим файлы 64-битной версии операционной системы Windows, был вирус Rugrat, созданный в мае 2004 года. Не остались без внимания вирусов и мобильные телефоны, коммуникаторы, смартфоны и другие подобные устройства. Так, например, в том же 2004 году в июне появился первый вирус-червь Cabir для смартфонов с операционной системой Symbian. Следующий месяц — июль 2004 года — стал месяцем рождения первого вируса Duts для коммуникаторов с операционной системы Windows Mobile. И даже новые всем известные телефоны iPhone не смогли уберечь от вирусов. Уже в январе 2008 года одиннадцатилетний школьник написал вирус 113prep для таких телефонов.

Файловые вирусы встречаются наиболее часто, имеют различные виды и способы действия, поэтому они популярны и для разработчиков вирусных программ, и для разработчиков антивирусных программ.

Вирусы-сценарии

Вирусы-сценарии — это класс вирусов, которые являются сценарием, а не исполняемым файлом, что отличает их от файловых вирусов. Например, это могут быть файлы PHP, BAT, VBS и JS для исполнения в среде операционной системы Windows. Такие вирусы, как и класс файловых вирусов, также находятся в файловой среде какой-либо операционной системы. Давайте рассмотрим вирусы-сценарии подробнее.

- *Файлы PHP*. Вирус в файле PHP не опасен пользователям домашнего компьютера. Этот вирус-сценарий опасен лишь если компьютер работает в качестве веб-сервера, или когда в операционной системе Windows установлена специальная среда для этого сценария.
- *Файлы BAT*. Команды в таких текстовых файлах записаны на своем языке программирования. Это могут быть не только команды, но и имена программ, циклы, переходы, условия. Используемый для этого язык достаточно развит для создания вируса, который начинает свою деятельность при запуске файла BAT.

- *Файлы в ОС Windows*. Операционная система Windows поддерживает работу сценариев различных типов, и все эти сценарии имеют широкий спектр возможностей по работе с информацией, хранимой на компьютере. Самым опасным является то, что при запуске сценариев на языках VBS и JS не появится никаких предупреждений.
- *Файлы VBS и JS*, заражающие HTML-файлы. HTML-файлы открываются браузерами, самыми известными из которых являются Opera, Mozilla Firefox, Internet Explorer. Наиболее уязвимым для вирусов является браузер IE, т. к. только он разрешает использовать ActiveX-объекты, т. е. встроенные в код веб-странички небольшие программы. Если эта программа — злонамеренная, то технология ActiveX дает вирусу возможность действовать на зараженном компьютере практически без ограничений. Также HTML-файлы, реализующие веб-странички, могут содержать сценарии на языках VBScript и JavaScript, которые вполне пригодны для написания вирусов.

Макровирусы

Макровирусы — популярные вирусы, которые встречаются довольно часто. Их существование зависит от какой-нибудь программы, поддерживающей язык, на котором написан макровирус. Макровирусы являются сценариями исходной программы, и в виде отдельных файлов никогда не распространяются, они встроены в файл, созданный программой. Причем программа должна поддерживать свой макроязык, средства которого напрямую определяют возможности макровируса, написанного на этом языке.

Очень важна для макровируса возможность макроязыка в исходной программе запускать сценарии. Если сценарий запускается пользователем, то макровирус теряет масштабы своего действия. Но если сценарии в исходной программе запускаются автоматически при открытии файла, то масштаб вреда может быть большой. Особенно опасны действия макровируса, когда макроязык исходной программы позволяет работать с файловой системой вашего компьютера.

Многие из нас постоянно пользуются программами Microsoft Office, они являются очень популярными и имеют свой макроязык. Это очень благоприятная среда для макровирусов, потому что возможности макроязыка пакета Microsoft Office очень широки. Сценарии в таких программах запускаются автоматически. Например, при открытии документа Microsoft Word исполняются макросы AutoOpen и Document_Open, при закрытии документа — макрос Document_Close, при сохранении документа исполняются макросы FileSaveAs и FileSave, при печати документа — макрос FilePrint и др.

Макровирусами могут быть заражены не только документы Microsoft Office, но и файлы-документы других программ. Так, например, в 1999 году макро-

вирусы появились в файлах-документах программ CorelDRAW, Corel VENTURA, Corel PHOTO-PAINT. В 2000 году появился макровирус, заражающий файлы проектов AutoCAD. Но лидирующее место по числу макровирусов занял все-таки пакет Microsoft Office. Поэтому компания Microsoft предприняла решительные действия на устранения этой проблемы, и уже в последних версиях пакета Microsoft Office запуск сценариев осуществляется не автоматически, а вручную. Только пользователь может разрешить запуск сценария макровируса.

1.1.2. Вирусы на вашем компьютере

Как же вирус проникает на ваш компьютер и что он там может заразить? Обсудим этот вопрос.

Разработчикам вирусов для его распространения удобнее всего выложить свою злонамеренную программу в Интернет, хорошенько его замаскировав. Поэтому основной причиной появления вирусов является Интернет, в котором вы легко можете скачать программу или файл, зараженный вирусом. Файловые вирусы, как правило, содержатся в исполняемых файлах, имеющих расширения EXE и COM. После запуска такого файла содержащийся в нем вирус может заразить все исполняемые файлы на вашем компьютере. Но, как уже говорилось, сейчас разработаны вирусы, способные заражать и другие типы файлов:

- файлы графического пакета CorelDRAW, Corel VENTURA и Corel PHOTO-PAINT;
- файлы пакета AutoCAD;
- файлы заставки ОС (SCR-файлы);
- файлы помощи Windows (HLP-файлы);
- апплеты, запускающие практически все инструменты Панели управления (CPL-файлы);
- VBS-файлы;
- PIF-файлы и т. д.

