[вредоносная программа; компьютерные вирусы; трояны; сетевые черви; антивирусное ПО]

7.4. Основные виды вредоносного программного обеспечения

Сегодня почти каждый пользователь ПК в своей практике сталкивался проявлением как вполне «безобидных», так и весьма серьезных нарушений и сбоев в работе ПК, вызванных *вредоносными программами*.

Вредоносные программы отличаются условиями существования, применяемыми технологиями на различных этапах жизненного цикла, собственно вредоносным воздействием – все эти факторы и являются основой для классификации. В результате по основному (с исторической точки зрения) признаку – размножению, вредоносные программы делятся на три типа: собственно *вирусы*, *черви* и *трояны*.

Определение компьютерного вируса – непростой вопрос, поскольку весьма сложно очертить свойства, присущие только вирусам и не касающиеся других программ. И напротив, давая жесткое определение вируса как программы, обладающей определенными свойствами, практически сразу же можно найти пример вируса, таковыми свойствами не обладающего.

ГОСТ Р 51188-98 определяет вирус следующим образом: *«Вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам»*.

Первый настоящий компьютерный вирус *Pervading Animal* появился в конце 1960-х годов и представлял собой игру, написанную с непреднамеренной ошибкой. Первым сетевым червем стал *Creeper* (конец 1970-х), умевший самостоятельно выйти в сеть через модем и записать свою копию на удаленной машине. Первый троян – *a Aids Information Diskette* (1989 год) сразу вызвал эпидемию: будучи зараженным, компьютер после 90 перезагрузок операционной системы показывал пользователю требование перевести на указанный в нем адрес около двухсот долларов, при этом все остальные файлы жесткого диска становились недоступны.

Первую глобальную эпидемию вызвал *Brain* (1986 год), по совместительству первый вирус для IBM-совместимых компьютеров, а также *стелс-вирус*. Он был написан в Пакистане двумя братьями-программистами с целью определения уровня пиратства у себя в стране.

В 1984г. *Фред Коэн* (*Fred Cohen*) в своей работе «*Computer Viruses – Theory and Experiments*» показал, что, теоретически, задача обнаружения компьютерных вирусов является неразрешимой. При этом он дал вирусу такое определение: «*Компьютерным вирусом является программа, способная заражать другие программы изменяя их таким образом, чтобы они включали, возможно измененную, копию вируса*».

Тем не менее, на практике оказывается, что все известные вирусы могут быть обнаружены антивирусными программами. Результат достигается, помимо прочего, еще и за счет того, что поврежденные или «неудачные» экземпляры вирусов, неспособные к созданию и внедрению своих копий, обнаруживаются и классифицируются наравне со всеми остальными «полноценными» вирусами. Следовательно, с практической точки зрения, т.е. с точки зрения алгоритмов поиска, способность к размножению вовсе не является обязательной для причисления программы к вирусам.

В зависимости от характерных свойств вирусов для их обнаружения и нейтрализации могут применяться различные методы. В связи с этим возникает вопрос о классификации вредоносных программ. На практике классификации, принятые различными производителями антивирусных продуктов, отличаются, хотя и построены на близких принципах. Поэтому ниже в этом разделе будут рассмотрены именно они.

Проблема, связанная с определением компьютерного вируса кроется в том, что сегодня под вирусом чаще всего понимается не «традиционный» вирус, а практически *любая вредоносная программа*. Это приводит к путанице в терминологии, осложненной еще и тем, что практически все современные антивирусы способны выявлять указанные типы вредоносных программ, и поэтому ассоциация «*вредоносная программа – вирус*» становится все более устойчивой.

Вредоносная программа – компьютерная программа или переносимый код, предназначенный для реализации угроз информации, хранящейся в компьютере, либо для скрытого использования ресурсов компьютера, либо иного воздействия, препятствующего его нормальному функционированию. К вредоносным программам относятся *компьютерные вирусы*, *трояны*, *сетевые черви* и др.

Вредоносное программное обеспечение классифицируется в основном по различным аспектам их функционирования, таким как: среде обитания; способу заражения среды обитания; воздействию; особенностям алгоритма.

