**Лекция 15. Технологии защиты от вредоносных программ.**

**Цель лекции:** изучить технологии защиты ПО от вредоносных программ.

**План лекции:**
Введение.
1 Классификация вредоносных программ
2 Защита от вредоносных программ
Заключение
Контрольные вопросы

**Ключевые слова:** [выбрать самостоятельно].

**Содержание лекции:**

**Введение**

**1 Классификация вредоносных программ**

***Общие сведения***

С некоторой степенью условности различают следующие типы вредоносных программ (ВП):

- ✓ *троянские программы;*
- ✓ *компьютерные вирусы (в том числе сетевые вирусы и программы- черви);*
- ✓ *прочие вредоносные программы.*

Троянские программы – это вредоносные программы, выполняющие действия, не санкционированные пользователем и, как правило, наносящие ему вред. Такие действия могут включать:

- ✓ *удаление данных;*
- ✓ *блокирование данных;*
- ✓ *изменение данных;*
- ✓ *копирование данных;*
- ✓ *замедление работы компьютеров и компьютерных сетей.*

Под компьютерным вирусом (или просто вирусом) понимается автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в сетях и отдельных компьютерах. Предшественниками вирусов принято считать троянские программы, тела которых содержат скрытые последовательности команд (модули).

Сетевые вирусы (автономные репликативные программы, репликаторы) – вредоносные программы, использующие для своего размножения средства сетевых операционных систем. К разновидности сетевых вирусов относят программы-черви.

***Троянские программы***

Троянские программы можно классифицировать в соответствии с типом действий, выполняемых ими на компьютере.

Бэкдоры – программы, предоставляющие злоумышленникам возможность удаленного управления зараженными компьютерами. Такие программы позволяют автору выполнять на зараженном компьютере любые действия, включая отправку, получение, открытие и удаление файлов, отображение данных и перезагрузку компьютера. Эти ВП часто используются для объединения группы компьютеров-жертв в ботнет (или зомби-сеть) для использования в криминальных целях.

Особенностью бэкдора как класса ВП является то, что на момент его внедрения злоумышленник обладает определенными привилегиями в системе. Нередко бэкдор может быть заложен в реализацию системы разработчиком. Частным случаем бэкдора является

ситуация, когда пользователь, временно имеющий в системе административные полномочия (возможно даже получив их легально), создает для себя потенциальную возможность вернуть таковые полномочия, после того как они у него были отозваны.

Рассмотрим упрощенный пример создания и последующего использования бэкдора. Предположим, существует Unix-система, в которой некоторый субъект временно имеет полномочия администратора. Желая сохранить за собой эти полномочия вне зависимости от сценария развития событий, субъект создает простейший бэкдор. Для этого он копирует исполняемый файл командного интерпретатора (shell) в произвольное место файловой системы, которое будет ему доступно и после утраты административных привилегий. Затем злоумышленник присваивает копии командного интерпретатора бит SUID. Наличие бита SUID в Unix-системах у исполняемого файла означает, что исполняться он будет не с правами пользователя, его вызвавшего, а с правами владельца файла. В данном случае владельцем файла является пользователь с административными привилегиями (root).

Эксплойты – программы, которые содержат данные или код, использующие уязвимость в работающих на компьютере приложениях. Основной целью выполнения эксплойтов может стать повышение привилегий в целевой системе или отказ в обслуживании. Нередко эксплойты объединяются в эксплойт-пак (эксплойт-pack) или эксплойт-кит (эксплойт-kit), т.е. набор эксплойтов. Функциональность этих наборов предполагает, помимо собственно эксплуатации уязвимости, предварительное уточнение среды функционирования объекта воздействия, а именно прояснение следующих вопросов:

- ✓ *выполняется ли ОС в среде виртуализации;*
- ✓ *присутствует ли в атакуемой среде отладчик;*
- ✓ *какие установлены антивирусные средства.*

В качестве «полезной» нагрузки эксплойта (функции, выполняемой после эксплуатации уязвимости и проникновения в систему) используется shell-код, предоставляющий атакующему доступ к командному интерпретатору в целевой системе.

Руткиты – программы, предназначенные для сокрытия в системе определенных объектов или действий. Часто основная их цель – предотвратить обнаружение ВП, чтобы увеличить время работы этих программ на зараженном компьютере. Руткит может быть реализован как прикладная утилита или модуль ядра, устанавливаемый злоумышленником после получения доступа к целевой системе. Основная задача руткита – скрыть признаки других ВП, выполняющихся в системе. Чаще всего руткиты модифицируют алгоритмы выполнения системных функций ОС или подменяют системные информационные структуры.