Совершенно не стоит бояться текстовых файлов с расширением TXT, в них никогда не смогут появиться вирусы. Но не забывайте о текстовых документах Microsoft Office, в файлах которых могут находиться макровирусы.

Как вы уже поняли, вирусы способны на многое, однако сами по себе зародиться у вас в системе они не могут. Вирус может попасть к вам из Интернета в виде какой-либо троянской программы или червя. Вы можете сами занести его в компьютер с какого-либо сменного носителя информации. Например,

достаточно установить в разъем USB популярный флэш-накопитель с вирусом и попробовать открыть появившийся раздел в Проводнике, как тут же, в зависимости от настроек, сработает система автозапуска и запустится программа, указанная в файле AUTORUN.INF. Если эта программа — злонамеренная, то первым делом она поможет вирусу проникнуть на ваш компьютер. Естественно, вирусы не сразу атакуют ваш компьютер, а только после запуска программы, в которой они находятся. Поэтому вот вам совет: всегда проверяйте на наличие вируса подозрительные и незнакомые программы, они могут быть вредоносными.

1.2. Троянские программы

Если файловый и другой вирус живет и размножается, заражая информацию у вас на компьютере, то принцип действия троянской программы совсем другой. Она не только может уничтожать информацию, но и воровать ее, управлять какими-либо процессами и многое другое.

В виртуальном мире мы постоянно сталкиваемся с регистрацией на каких-то веб-страничках, с созданием аккаунтов, постоянно придумываем логины и пароли для использования тех или иных ресурсов. Это могут быть игры, банковские счета, кошельки платежных систем, интернет-магазины и многое другое, доступ к чему является ценной и конфиденциальной информацией. Именно логины и пароли воруют троянские программы, называемые "*spyware*", т. е. программы-шпионы.

Существуют, конечно, и другие типы троянских программ, нацеленные на иной результат. Но большинство вирусописателей создают троянские программы, а также и другие "трояноподобные" программы, которые заняты похищением всякого рода конфиденциальной информации.

В отличие от файлового вируса троянская программа не размножается. Троянская программа может быть отдельной программой, или же быть реализованной в виде скрытой функциональности какой-либо программы, которая собирает необходимую ценную информацию или воздействует на работу вашего компьютера. Таким образом, троянская программа может находиться и в маленькой игре, и в увлекательной программе (наподобие "Подбор причесок", "Физические формулы" и т. д.), которую вам принесли или вы скачали с Интернета.

Но для того чтобы эта скрытая функциональность программы заработала, необходимо установить эту игру или подобную "интересную" программу на свой компьютер и запустить ее работу. После этого вы не заметите, как троянская программа начнет "действовать" в интересах ее создателя.

Даже мобильные телефоны, исполняющие Java-приложения (J2ME), стали уязвимы. Так в 2006 году первой троянской программой для таких мобильных телефонов стала программа Red Browser. Что касается других ОС, то разработчики создавали троянские программы для Mac OS, UNIX, не обошли и операционные системы карманных компьютеров Pocket PC и Palm Pilot.

Иногда троянскую программу называют троян, троянец, троянский конь, трой. Разработчики вредоносных программ могут замаскировать троянскую программу так, что вы сами ее скачаете, установите и запустите на своем компьютере. Например, вполне возможно, что для этого какая-либо программа потребует у вас загрузить обновление, или кодек, или какую-то дополнительную информацию, и вы, поддавшись на запрос, загрузите троянскую программу. Или вы получите письмо со ссылкой, приглашающее вас загрузить некую ну очень интересную для вас информацию. Таких мошеннических приемов очень много, и все они составляют то, что по-научному называют "социальной инженерией".

Троянских программ написано немало. Познакомимся с некоторыми их разновидностями.

1.2.1. Виды троянских программ

Троянские программы можно условно разделить на следующие виды по выполняемым вредоносным действиям:

- шпионские и рекламные программы, программы дозвона;
- утилиты несанкционированного удаленного администрирования (такие утилиты позволяют злоумышленнику удаленно управлять зараженным компьютером);
- утилиты для проведения DDoS-атак (Distributed Denial of Service — распределенные атаки отказа в обслуживании);
- серверы рассылки спама;
- многокомпонентные троянские программы-загрузчики (переписывают из Интернета и внедряют в ОС различные вредоносные программы).

Часто можно встретить троянские программы, которые относятся сразу к нескольким вышеперечисленным видам. Опишем некоторые классы таких программ, подразделив их по функциональным возможностям.

- *Backdoor* — содержит в себе RAT-функцию (RAT — Remote Administration Tool — утилита удаленного администрирования). Эта функция позволяет злоумышленнику удаленно управлять вашим компьютером.
- *PWS* — это "троянский конь", который ворует пароли. Как правило, префикс такой вирусной программы дополняется словом "Trojan.", например,

Trojan.PWS. Это могут быть все пароли, данные о системе, регистрационная информация от лицензионных программ, установленных на вашем компьютере, номера телефонов, адреса электронной почты.