Поскольку отличительной особенностью вирусов в традиционном смысле является способность к размножению в рамках одного компьютера, деление вирусов на типы происходит в соответствии со способами размножения.

Сам процесс размножения может быть условно разделен на несколько стадий:

- *проникновение* на компьютер*;*
- *активация* вируса*;*
- *поиск объектов* для заражения*;*

- *подготовка* вирусных копий*;*
- *внедрение* вирусных копий.

Вирусы проникают на компьютер вместе с зараженными файлами или другими объектами (загрузочными секторами носителей информации), не влияя на процесс проникновения. Возможности проникновения полностью определяются возможностями заражения.

Для активации вируса необходимо, чтобы зараженный объект получил управление. На этой стадии деление вирусов происходит по типам объектов, которые могут быть заражены:

- *загрузочные* вирусы – вирусы, заражающие загрузочные сектора постоянных и сменных носителей.
- *файловые* вирусы – вирусы, заражающие файлы, и дополнительно подразделяющиеся на три вида, в зависимости от среды, в которой выполняется код:
  - собственно файловые вирусы те, которые непосредственно работают с ресурсами операционной системы (ОС);
  - *макровирусы* – вирусы, написанные на языке макрокоманд и исполняемые в среде какого-либо приложения (в подавляющем большинстве случаев речь идет о макросах в документах Microsoft Office);
  - *скрипт-вирусы* – вирусы, исполняемые в среде определенной командной оболочки: раньше – *bat-файлы* в командной оболочке DOS, сейчас чаще *VBS* и *JS* - скрипты в командной оболочке *Windows Scripting Host* (*WSH*).

Стоит отметить тот факт, что вирусы, рассчитанные для работы в среде определенной ОС или приложения, обычно оказываются неработоспособными в среде других ОС и приложений. Поэтому как отдельный атрибут вируса выделяется среда, в которой он способен выполняться. Для файловых вирусов это *Windows*, *Linux*, *MacOS* и т.п. Для макровирусов – *Word*, *Excel*, *PowerPoint*, *Office*.

На стадии поиска объектов для заражения встречается два способа поведения вирусов:

- получив управление, вирус производит разовый поиск жертв, после чего передает управление ассоциированному с ним объекту (зараженному объекту);
- получив управление, вирус, так или иначе, остается в памяти и производит поиск жертв непрерывно, до завершения работы среды, в которой он выполняется.

Вирусы второго типа во времена однозадачной DOS было принято называть резидентными. С переходом на Windows проблема остаться в памяти перестала быть актуальной: практически все вирусы, исполняемые в среде Windows, равно как и в среде приложений MS Office, являются вирусами второго типа. И напротив, скрипт-вирусы являются вирусами первого типа.

Отдельно имеет смысл отметить так называемые *stealth-вирусы* (*невидимки*) – вирусы, которые, находясь постоянно в памяти, перехватывают обращения к зараженному файлу и на ходу удаляют из него вирусный код, передавая в ответ на запрос неизмененную версию файла. Таким образом, эти вирусы маскируют свое присутствие в системе. Для их

обнаружения антивирусным средствам требуется возможность прямого обращения к диску в обход средств ОС. Сейчас этот тип вирусов распространен мало.

Процесс подготовки копий для распространения может существенно отличаться от простого копирования. Авторы наиболее сложных в технологическом плане вирусов стараются сделать разные копии максимально непохожими для усложнения их обнаружения антивирусными средствами. Как следствие, составление сигнатуры для такого вируса крайне затруднено либо вовсе невозможно.

Внедрение вирусных копий может осуществляться двумя принципиально разными методами:

- внедрение вирусного кода непосредственно в заражаемый объект;
- замена объекта на вирусную копию; замещаемый объект, как правило, переименовывается.

Для вирусов характерным является преимущественно первый метод. Второй метод намного чаще используется, так называемыми, червями и троянами (см. далее), а точнее троянскими компонентами червей, поскольку трояны сами по себе не распространяются.

Червь (*сетевой червь*) – тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, и осуществлению иного вредоносного воздействия.

Так же как для вирусов, жизненный цикл червей можно разделить на определенные стадии: проникновение в систему; активация; поиск «жертв»; подготовка копий; распространение копий.

