Защита информации, антивирусная защита

Вредоносные программы

Вредоносные программы - программы, использующие уязвимые места защиты систем. Такие программы можно разделить на две категории: программы, *нуждающиеся в программе-носителе*, и *независимые программы*. К первой категории относится программный код, который не может работать независимо от некоторой реальной прикладной программы или утилиты. Ко второй категории относятся самостоятельные программы, которые могут быть запущены стандартными средствами операционной системы, как любая другая программа.

Рисунок Классификация вредоносных программ

Люк (лазейка) - это секретная точка входа в программу, позволяющая тому, кто знает о существовании люка, получить доступ в обход стандартных процедур защиты. Люки уже совершенно законно используются в программистской практике для ускорения отладки и тестирования программ. Люк - программный код, реагирующий на специальную последовательность введенных с клавиатуры символов, либо активизирующийся в ответ на ввод определенного идентификатора пользователя или последовательность каких-то маловероятных событий.

Логические бомбы представляют собой программный код, внедренный в какую-то полезную программу, который должен «взорваться» при выполнении определенных условий. (присутствие или отсутствие каких-то файлов, наступление определенного дня недели или определенной даты, имя конкретного пользователя).

После запуска бомба может изменять или удалять данные файлов, вызывать зависание машины или выполнять какие-то другие разрушительные действия.

Квазивирусы *(«Троянский конь»)* - представляют собой полезную или кажущуюся полезной программу, содержащую скрытый код, который после запуска программы- носителя выполняет нежелательные или разрушительные функции. Программа этого типа может использоваться для опосредованного выполнения операций, которые несанкционированный пользователь не может выполнить непосредственно.

Вирусы - представляют собой программу, которая может «инфицировать» другие программы путем их модификации. В модифицированный код включается код вируса, с помощью которого вирус может «заразить» другие программы. Внесенный в компьютерную систему, типичный вирус временно захватывает управление дисковой операционной системой компьютера. Затем при каждом контакте зараженного компьютера с незараженным программным обеспечением очередная копия вируса помещается в новую программу. Таким образом, инфекция может передаваться от компьютера к компьютеру ничего не подозревающими пользователями, обменивающимися содержимым магнитных дисков или пересылающими программы по сети.

«Черви» (вирусы-репликаторы) - используют сетевые соединения для распространения от одной системы к другой. Во время работы на отдельном компьютере сетевой «червь» может вести себя как компьютерный вирус или «бактерия», внедрять «троянских коней», или же выполнять какие-то другие разрушительные или подрывные действия. Для размножения сетевой «червь» использует сетевые средства доставки информации. Сетевой «червь» во многом подобен компьютерному вирусу - у него тоже есть инкубационный период, фаза распространения, фаза активизации и фаза выполнения.

Бактерии являются программами, не повреждающими сами по себе никаких файлов. Единственной целью «бактерии» является воспроизведение себе подобных. Скорость размножения «бактерий» растет экспоненциально, что, в конце концов, приводит к быстрому захвату всех ресурсов процессора, памяти или дискового пространства.

3.7.2. Природа и структура вируса

Жизненный цикл типичного вируса состоит из четырех этапов:

1. ***Инкубационный период*** имеют не все вирусы. Вирус никак не проявляется. В конце концов, вирус будет активизирован некоторым событием, например, наступлением определенной даты, присутствием другой программы или файла, появлением достаточного места на диске.
2. ***Фаза распространения***. Вирус помещает свою копию в другие программы или в определенные системные области на диске. Все инфицированные программы будут содержать точную копию вируса, каждая их которых тоже должна будет когда-нибудь пройти свою фазу распространения;
3. ***Фаза активизации***. Вирус активизируется для выполнения своей функции. Фаза активизации может быть инициирована самыми разными системными событиями, например, наличием определенного числа копий данного вируса в системе;
4. ***Фаза выполнения***. Выполняется содержащаяся в вирусе функция. Эта функция может

быть как вполне безобидной (например, вывод сообщения на экран), так и совершенно деструктивной (например, уничтожение программ и файлов с данными).