- *Trojan-Spy* — имеет такие же цели, как и класс троянских программ PSW. Служит для передачи информации. Этой информацией могут быть снимки экрана, аудиоданные (при наличии подключенного к компьютеру микрофона), видеоданные (если к компьютеру подключена веб-камера), набранная на клавиатуре информация.
- *Trojan.Clicker* — троянская программа, которая различными способами заставляет пользователя открыть веб-страницу какого-то специально созданного сайта. Программа выполняет установку страницы в качестве домашней страницы браузера, с помощью коррекции файла hosts меняет IP-адрес популярного сайта на IP-адрес хакерской веб-страницы, а уж к чему это приведет, зависит от цели, которую преследуют создатели трояна.
- *Trojan-Notifier* — после установки этой троянской программы она попытается передать информацию о степени зараженности, конфигурации и настройках инфицированного компьютера своему создателю. Казалось бы, что эта программа не несет таких страшных последствий. Но после этого могут последовать и другие атаки, бывает, приводящие к очень тяжелым последствиям.
- *Trojan-Dropper* — класс троянских программ, в составе которых находятся программы вирусов и другие нежелательные программы, автоматически устанавливающиеся на ваш компьютер. Эту автоматическую установку вы можете даже не заметить, т. к. она прикрывается установкой другой программы, т. е. троянская программа устанавливает их параллельно с другой, безвредной программой, в фоновом режиме.
- *Trojan-DDoS* — DDoS (Distributed Denial of Service) — распределенный отказ в обслуживании. Такой класс троянских программ предназначен для атаки конкретного сайта, скажем, интернет-магазина, со злонамеренной целью, например, шантажа. Вред такая программа принесет больше хозяину атакуемого сайта, но и вы можете понести потери. Например, исчерпать лимиты трафика, установленные провайдером Интернета, а в случае расследования вашим компьютером могут заинтересоваться правоохранительные органы.
- *Trojan-Proxy* — такой троян реализует прокси-сервер, т. е. компьютер-посредник, через который вы можете соединяться с Интернетом или с другой сетью. При этом вы будете использовать посторонний IP-адрес, присвоенный вам прокси-сервером. Цель такой программы — скрыть реальный IP-адрес хакерского компьютера, заменив его чьим-либо другим IP-адресом. Таким образом, с вашего IP-адреса при помощи такого рода

трояна могут рассылать спам, проводить атаки и совершать любые другие преступления.

- *Trojan-Downloader* — при помощи этой программы на ваш компьютер загружаются вирусы и другие вредоносные программы. Этот "троян" просто скачивает их с Интернета и далее устанавливает на ваш компьютер.

1.2.2. Примеры троянских программ

А теперь познакомимся поближе с некоторыми, наиболее часто встречающимися, примерами троянских программ.

Наибольшую известность в настоящее время получили троянские программы *Back Orifice*, *Net Bus* и *SubSeven*. Группа разработчиков Back Orifice именует себя Cult of Dead Cow (Культ мертвой коровы).

А вот другая, также очень интересная, троянская программа *AOLGOLD*. Существует такой крупнейший американский интернет-провайдер America Online (AOL). И вот, эта троянская программа рассылалась ее авторами в виде заархивированного файла по электронной почте вместе с сопроводительным письмом, в котором сообщалось, что программа AOLGOLD предназначена для повышения качества услуг провайдера AOL. Архив состоял из двух файлов, один из которых именовался INSTALL.BAT, который мог стереть все файлы из каталогов C:\, C:\DOS, C:\WINDOWS и C:\WINDOWS\SYSTEM на вашем жестком диске.

Троянская программа *MonaRonaDona* автоматически запускается при входе в систему. Любопытно то, что троян меняет в браузере Internet Explorer вашу стартовую страницу на страницу со статьей о правах человека, а также завершает работу некоторых приложений (Adobe, WMP, Winamp, Microsoft Office и т. д.). Когда же вы в очередной раз посетите Интернет, вам предложат купить программу для удаления этого трояна.

Троянская программа *Sinowal.FY* действует по такому же принципу, она шифрует файлы на зараженном компьютере и предлагает купить программку для расшифровки. Многим стала известна троянская программа *Win32.Ntldrbot*, которую очень долго не мог определить ни один антивирус, благодаря ее способностям скрываться в компьютере.

Какие только уловки, хитрости и любые изощрения можно встретить в троянских программах! Поэтому их существует огромное количество. Вот краткий список подобных троянских программ: SpyAxe, Zeus, AttachMsngr.G, Zlob, Brave Sentry, Trojan.BAR.Tiny.a, Pinch, Pest Trap, SpywareQuake, Prorat, LiveDeath.A, Sohanat.DB, Vundo, Adware Sheriff, Trojan.BAT.KillWin.dg, Alpha Cleaner, AntiVirGear и многие другие.

1.3. Черви

Черви относятся к вредоносным программам, распространяющимся между компьютерами чаще всего без всякого участия пользователя. Это основное свойство червя — воспроизводить себя на компьютере. Червь можно принести на компьютер вместе с файлом, который в дальнейшем нужно запустить. Также червь может оказаться на компьютере и не по вине пользователя: он сам создается на компьютере, когда операционная система или программное обеспечение содержит много ошибок. Чтобы не допустить этого, необходимо устанавливать обновления для используемой ОС или программы. Чем дольше червь находится в системе вашего компьютера, тем больше вреда он приносит.