Банковские троянские программы (Trojan-Bankers) – программы, предназначенные для кражи учетных данных систем интернет-банкинга, систем электронных платежей и кредитных или дебетовых карт. Будучи установленной на компьютере жертвы, программа перехватывает клавиатурный ввод в формах браузера, обладающих определенными признаками, и передает данные злоумышленнику. Некоторые разновидности банковских троянских программ могут также выкрасть цифровой сертификат пользователя и файлы секретного ключа. Именно эта разновидность ВП наносит жертве наибольший прямой финансовый ущерб.

DoS-троянские программы предназначены для проведения атак типа «отказ в обслуживании» (Denial of Service, DoS) по целевым адресам. При такой атаке с зараженных компьютеров системе с определенным адресом отправляется большое количество запросов, что может вызвать ее перегрузку и привести к отказу в обслуживании.

Троянские программы класса Trojan-Downloader способны загружать и устанавливать на компьютер-жертву новые версии ВП, включая троянские и рекламные программы. Как таковая данная вредоносная программа не несет угрозы – опасность представляет именно возможность неконтролируемой загрузки.

Троянские программы класса Trojan-Dropper используются хакерами, чтобы установить троянские программы и/или вирусы или предотвратить обнаружение ВП. Не

каждая антивирусная программа способна выявить все компоненты троянских программ этого класса.

Троянские программы класса Trojan-FakeAV имитируют работу антивирусного программного обеспечения. Они созданы, чтобы вымогать деньги у пользователя в обмен на обещание обнаружения и удаления угроз, хотя угроз, о которых они сообщают, в действительности не существует.

Игровые троянские программы крадут информацию об учетных записях участников сетевых игр.

IM-троянские программы (Trojan-IM) крадут логины и пароли к программам мгновенного обмена сообщениями, таким как ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype и многие другие.

Троянские программы класса Trojan-Ransom могут изменить данные на компьютере таким образом, что последний перестает нормально работать, а пользователь лишается доступа к определенным данным. Злоумышленник обещает восстановить нормальную работу компьютера или разблокировать данные после уплаты запрашиваемой суммы.

SMS-троянские программы отправляют текстовые сообщения с мобильного устройства на платные телефонные номера с повышенным тарифом.

Шпионские троянские программы (Trojan-Spy) способны скрытно наблюдать за использованием компьютера, например, отслеживая вводимые с клавиатуры данные, делая снимки экрана, включая микрофон, видеокамеру и получая список работающих приложений.

Троянские программы класса Trojan-Mailfinder способны собирать на компьютере адреса электронной почты.

Встречаются и другие виды троянских программ: Trojan-ArcBomb, Trojan-Clicker, Trojan-Notifier, Trojan-Proxy, Trojan-PSW и др., каждая из которых имеет свои специфические особенности.

***Компьютерные вирусы***

***Физическая структура компьютерного вируса*** достаточно проста, поскольку состоит из головы и, возможно, хвоста. Голова вируса – компонента вируса, получающая управление первой. Хвост – это часть вируса, расположенная в коде зараженной программы отдельно от головы. Вирусы, состоящие из одной головы, называют несегментированными; вирусы, содержащие голову и хвост, – сегментированными.

Жизненный цикл вируса обычно включает следующие периоды:

- ✓ *внедрение;*
- ✓ *инкубационный период;*
- ✓ *период репликации (саморазмножение);*
- ✓ *проявление.*

В течение инкубационного периода вирус пассивен, что усложняет задачу его поиска и нейтрализации. На этапе проявления вирус выполняет свойственные ему целевые функции, например, необратимую коррекцию информации в компьютере или на носителях информации.

***Принцип работы вируса.*** Принципиальное отличие вируса от троянской программы состоит в том, что вирус после его активации существует самостоятельно (автономно) и в процессе своего функционирования заражает (инфицирует) программы путем включения (имплантации) в них своего кода. Таким образом, компьютерный вирус можно рассматривать как своеобразный «генератор троянских программ». Программы, зараженные вирусом, называются вирусоносителями.

Заражение программы, как правило, выполняется таким образом, чтобы вирус получил управление раньше самой программы. Для этого он либо встраивается в начало программы, либо имплантируется в ее тело так, что первой командой зараженной программы является безусловный переход на компьютерный вирус, текст которого заканчивается аналогичной командой безусловного перехода на команду вирусоносителя,

бывшую первой до заражения. Получив управление, вирус выбирает следующий файл, заражает его, возможно, выполняет какие-либо другие действия, после чего отдает управление вирусоносителю.