На этапе проникновения в систему черви делятся преимущественно по типам используемых протоколов:

- *сетевые черви* – черви, использующие для распространения протоколы Internet и локальных сетей. Обычно этот тип червей распространяется с использованием неправильной обработки некоторыми приложениями базовых пакетов стека протоколов TCP/IP;
- *почтовые черви* – черви, распространяющиеся в формате сообщений электронной почты;
- *IRC-черви* – черви, распространяющиеся по каналам *IRC* (*Internet Relay Chat*);
- *P2P-черви* – черви, распространяющиеся при помощи пиринговых (*peer-to-peer*) файлообменных сетей;
- *IM-черви* – черви, использующие для распространения системы мгновенного обмена сообщениями (*IM, Instant Messenger – ICQ, MSN Messenger, AIM* и др.)

Сегодня наиболее многочисленную группу составляют почтовые черви. Сетевые черви тоже являются заметным явлением, но не столько из-за количества, сколько из-за качества: эпидемии, вызванные сетевыми червями, зачастую отличаются высокой скоростью распространения и большими масштабами. IRC-, P2P- и IM-черви встречаются достаточно

редко, чаще они служат альтернативными каналами распространения для почтовых и сетевых червей.

На этапе активации черви делятся на две большие группы, отличающиеся как по технологиям, так и по срокам жизни: в одном случае *для активации необходимо активное участие пользователя*; в другом – для активации *участие пользователя не требуется вовсе либо достаточно лишь пассивного участия*. Под пассивным участием пользователя во второй группе понимается, например, просмотр писем, при котором пользователь не открывает вложенные файлы, но его компьютер, тем не менее, оказывается зараженным. В последнее время наметилась тенденция к совмещению в червях обоих способов распространения.

Способ поиска компьютера-жертвы полностью базируется на используемых протоколах и приложениях. В частности, если речь идет о почтовом черве, производится сканирование файлов компьютера на предмет наличия в них адресов электронной почты, по которым в результате и производится рассылка копий червя. Точно так же Internet-черви сканируют диапазон IP адресов в поисках уязвимых компьютеров, а P2P-черви встраивают свои копии в общедоступные каталоги клиентов пиринговых сетей.

Сказанное выше о подготовке копий для распространения вирусов, применимо и для червей. Некоторые черви способны рассылать свои копии в письмах, как с внедрением скрипта приводящего к автоматической активации червя, так и без внедрения. Такое поведение червя обусловлено двумя факторами: скрипт автоматической активации повышает вероятность запуска червя на компьютере пользователя, но при этом уменьшает вероятность проскочить антивирусные фильтры на почтовых серверах. Черви также могут менять тему и текст инфицированного сообщения, имя, расширение и даже формат вложенного файла – исполняемый модуль может быть приложен «как есть» или в заархивированном виде.

Троян (*троянский конь*) – тип вредоносных программ, основной целью которых является вредоносное воздействие по отношению к компьютерной системе. Трояны отличаются отсутствием механизма создания собственных копий. Некоторые трояны способны к автономному преодолению систем защиты компьютера с целью проникновения и заражения системы. В общем случае, троян попадает в систему вместе с вирусом либо червем, в результате неосмотрительных действий пользователя или же активных действий злоумышленника.

В силу отсутствия у троянов функций размножения и распространения, их жизненный цикл включает в себя всего три стадии: проникновение на компьютер; активация; выполнение заложенных функций. Но это не означает малого времени жизни троянов. Напротив, троян может длительное время незаметно находиться в памяти компьютера, никак не выдавая своего присутствия, до тех пор, пока не будет обнаружен антивирусными средствами.