Хотелось бы еще отметить, что червь может перенестись на другой компьютер при помощи электронной почты, программ мгновенного обмена сообщениями, IRC-чатов и других средств интернет-общения. Также вы можете активировать червя сами, запустив какую-нибудь вредоносную программу, щелкнув на ссылке в полученном письме. Поэтому будьте внимательны и используйте средства для их обнаружения. А далее давайте рассмотрим виды компьютерных червей.

1.3.1. Виды компьютерных червей

Можно поделить червей по видам в зависимости от способа их распространения. Рассмотрим следующие известные виды компьютерных червей:

- *сетевые черви* (способ распространения — протоколы Интернета и локальных сетей). Этот вид червей может: посылать свою копию на сетевые ресурсы, включая ресурсы публичного использования; проникать на другие компьютеры через уязвимость в ОС или приложений; заражать другие вредоносные программы удаленного администрирования;
- *почтовые черви* (способ распространения — электронная почта). Когда почтовый червь попадает на ваш компьютер, он посылает на все адреса вашей электронной почты письма с вредоносной ссылкой или файлом. Кстати, этот червь был очень популярен, т. к. наряду с некоторыми троянскими программами в основном он рассылал большинство вредоносных файлов;
- *IM-черви* (способ распространения — системы мгновенного обмена сообщениями). Этот вид червей использовал такие программы, как ICQ и подобные ей. Как и почтовые черви, выбирал из списка контактов пользователей и посылал им сообщения со ссылкой на вредоносный файл;
- *IRC-черви* (способ распространения — каналы Internet Relay Chat). Такой вид червей очень похож на IM-черви, т. к. IRC-черви в IRC-сетях также

отправляют сообщения с вредоносной ссылкой пользователям из вашего списка. Но такие черви могут отправить и вредоносный файл, который неопытный пользователь может по ошибке запустить и установить на свой компьютер;

- *P2P-черви* (способ распространения — пиринговые файлообменные сети). Все вы прекрасно знаете, что такое файлообменные сети. Именно в этом месте и заводятся P2P-черви. Способ распространения таких червей очень необычен. Они создают свои копии с привлекательными именами в каталоге файлов для скачивания, и какой-либо пользователь естественно может скачать новые файлы с таким "привлекательным" названием, например, "Как взломать электронный кошелек" или "Бесплатные пароли к платным сайтам" и т. д.

Если делить червей по принципу действия, то можно выделить два вида.

- *Обычные черви*. Действуют как обычные вирусы. Попадают на ваш компьютер, создают там свою копию, затем развиваются и ведут поиск всевозможных сетевых, почтовых адресов других пользователей.
- *Пакетные черви*. В отличие от обычных червей такие черви в виде сетевых пакетов попадают на ваш компьютер и никакие файлы не заражают. Они пытаются заразить оперативную память и достичь своей цели, например, сбор конфиденциальной информации. После перезагрузки системы вы уже не узнаете, что на нем "поработал" сетевой червь.

1.3.2. Примеры червей

Червей существует очень много. Рассмотрим некоторые примеры червей, известных широкому кругу пострадавших:

- *Lovesan* — червь использует уязвимые места в безопасности программного обеспечения компьютера, что приводит к быстрому его распространению внутри сети с большим числом станций. Червь увеличивает загрузку каналов связи и может полностью парализовать сеть. Для производственных непрерывных процессов это бывает весьма значимый урон;
- *Sasser* — червь действует по такому же принципу, как и ранее рассмотренный Lovesan. Таким же образом может остановить работу сети;
- *RogueMario.A* — этот червь очень оригинален по принципу действия. Он устанавливает на зараженном компьютере игру Mario Bros;
- *Mytob* — этот червь соединил в себе два способа распространения. Одна функция распространения через электронную почту, другая — через уязвимость в службе LSASS;
- *Storm* — некоторые относят данный пример угроз к троянским программам, некоторые к червям. Ведь этот червь содержит и функции "трояна", и

функции червя по способу проникновения и разрушения. Такой вид червя считали самым зловредным из всех известных, потому что этот червь заразил за короткое время большое количество компьютеров;

- *Conficker* — червь может добавить на съемный диск определенный файл, и в диалоговом окне автозапуска этого диска появляется дополнительный вариант выбора действия с этим диском, который и приведет к плохому результату. Червь способен реализовать удаленное управление вашим компьютером, если не установлены обновления для системы безопасности вашего компьютера. Таким образом, ваш компьютер превращается в сетевого "раба" хакера, который с помощью удаленного управления получает полный контроль над вашей системой. Итогом может быть потеря конфиденциальной информации или ее разрушение — все зависит от прихоти хозяина.

1.4. Потенциально нежелательные программы

Потенциально нежелательными программами (PUPs — Potentially Unwanted Programs) могут являться обычные программы, которыми вы пользуетесь повседневно. Они совершенно легальны и многим известны. Тем не менее антивирус относит их к нежелательным программам, но всего лишь потенциально, т. е. такие программы сами по себе безвредны, но могут стать опасными при выполнении ряда условий.

Например, на ваш компьютер может быть установлена полезная программа удаленного управления, которой пользуются многие системные администраторы для настройки сетевых компьютеров. Если злоумышленник сможет перехватить управление этой программой, взломав пароль доступа, то ваш компьютер попадет под полный его контроль.