«Первичное» заражение происходит в процессе поступления инфицированных программ из памяти одной машины в память другой, причем в качестве средства перемещения этих программ могут использоваться как носители информации (CD, флеш-карты и т.п.), так и каналы локальных и глобальных сетей. Вирусы, использующие для размножения сетевые средства, принято называть сетевыми.

Наиболее существенные признаки компьютерных вирусов позволяют классифицировать последние по четырем критериям.

Классификация компьютерных вирусов по критерию «режим функционирования» включает:

- ✓ *резидентные вирусы – вирусы, которые после активации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;*
- ✓ *транзитные вирусы – вирусы, которые выполняются только в момент запуска зараженной программы.*

Классификация компьютерных вирусов по критерию «объект внедрения» такова:

- ➢ *файловые вирусы – вирусы, заражающие файлы.*

  В свою очередь, файловые вирусы подразделяются на вирусы, заражающие:
  - исполняемые файлы;
  - командные файлы;
  - файлы, составляемые на макроязыках программирования, или файлы, содержащие макросы (макровирусы);
  - файлы с драйверами устройств;
  - файлы с библиотеками исходных, объектных, загрузочных и оверлейных модулей, с библиотеками динамической компоновки и т.п.;
- ➢ *загрузочные (бутовые) вирусы – вирусы, заражающие код, хранящийся в системных областях дисков.*

  Загрузочные вирусы подразделяются на вирусы, заражающие:
  - системный загрузчик, расположенный в загрузочном секторе логических дисков;
  - внесистемный загрузчик, расположенный в загрузочном секторе жестких дисков.

***Классификация компьютерных вирусов по критерию «способ заражения»*** представляет:

- ✓ *перезаписывающие вирусы (overwriting);*
- ✓ *паразитические вирусы (parasitic);*
- ✓ *вирусы-компаньоны (companion);*
- ✓ *вирусы-ссылки (.link);*
- ✓ *вирусы, заражающие объектные модули (OBJ);*
- ✓ *вирусы, заражающие библиотеки компиляторов (LIB);*
- ✓ *вирусы, заражающие исходные тексты программ.*

***Перезаписывающие вирусы*** записывают свой код вместо кода заражаемого файла, уничтожая его содержимое. Как результат файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

***Паразитические вирусы.*** К таковым относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.

Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (prepending), в конец файлов (appending) и в середину файлов (inserting).

Внедрение вируса в начало файла. Известны два способа внедрения паразитического файлового вируса в начало файла. Первый способ заключается в том, что вирус переписывает начало заражаемого файла в его конец, а сам копируется на освободившееся место.

При заражении файла вторым способом вирус дописывает заражаемый файл к своему телу. Таким образом, при запуске зараженного файла первым управление получает код вируса. При этом вирусы, чтобы сохранить работоспособность программы, либо лечат зараженный файл, повторно запускают его, ждут окончания его работы и снова записываются в его начало (иногда для этого используется временный файл, в который записывается обезвреженный файл), либо восстанавливают код программы в памяти компьютера и настраивают необходимые адреса в ее теле (т.е. дублируют работу ОС).

Внедрение вируса в конец файла. Наиболее распространенным способом внедрения вируса в файл является дописывание вируса в его конец. При этом вирус изменяет начало файла таким образом, что первыми выполняемыми командами программы, содержащейся в файле, являются команды вируса. Для того чтобы получить управление при старте файла, вирус корректирует стартовый адрес программы (адрес точки входа). Для этого вирус производит необходимые изменения в заголовке файла.

Внедрение вируса в середину файла. Существует несколько методов внедрения вируса в середину файла. В наиболее простом из них вирус переносит часть файла в его конец или «раздвигает» файл и записывает свой код в освободившееся пространство. Этот способ во многом аналогичен методам, перечисленным выше. Некоторые вирусы при этом компрессируют переносимый блок файла так, что длина файла при заражении практически не изменяется.

Часто используется метод cavity, при котором вирус записывается в заведомо неиспользуемые области файла. Вирус может быть скопирован в незадействованные области заголовка EXE-файла, в «дыры» между секциями EXE-файла или в область текстовых сообщений популярных компиляторов.

Существуют вирусы, заражающие только те файлы, которые содержат блоки, заполненные каким-либо постоянным блоком байтов, при этом вирус записывает свой код вместо такого блока. Кроме того, копирование вируса в середину файла может произойти в результате ошибки вируса – в этом случае файл может быть необратимо испорчен.