Классификация компьютерных вирусов

В настоящее время программные вирусы можно классифицировать по следующим признакам:

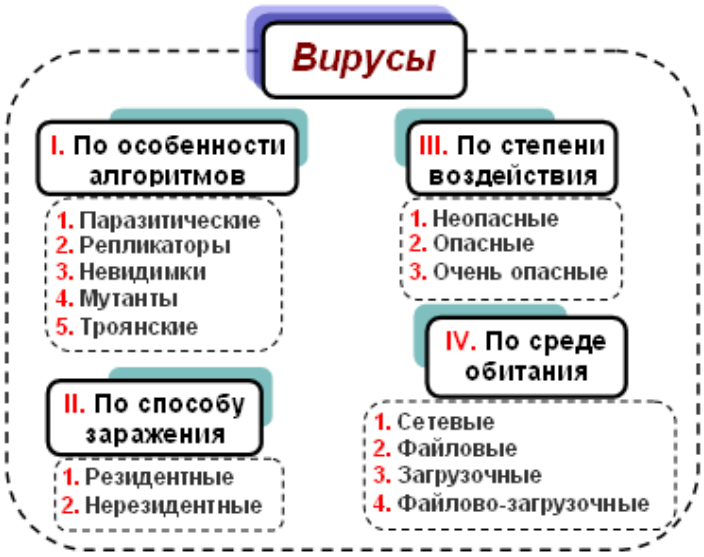

Рисунок Классификация вирусов

По среде обитания все вирусы можно разделить на файловые, загрузочные и сетевые.

Файловым вирусом называют вирус, который внедряется в выполняемые файлы. Файл, в теле которого присутствует код программы-вируса, называется зараженным (инфицированным) файлом.

Загрузочным вирусом (бутовым) называют вирус, который внедряется в загрузочный сектор диска (Boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record).

Сетевым вирусом называют вирус, который распространяется по компьютерным сетям.

По способам заражения различают резидентные и нерезидентные вирусы:

Резидентный вирус размещает себя или некоторую свою часть в оперативной памяти, получая возможность перехватывать обращения операционной системы к дискам и файлам. При обращении операционной системы к этим объектам вирус внедряется в них. Вирус находится в оперативной памяти и является активным вплоть до выключения или перезагрузки компьютера. Резидентными являются все загрузочные вирусы.

Нерезидентный вирус не заражает оперативную память компьютера, то есть, не размещает свой код в оперативной памяти. Он является активным только во время работы зараженной программы.

По особенностям алгоритма можно выделить следующие группы вирусов:

Паразитические - это вирусы, изменяющие содержимое файлов и секторов диска.

Репликаторы - называемые червями, они распространяются по компьютерным сетям, вычисляя адреса сетевых компьютеров, они записывают по этим адресам свои копии.

Невидимки (стелс-вирусы) - их трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

Полиморфный, мутант (мимикрирующий) - вирус, код которого изменяется при новом заражении, что делает практически невозможным обнаружить его по «сигнатуре».

Макровирусы. Существование макровирусов построено на использовании средств поддержки макросов, предлагаемых в Word и других офисных приложениях. Макрос - программа, встроенная в документ текстового процессора или файл какого-то другого типа. Макровирусы особенно опасны по следующим причинам:

- Макровирусы независимы от платформы и, практически все макровирусы, поражают документы. Поэтому любая аппаратно-программная система, поддерживающая Word, может быть заражена таким вирусом;
- Макровирусы инфицируют документы, а не выполняемый код. Информация, вводимая в компьютерную систему, в основном представлена в форме документов, а не программ;
- Макровирусы быстро распространяются (чаще всего по электронной почте).

Классификация программных закладок

Имеются вредоносные программы еще одного класса - это так называемые ***программные закладки***, которые могут выполнять хотя бы одно из перечисленных ниже действий:

- ***вносить произвольные искажения в коды программ***, находящихся в оперативной памяти компьютера (программная закладка первого типа);
- ***переносить фрагменты информации*** из одних областей оперативной или внешней памяти компьютера в другие (программная закладка второго типа);
- ***искажать выводимую на внешние компьютерные устройства*** или в канал, связи информацию, полученную в результате работы других программ (программная закладка третьего типа).

Чтобы программная закладка могла произвести какие-либо действия по отношению к другим программам или по отношению к данным, процессор должен приступить к исполнению команд, входящих в состав кода программной закладки. ***Это возможно только при одновременном соблюдении следующих условий:***

1. программная закладка должна попасть в оперативную память;
2. работа закладки, находящейся в оперативной памяти, начинается при выполнении ряда

условий, которые называются активизирующими.

Все программные закладки *обязательно выполняют операцию записи в оперативную или внешнюю память системы.* При отсутствии данной операции никакого негативного влияния программная закладка оказать не может.