В настоящее время к условно нежелательным программам можно отнести программы классов Pornware, Adware и Riskware.

- *Pornware* — это программы, которые несут информацию порнографического характера. Они открывают ее пользователю без его согласия (картинки, порнографические сайты);
- *Adware* — такие программы очень распространены. При загрузке пользователем определенных сайтов нежелательные программы автоматически открывают страницы с рекламными объявлениями, воспользовавшись которыми наивный пользователь может понести значительные потери;
- *Riskware* — это обычные программы, которые в руках злоумышленника могут причинить вред вашему компьютеру (нарушить работу компьюте-

ров или сетей, уничтожить, блокировать, исказить или скопировать информацию). Это могут быть такие программы, как клиенты IRC, утилиты для загрузки файлов, работы с паролями и многие другие.

Существуют и некоторые другие нежелательные программы:

- *ArcBomb* — это архив, при открытии которого компьютер может зависнуть либо возникнет ошибка в работе операционной системы. Такие архивы могут содержать большое количество одинаковых файлов, либо файл огромных размеров;
- *Bad-Joke* — дословный перевод названия "плохая-шутка" хорошо отображает функции этого червя. Такие программы могут очень сильно напугать пользователя, если, например, в виде "шутки" вам отобразят сообщение о начале форматирования жесткого диска. Но потом все это окажется "всего лишь" только шуткой. Таких нежелательных программ большое количество, и все они имеют различные принципы действия;
- *ложные антивирусные* и *антишпионские программы*. Представьте ситуацию, когда вы, поддавшись рекламе на каком-то сайте, загрузили и установили антивирусную программу в надежде очистить от вирусов свой компьютер. А потом оказывается, что вы сами, своими же руками, создали для него большую угрозу. Угрозой являются вредоносные программы, которые маскируются под этим антивирусом. И самое страшное, что люди верят таким объявлениям на сайтах и продолжают устанавливать неведомо кем созданные программы. После чего эти программы, бывает, просят у вас деньги за очистку вашего компьютера от них же самих. Так что не поддавайтесь никаким уловкам, помните, что только настоящие фирменные программы, загруженные из надежных источников, могут считаться безопасными.

1.5. Фишинг

Фишинг (fishing) переводится с английского как рыбная ловля, выуживание. Фишинг это вид интернет-мошенничества, целью которого является получение ваших конфиденциальных данных.

Принцип действия фишинга довольно прост: от имени известной фирмы или бренда ведется рассылка писем, в которых указывается вредоносная ссылка. Эта ссылка ведет вас на сайт, *подобный* фирменному сайту, но на самом деле являющемуся только *копией*, которая, помимо всего прочего, содержит обычную форму для регистрации на данном ресурсе (поля ввода логина и пароля). Введенные в форму сведения пересылаются хакеру, который далее может зарегистрироваться под вашим именем на настоящем, подлинном сайте, и воспользоваться вашими ресурсами, скажем, счетом в интернет-банке.

Основной характеристикой фишинга является высокое качество подделки сайтов. При фишинге не может быть сайта с таким же интернет-адресом, как у оригинального сайта, но нечто подобное — вполне реально. Например, в интернет-адресе поддельного сайта вместо буквы "o" может стоять нуль "0", что может быть незамечено пользователем — часто ли мы смотрим на текст в поле адреса своего браузера?

Фишингом может являться и обычное сообщение с просьбой предоставить конфиденциальные данные. Эти данные злоумышленникам нужны для получения денег, например, это может быть запрос тех же паролей входа в интернет-ресурс, якобы нужный администратору сайта для восстановления вашей учетной записи. Наиболее часто методом фишинга атакуют банки, электронные платежные системы, аукционы, т. к. такие данные дают непосредственный доступ к деньгам. Персональные данные вашего почтового ящика пригодятся тем, кто рассылает вирусы.

Технологии "фишеров" постоянно совершенствуются. Наряду с фишингом появилось похожее по принципу действия явление как фарминг (pharming). Фарминг является также интернет-мошенничеством, только здесь хакеры получают конфиденциальные данные прямо с оригинала сайта без применения почты. Происходит это путем подмены интернет-адреса официального сайта поддельным адресом, пользуясь некоторыми, достаточно продвинутыми, возможностями протоколов работы Интернета. При этом вы вводите в адресную строку браузера корректный адрес нужного вам сайта, но попадаете на поддельный, хакерский сайт. Опасность фарминга состоит в сложности выявления различий между поддельным сайтом и официальным.

1.5.1. Атаки фишеров

Что касается атак фишеров, то они могут носить целевой и случайный характер. *Целевой фишинг* — это случай достаточно сложный и бывает довольно дорогим для мошенников. Их целью являются конфиденциальные данные конкретного адресата, т. е. необходимо узнать каким банком, какой платежной системой, провайдером и другими ресурсами пользуется данный конкретный человек. Для этого ему нужно соответствующим образом преподнести ложную информацию, создать условия для того, чтобы адресат поверил этой информации и выдал необходимые сведения конфиденциального характера.

Случайный фишинг — это атаки случайные, в основном применимые для аукционов (например, Ebay). Хакеры рассчитывают на то, что вероятность попадания нужного им человека в число пользователей аукциона высока, т. к. аукционы и подобные проекты посещаются многими людьми. Часто подвергалась фишингу и платежная система PayPal.