Задачу проникновения на компьютер пользователя трояны решают обычно одним из двух следующих методов:

- *Маскировка* – троян выдает себя за полезное приложение, которое пользователь самостоятельно загружает из Internet и запускает. Иногда пользователь исключается из этого процесса за счет размещения на web-странице специального скрипта, который, используя дыры в браузере, автоматически инициирует загрузку и запуск трояна. Чаще всего внедрение троянов на компьютеры пользователей происходит через web-сайты. При этом используется либо вредоносный скрипт, загружающий и запускающий троянскую программу на компьютере пользователя, используя уязвимость в web-браузере, либо наполнение и оформление web-сайта провоцирует пользователя к самостоятельной загрузке трояна. При таком методе внедрения может использоваться не одна копия трояна, а несколько; новая копия создается при каждой загрузке.
- *Кооперация* с вирусами и червями – троян путешествует вместе с червями или, реже, с вирусами. В принципе, такие пары червь-троян можно рассматривать целиком как составного червя, но в сложившейся практике принято троянскую составляющую червей, если она реализована отдельным файлом, считать независимым трояном с собственным именем. Кроме того, троянская составляющая может попадать на компьютер позже, чем файл червя. Нередко наблюдается кооперация червей с вирусами, когда червь обеспечивает транспортировку вируса между компьютерами, а вирус распространяется по компьютеру, заражая файлы.

Активация троянов та же, что и у червей: ожидание запуска файла пользователем, либо использование уязвимостей для автоматического запуска.

В отличие от вирусов и червей, деление которых на типы производится по способам размножения-распространения, трояны делятся на типы по характеру выполняемых ими вредоносных действий. Наиболее распространены следующие виды троянов:

- *Клавиатурные шпионы* – трояны, постоянно находящиеся в памяти и сохраняющие все данные, поступающие от клавиатуры с целью последующей передачи этих данных злоумышленнику. Обычно таким образом злоумышленник пытается узнать пароли или другую конфиденциальную информацию.
- *Похитители паролей* – трояны, также предназначенные для получения паролей, но не использующие слежение за клавиатурой. В таких троянах реализованы способы извлечения паролей из файлов, в которых эти пароли хранятся различными приложениями.
- *Утилиты удаленного управления* – трояны, обеспечивающие полный удаленный контроль над компьютером пользователя. Существуют легальные утилиты такого же свойства, но они отличаются тем, что сообщают о своем назначении при установке или же снабжены документацией, в которой описаны их функции. Троянские утилиты удаленного управления, напротив, никак не выдают своего реального назначения, так что пользователь и не подозревает о том, что его компьютер подконтролен злоумышленнику.
- *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.

- *Анонимные SMTP-серверы* и *прокси* – трояны, выполняющие функции почтовых серверов или прокси и использующиеся в первом случае для спам-рассылок, а во втором для заметания следов хакерами.
- *Утилиты дозвона* – сравнительно новый тип троянов, представляющий собой утилиты *dial-up* доступа в Internet через почтовые службы. Такие трояны прописываются в системе как утилиты дозвона по умолчанию и влекут за собой огромные счета за пользование Internet.
- *Модификаторы настроек браузера* – трояны, которые меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна браузера, имитируют нажатия на баннеры и т.п.
- *Логические бомбы* – чаще не столько трояны, сколько троянские составляющие червей и вирусов, суть работы которых состоит в том, чтобы при определенных условиях (дата, время суток, действия пользователя, команда извне) произвести определенное действие: например, уничтожение данных.

Независимо от типа, вредоносные программы способны наносить значительный ущерб, реализуя любые угрозы информации - угрозы нарушения целостности, конфиденциальности, доступности. В связи с этим при проектировании комплексных систем антивирусной защиты, и даже в более общем случае - комплексных систем защиты информации, необходимо проводить градацию и классифицировать объекты сети по важности обрабатываемой на них информации и по вероятности заражения этих узлов вирусами.

7.5. Антивирусная защита информации

Антивирусная программа (*антивирус*) – любая программа для обнаружения нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики – предотвращения заражения (модификации) файлов или ОС вредоносным кодом.

На данный момент антивирусное программное обеспечение разрабатывается в основном для ОС семейства Windows от компании Microsoft, что вызвано большим количеством вредоносных программ именно под эту платформу. Это, в свою очередь, вызвано большой популярностью ОС этого семейства, также как и большим количеством средств разработки, в том числе бесплатных, и даже «инструкций по написанию вирусов». В настоящий момент на рынок выходят продукты и под другие платформы настольных компьютеров, такие как Linux и Mac OS X. Это вызвано началом распространения вредоносных программ и под эти платформы, хотя UNIX-подобные системы всегда славились своей надежностью.