Модели воздействия программных закладок на компьютеры:

Перехват - программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию, вводимую с внешних устройств компьютерной системы или выводимую на эти устройства, в скрытой области памяти локальной или удаленной компьютерной системы. Объектом сохранения, например, могут служить символы, введенные с клавиатуры (все повторяемые два раза последовательности символов), или электронные документы, распечатываемые на принтере.

Искажение - программная закладка изменяет информацию, которая записывается в память компьютерной системы в результате работы программ, либо подавляет/инициирует возникновение ошибочных ситуаций в компьютерной системе.

Наблюдение и компрометация. При использовании модели типа «наблюдение» программная закладка встраивается в сетевое или телекоммуникационное программное обеспечение. Так как, подобное программное обеспечение всегда находится в состоянии активности, внедренная в него программная закладка может следить за всеми процессами обработки информации и осуществлять установку и удаление других программных закладок.

Троянской программой (квазивирусной программой) называется:

- *программа, которая, являясь частью другой программы* с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба;
- *программа с известными пользователю функциями, в которую был внесены изменения,* позволяющие втайне выполнять другие (разрушительные) действия.

Таким образом, ***троянская программа - это особая разновидность программной закладки***.

Характеристика антивирусных программ

В антивирусные программы разделяются на четыре поколения:

- Первое поколение: обычные сканеры.
- Второе поколение: эвристические анализаторы.
- Третье поколение: мониторы.
- Четвертое поколение: полнофункциональные системы защиты.

Антивирусные ***программы-сканеры*** первого поколения для идентификации вирусов

использовали характерные для соответствующих вирусов *сигнатуры*. Вирусы могли содержать «групповые символы», но все копии вируса имели одну и ту же структуру и неизменный код. Такие программы-сканеры могли обнаруживать только известные вирусы. Другой тип сканеров первого поколения предполагал *поиск несоответствий* текущих значений длины файлов в сравнении со значениями, сохраненными в специальной базе данных.

Сканеры второго поколения уже не ориентированы на конкретные сигнатуры. Вместо этого применяется эвристический анализ, с помощью которого можно сделать вывод о вероятном наличии вируса в программе. Одна из разновидностей таких сканеров предполагала поиск в программе фрагментов кода, характерного для вирусов.

Программы третьего поколения представляют собой ***резидентные программы,*** выявляющие вирусы по выполняемым ими действиям, а не по их коду в инфицированной программе. Преимущество таких программ заключается в том, что для них не требуется постоянно обновлять базу данных сигнатур и эвристик для большего числа новых вирусов. Вместо этого достаточно определить относительно небольшой набор действий, характеризующих возможные проявления вируса.

Продукты четвертого поколения представляют собой пакеты, ***объединяющие в единое целое все существующие антивирусные технологии.*** Такой подход, помимо выполнения сканирования и наличия компонентов, позволяющих регистрировать определенные действия вирусов, предполагает наличие средств управления доступом. Эти средства позволяют ограничить возможности вирусов по проникновению в систему и внесению изменений в файлы под видом обновления.

Различают следующие виды антивирусных программ:

- программы-детекторы;
- программы-доктора или фаги;
- программы-ревизоры;
- программы-вакцины или иммунизаторы;
- программы-мониторы, или резидентные сторожа.

Программы-детекторы осуществляют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора (флаги, а также программы-вакцины) не только находят зараженные

вирусами файлы, но и лечат их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы флаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов.

Среди фагов выделяют *полифаги*, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известные: Aidstest, Scan, Norton AntiVirus, Doctor Web.

Программы–ревизоры относятся к самым надежным средствам от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, и периодически или по желанию пользователя сравнивают текущее состояние с исходным. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля, дата и время модификации, другие параметры. К числу программ-ревизоров относится широко распространенная в России программа ADinf.

Вакцины или иммунизаторы - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы–доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедриться. В настоящее время программы-вакцины имеют ограниченное применение.

Программы – мониторы или резидентные сторожа - это класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. Их цель - не пропустить вирус на компьютер. И поэтому они контролируют обращение к дискам.

При обнаружении «подозрительного» действия программа-монитор либо блокирует выполнение такого действия до специального разрешения пользователя, либо просто выдаёт на экран предупреждающее сообщение, либо совершает другие специальные действия. К недостаткам программ-сторожей можно отнести их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением. Примером программы-фильтра является программа Vsafe.