Фишерская ссылка может привести не только к воровству конфиденциальных данных. Следуя по этой ссылке можно получить троянскую программу, программу-шпиона и другое вредоносное программное обеспечение.

1.5.2. Антифишинг

Фишинг продвигается вперед благодаря низкому уровню знаний пользователей о компаниях и их правилах, от имени которых действуют мошенники. На сайтах разных компаний очень часто содержатся предостережения об угрозе фишинга, о том, что они никогда не требуют конфиденциальной информации и т. д. Но пользователей все равно продолжают обманывать, и все больше людей несут убытки.

Поэтому несколько лет назад было решено создать *антифишинговую группу*, которая называется Anti-Phishing Working Group (APWG). APWG занималась борьбой с фишингом. В эту группу входили компании, которые постоянно атаковали фишеры, и компании-разработчики специального антифишингового и антиспамерского программного обеспечения. Члены этой группы информируют друг друга о новых атаках и угрозах. Также проводятся мероприятия по информированию пользователей о проблеме фишинга, даются рекомендации о методах защиты от фишинга. На данный момент уже около 2500 IT-компаний, крупных мировых банков и других организаций входят в состав APWG. Можно констатировать, что в настоящее время прилагаются большие усилия по защите пользователей от фишеров.

Основной защитой от фишинга на сегодняшний день являются спам-фильтры. Самые популярные браузеры содержат такие фильтры. Принцип действия антифишингового фильтра прост. Существует база фишинговых сайтов, которая постоянно пополняется. Фильтр браузера посылает запрос в эту базу, и в случае положительного результата выводит на страницу уведомление об опасности сайта. Фильтр в браузере может быть выключен, так что обязательно включите его, он может вас спасти от больших потерь. Но всегда имейте в виду, что бывают случаи, когда база фишинговых сайтов еще не успела обновиться новыми сайтами. Поэтому при посещении такого сайта вы никакого уведомления не получите, следовательно, ваша безопасность оказывается в ваших руках. Будьте бдительны!

1.5.3. Нигерийские письма

Одним из популярных видов интернет-мошенничества являются "нигерийские письма". Не трудно догадаться, что такое название письма получили по той причине, что большое распространение эти письма получили в Нигерии. Такие письма писались на обычной бумаге и посылались по обычной почте

еще до появления Интернета. Рассылка писем шла и от других африканских стран, и некоторых европейских (Мадрид, Лондон, Амстердам и др.). Также есть мнение, что название таких писем произошло из-за того, что в содержании речь шла о нигерийских бизнесменах.

Смысл писем довольно разнообразен, но все они несут одну цель — получение денег. В письмах могут просить о помощи перевести большую сумму с одного банка в другой, и за это вам дадут процент с перевода. То есть вы выступаете в роли посредника. При согласии на такие операции с вас могут постепенно выманивать деньги на уплату взяток, сборов, сделок и тому подобное. Иногда у вас могут при помощи нигерийских писем просить номер счета в банке и пароль. Эта ситуация по выманиванию денег может длиться очень долго, до тех пор, пока пострадавший не одумается и не заподозрит обман.

Чтобы заинтересовать пользователя, ему могут послать несколько документов, в которых используются подлинные печати и бланки крупных фирм и правительственных организаций. Таким документам верят, к сожалению, многие.

1.6. Спам

Слово "спам" (spam) своим появлением на свет обязано рекламе ветчины. Этот термин имеет свою историю, о которой вы можете узнать в Интернете. Для нас смысл термина "спам" уже известен, и многие из вас, надо думать, уже столкнулись с этой проблемой. Давайте все же рассмотрим, что же собой представляет смысл слова "спам".

Достаточно точное определение спама дала "Лаборатория Касперского": *спам — это анонимная массовая непрошенная рассылка*. Такое определение точно показывает все важнейшие характеристики спама.

- Анонимность — поскольку рассылки генерируются автоматически, в них используются скрытые или фальсифицированные обратные адреса.
- Массовость — рассылки идут по тысячам адресов, создавая проблемы для пользователей.
- Отсутствие запроса — под таким видом рассылок никто не подписывался, и запроса поступившей информации с вашей стороны не было. Тем не менее, к вам регулярно приходят все новые письма с назойливой рекламой товаров и услуг, просьбой перечислить деньги на лечение, присоединиться к какому-то политико-общественному движению и прочее тому подобное — всего не перечислишь.

Ни в коем случае не путайте обычные рассылки со спамом. Обычные рассылки могут вам приходить, если вы подписались на них (журнал, новости, горо-

скоп и т. д.). Даже если вы не подписывались, то рассылка, в письме которой вы найдете слова о возможности отписаться от нее, не является спамом.

Людей, которые отправляют такие письма в массовом количестве, называют "спамерами". В своих почтовых рассылках спамеры не обязательно рекламируют что-либо или делают некие коммерческие предложения. Спамом называются любые массовые и непрошеные письма. Это могут быть и рассылки политического спама, и благотворительный спам и т. д. Ранее мы рассматривали компьютерные угрозы, такие как фишинг и нигерийские письма. Такие виды рассылок также являются спамом, только он уже мошеннический. Не стоит переходить по ссылкам в спамерских письмах, потому что спам может быть вирусным, а ссылки могут оказаться вредоносными.