Помимо ОС для настольных компьютеров и ноутбуков, также существуют платформы и для мобильных устройств, такие как *Windows Mobile*, *Symbian*, *iOS Mobile*, *BlackBerry*, *Android*, *Windows Phone 7* и др. Пользователи устройств с такими ОС также подвержены риску заражения вредоносным программным обеспечением, и некоторые разработчики

антивирусных программ выпускают продукты и для таких устройств.

Классифицируются антивирусные продукты по различным признакам, например: используемые технологии антивирусной защиты, функционал продуктов, целевые платформы.

На сегодня на рынке программного обеспечения представлены антивирусные продукты многочисленных производителей. Среди них большой популярностью пользуются и антивирусные пакеты российских программистов, которые и будут рассмотрены ниже.

Любая компьютерная программа потенциально может быть инфицирована. Это означает, что необходимо постоянно следить за выпуском заплат и обновлений к ней. Обычно информация такого рода всегда доступна на сайте компании-производителя.

Любой компьютер, способный к обмену информацией (через съемные носители или по сети) потенциально может быть инфицирован. Следовательно, даже если компьютер включается всего раз в год, то во время этого сеанса он все равно может быть заражена вирусом. В защите не нуждаются разве что нерабочие и никогда не включаемые компьютеры.

Для проверки работоспособности установленной антивирусной защиты существует специальный тестовый вирус – *Eicar*. Все ведущие антивирусные продукты его детектируют, при этом никаких действий он не совершает. Загрузить сам тестовый вирус в разных форматах или инструкцию по его написанию можно на сайте *www.eicar.org*.

Основанием для подозрения на наличие вируса в системе могут служить:

- внезапное и несанкционированное изменение настроек браузера;
- необычные всплывающие окна и другие сообщения;
- неожиданный несанкционированный дозвон в Internet;
- самопроизвольное блокирование антивирусной программы;
- невозможность загрузки файлов с веб-сайтов антивирусных компаний;
- необоснованные на первый взгляд сбои в работе операционной системы или других программ;
- почтовые уведомления с заслуживающих доверие сайтов об отправке пользователем инфицированных сообщений.

Для предотвращения проникновения в систему вредоносной программы необходимо соблюдать следующие правила:

- вовремя устанавливать последние обновления и заплаты используемого программного обеспечения, особенно – для ОС семейства Microsoft Windows;
- перед чтением данных с любого сменного носителя обязательно проводить проверку на наличие на нем вирусов;
- не загружать из Internet файлы неизвестного происхождения, тем более – программы, и не устанавливать их. Особенно это касается не заслуживающих доверия сайтов;
- не открывать электронные письма, полученные от незнакомых людей или имеющие подозрительную тему сообщения;
- если на компьютере установлен антивирус – никогда не выключать постоянную проверку, поддерживать актуальность антивирусных баз (регулярно загружая обновления),

периодически проводить тщательную проверку жестких дисков на наличие вирусов;

- при интенсивном обмене электронными сообщениями или привычке оставлять свой электронный адрес на публичных сайтах, рекомендуется установить и использовать *антиспамовую* программу.

Обязательно следует помнить, что попытки создавать вредоносные программы или сознательно участвовать в их распространении подпадают под действие ряда статей Уголовного Кодекса Российской Федерации, предусматривающих наказание за такую деятельность, вплоть до лишения свободы на срок до пяти лет, а современные технологии позволяют весьма быстро вычислить автора или распространителя вредоносных программ.

Установка и правильная настройка антивирусного программного обеспечения - это самый надежный способ обеспечить защиту против вредоносных программ.

Существуют вредоносные программы и для мобильных устройств (планшеты, смртфоны). Поэтому в работе с любыми компьютеризированными устройствами необходимо соблюдать перечисленные выше правила «*компьютерной гигиены*», а именно – не допускать загрузку файлов, сообщений и программ из неизвестных или подозрительных источников.

Антивирусы для мобильных платформ тоже существуют: для большинства из них уже налажен выпуск антивирусных средств. Поэтому, если на мобильном устройстве хранится важная информация или, тем более, конфиденциальные данные, установка антивирусной защиты является обязательной.