С таким почтовым мусором обходитесь осторожно: рассылки, содержащие рекламу, лучше сразу удаляйте, а к коммерческим предложениям относитесь с опаской.

1.6.1. Вред от спама

Спам на сегодняшний день представляет техническую, экономическую, политическую и даже социальную угрозу. Поэтому с ним нужно бороться. Перечислим, какой же вред может принести спам.

- *Потеря времени*. Если ваш почтовый ящик является конечным для рассылки, то вам будет прислано огромное количество спама, и вычищать ящик от спама вам придется очень долго, а главное — постоянно. Если этот электронный ящик является вашим рабочим, то вы, безусловно, потеряете на этом занятии много рабочего времени.
- *Случайная потеря нужного письма в пачке спама*. Достаточно много людей получают ценные важные письма, которые ни в коем случае нельзя потерять. Бывает, что затраты от потери такого важного письма слишком высоки, поэтому этот пункт действительно является важным для многих.
- *Нагрузка на коммуникации*. Спам очень часто приходит в больших объемах, следовательно, засоряет каналы связи. Создает лишний трафик, который оплачивает провайдер или пользователь. Существуют еще и почтовые серверы, для которых спам это огромная проблема.
- *Раздражение и недовольство*. Эмоциональный фактор тоже является проблемой. Бывает, что огромное количество "почтового мусора" очень долго надо убирать.
- *Криминализация спама*. Это самый существенный вред, который может нанести спам. Рассылки спама как преступления стали многовекторными, т. е. могут причинить вред по разным направлениям. Одних только спосо-

бов вытягивания денег с пользователя существует большое множество. Не стоит забывать, что спам может содержать вирусы, которые могут принести серьезный ущерб и вашему компьютеру, и сети какой-нибудь компании. Это мы еще не затрагиваем политические, социальные и другие аспекты криминализации спама, а ведь письмо может нести за собой любую угрозу, не только компьютеру, но и человеку.

1.6.2. Методы борьбы со спамом

Далее перечислим самые известные и наиболее распространенные технологии борьбы со спамом.

- *Черные списки DNSBL* (DNS-based Blackhole Lists). Отправив подозрительный источник в черные списки, вы полностью отсекаете почту из этого источника. Но черные списки могут ложно сработать и не пропустить какое-нибудь на самом деле важное письмо.
- *Контентная фильтрация*. Происходит анализ тем спамерских сообщений и их частей на наличие специфических для спама слов, картинок, фрагментов текста и другого. Поэтому технология является проверенной, а спам-фильтры проверяют все части сообщений. Но недостатком спам-фильтра является необходимость в обновлениях и дорогостоящих настройках. Достаточно известна контентная фильтрация — байесовская. Она не нуждается в постоянной настройке, ей достаточно заранее настроиться на тематику писем пользователя. Но настройка байесовских фильтров на корпоративном сервере очень сложная задача, т. к. тематика писем может быть самой различной.
- *Контроль массовости* (DCC, Razor, Pyzor). Предлагается технология определения массовости рассылок. Выявляются в потоке письма, которые идентичны или имеют незначительное отличие. Но эта технология может запретить и вполне легитимные письма, а спамеры научились пробивать эту технологию защиты.
- *Грейлистинг* (greylisting) — "серые списки". Бывает, что почтовые системы задерживают почту и происходит отказ с кодом ошибки. Программы, которые рассылают спам, повторно это письмо не присылают. Но с задержкой в доставке писем многие пользователи не согласятся.
- *Проверка корректности почтовых сообщений*. При написании программ для генерации спама многие спамеры допускают ошибки, в результате чего спамерские почтовые сообщения не соответствуют определенному стандарту. Этого ни в коем случае не допускают настоящие фирменные почтовые клиенты, поэтому контроль корректности писем дает неплохие результаты.

Спамеры находят адреса для рассылки спама многими способами. Например, если адрес вашей почты состоит из одного общеизвестного слова (например, zina@..., info@..., bolt@..., support@...), то он является легкой добычей для спамерских атак. Короткие адреса типа go@..., aa@..., abc@)... тоже часто используются для рассылок спама. Спамеры очень часто сканируют веб-сайты, доски объявлений, чаты, форумы и находят адреса пользователей, на которые будет совершаться рассылка спама. Поэтому не спешите публиковать свои важные почтовые адреса в Интернете — этим вы защитите их от превращения в помойку для спамерских писем.

1.7. Заключение

Вот мы и подошли к концу изучения основных угроз для вашего компьютера. Как вы уже увидели, угроз вполне достаточно для того, чтобы начать от них защищаться.

Может быть, информация в этой главе показалась вам скучной, серой, несущей только одни проблемы и опасности. Однако все ранее описанные угрозы могут очень серьезно вас побеспокоить, если вы неопытны или не осведомлены об их природе. Но если вы же уже информированы о характере этих угроз, вам только осталось постичь способы борьбы с вирусами и другими вредоносными программами. Обо всех этих методах антивирусной защиты вы и узнаете в следующих главах этой книги.

ГЛАВА 2

Как защитить свой компьютер от вирусов

В предыдущей главе мы подробно обсудили, какие существуют вирусные угрозы. Новичка эта информация может, как минимум, повергнуть в уныние, ведь такое количество различных угроз может стать серьезной проблемой, способной парализовать работу вашего компьютера. Однако не спешите отключать компьютер от сети. Все не так плохо. Теперь мы знаем своего врага и нам будет легче от него защититься. В этом нам поможет антивирусная программа. Существует множество различных антивирусных программ, о которых мы и поговорим далее, в этой главе.

2.1. Знакомимся с антивирусными программами

Антивирусная программа — это ваш верный помощник. С помощью антивирусной программы вы можете защитить свой компьютер от вирусных угроз. Она поможет нам найти и обезвредить вирусы, компьютерные черви и трояны, пытающиеся проникнуть на наш компьютер. При этом совершенно неважно, как именно они хотят это сделать и где спрятаться. Антивирусная программа одинаково легко найдет и обезвредит сетевого червя, спрятавшегося в оперативной памяти компьютера, троянского коня, пришедшего по электронной почте, и вирус, пытающийся с флэш-карты скопировать себя в системную папку Windows.

При этом хорошая антивирусная программа не создает проблем с работой легальных программ, которые используются нами каждый день. Например, офисные приложения или компьютерные игры.

2.1.1. Методы выявления вирусов

История развития антивирусных программ неразрывно связана с развитием самих вирусов, поэтому описание способов работы антивирусов мы начнем с истории вирусов.

Первые вирусы и антивирусы

Первые вирусные программы появились еще в начале 70-х годов прошлого столетия. С появлением первых персональных компьютеров Apple в 1977 году и развитием сетевой инфраструктуры начинается новая эпоха истории компьютерных вирусов. Появились первые программы-вандалы, которые распространялись под видом полезных программ, однако после запуска уничтожали данные пользователей. В это же время появляются троянские программы-вандалы, проявляющие свою деструктивную сущность лишь через некоторое время или при определенных условиях.

Первые антивирусные программы появились в 1984 году. Программа CHK4BOMB позволяла проанализировать текст загрузочного модуля и выявляла все текстовые сообщения и подозрительные участки кода, такие, например, как команды прямой записи на диск. При выявлении запрещенной операции можно запретить ее выполнение. Были также специальные антивирусные утилиты, которые не ловили вирусы, а вместо этого "обманывали" вирус, заставляя его "думать", что все файлы на вашем компьютере уже заражены.

С течением времени антивирусные программы стали *резидентными*, т. е. постоянно находились в памяти компьютера и контролировали выполнявшиеся в системе операции.

Также изменялись методы обнаружения вирусов, подробнее об этих методах мы поговорим далее.

Обнаружение, основанное на сигнатурах

Метод обнаружения, основанный на сигнатурах, это метод, при котором программа, просматривая файл обращается к словарю с известными атаками, который составили и дополняют авторы антивирусной программы. В случае соответствия какого-либо фрагмента кода просматриваемой программы известному коду (сигнатуре) вируса в словаре, программа антивирус удаляет инфицированный файл, пытается восстановить файл, удалив сам вирус из тела файла. Также антивирусная программа может отправить его в карантин, т. е. делает невозможным его запуск во избежание дальнейшего распространения вируса.

Этот метод можно сравнить с паспортным контролем на границе, к примеру, в аэропорту. Когда вы показываете свой паспорт, ваши паспортные данные проверяют в специальной базе разыскиваемых преступников, и если вас там нет, то вас благополучно пропускают.

Такой способ обнаружения вирусов является старейшим. Первые антивирусные программы умели обнаруживать вирусы только таким способом, сверяя содержимое каждого файла со своим словарем. Современные антивирусные программы также используют *сигнатурный анализ*, однако он не является единственным средством обнаружения вирусов.

Основным недостатком сигнатурного анализа является то, что он позволяет обнаруживать только уже известные вирусы. А вирусы, сигнатуры которых еще не занесены в словари, обнаружить таким способом не получится. Иногда, для того чтобы вирус смог проникнуть в сеть какой-то конкретной организации, его код разрабатывают специально таким образом, чтобы данной сигнатуры не было в словаре антивируса, используемого в этой организации. Так как при сигнатурном анализе антивирус ничего не знает об этом новом вирусе, вирус с успехом проникает в корпоративную сеть. Кроме того, разработчики вирусов специально шифруют и видоизменяют код вирусов, для того, чтобы сигнатура этого кода отсутствовала в базе.

Еще одним существенным недостатком метода обнаружения, основанного на сигнатурах, является необходимость регулярного обновления сигнатур. Для такого обновления необходим доступ в Интернет. В случае, если вы не обновляли свою базу антивирусных сигнатур хотя бы один месяц, вы подвергаете свой компьютер серьезной угрозе, т. к. за это время появились тысячи вирусов, неизвестные вашей антивирусной программе. Не забывайте об этом и ежедневно обновляйте свою антивирусную программу.

Обнаружение программ подозрительного поведения

Чтобы избежать недостатков метода обнаружения вирусов основанного на сигнатурах, разработчики антивирусных программ применили ряд новых технологий. Одной из них является обнаружение аномалий (подозрительного поведения), т. е. динамический метод работы антивирусов. Программа, использующая этот метод, наблюдает определенные действия (работу программы/процесса, сетевой трафик, работу пользователя), следя за возможными необычными и подозрительными событиями или тенденциями.

Здесь, если производить сравнение с тем же контролем при пересечении границы, пограничники внимательно следят за каждым пересекающим границу и в случае странностей в его поведении, задерживают подозрительного гражданина.