Вирусы без точки входа. Отдельно следует отметить довольно незначительную группу вирусов, не имеющих точки входа (EPO-вирусы — Entry Point Obscuring viruses). К ним относятся вирусы, не изменяющие адрес точки старта в заголовке EXE-файлов. Такие вирусы записывают команду перехода на свой код в какое-либо место в середину файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус может долгие годы «спать» внутри файла и «проснуться» только при некоторых ограниченных условиях. Перед тем как записать в середину файла команду перехода на свой код, вирусу необходимо выбрать «правильный» адрес в файле – иначе зараженный файл может оказаться испорченным. Известно несколько способов, с помощью которых вирусы определяют такие адреса внутри файлов, например: поиск в файле последовательности стандартного кода заголовков процедур языков программирования (C/C++), дизассемблирование кода файла или замена адресов импортируемых функций и др.

***Вирусы-компаньоны*** – это вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вредоносных программ состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник.

К вирусам данного типа относятся вирусы, которые при заражении переименовывают файл, запоминают его (для последующего запуска файла-хозяина) и

записывают свой код на диск под именем заражаемого файла. Например, файл Notepad.exe переименовывается в Notepad.exd, а вирус записывается под именем Notepad.exe. При запуске управление получает код вируса, который затем запускает оригинальный Notepad, exe, который был переименован в Notepad.exd.

Существуют и другие типы вирусов-компаньонов, использующих иные оригинальные идеи или особенности операционных систем. Например, path-компаньоны размещают свои копии в основном каталоге Windows, используя тот факт, что этот каталог является первым в списке переменной окружения Path и файлы для запуска Windows в первую очередь будут искать именно его (этот каталог). Данным способом собственного запуска пользуются также многие программы-черви и троянские программы.

***Вирусы с прочими способами заражения.*** Существуют вирусы, которые никоим образом не связывают свое присутствие с каким-либо исполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков «в надежде», что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям «специальные» имена, чтобы подтолкнуть пользователя на запуск своей копии: например, Install.exe или Winstart.bat.

Некоторые вирусы записывают свои копии в архивы (Arj, Zip, Rar), другие записывают команду запуска зараженного файла в бат-файлы (bat-файлы). Link-вирусы также не изменяют физического содержимого файлов, однако при запуске зараженного файла «заставляют» ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

***Классификация компьютерных вирусов по критерию «степень и способ маскировки»*** включает:

- ✓ *вирусы, не использующие средств маскировки;*
- ✓ *stealth-вирусы – вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных;*
- ✓ *вирусы-мутанты (MtE-вирусы) – вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.*

  В свою очередь, MtE-вирусы подразделяются на две группы:
  - *обычные вирусы-мутанты, в разных копиях которых различаются только зашифрованные тела, а дешифрованные тела вирусов совпадают;*
  - *полиморфные вирусы, в разных копиях которых различаются не только зашифрованные, но и их дешифрованные тела.*

Наиболее распространенные типы вирусов характеризуются следующими основными особенностями.

***Файловый транзитный вирус*** целиком размещается в исполняемом файле, в связи с чем он активируется только в случае активирования вирусоносителя, а по выполнении необходимых действий возвращает управление самой программе. При этом выбор очередного файла для заражения осуществляется вирусом посредством поиска по каталогу.

***Файловый резидентный вирус*** отличается от нерезидентного вируса логической структурой и общим алгоритмом функционирования. Резидентный вирус состоит из так называемого инсталлятора и программ обработки прерываний. Инсталлятор получает управление при активации вирусоносителя и инфицирует оперативную память путем размещения в ней управляющей части вируса и замены адресов в элементах вектора прерываний на адреса своих программ, обрабатывающих эти прерывания. На так называемой фазе слежения, следующей за фазой инсталляции, при возникновении какого-либо прерывания управление получает соответствующая подпрограмма вируса.

В связи с существенно более универсальной по сравнению с нерезидентными вирусами общей схемой функционирования, резидентные вирусы могут реализовывать самые разные способы инфицирования, среди которых наиболее распространенным является инфицирование запускаемых программ, а также файлов при их открытии или чтении. Отличительной особенностью последних является инфицирование загрузочного

сектора (бут-сектор) носителя данных. Голова бутового вируса всегда находится в бут-секторе, а хвост – в любой другой области носителя. Наиболее безопасным для вируса способом считается размещение хвоста в так называемых псевдосбойных кластерах, логически исключенных из числа доступных для использования. Существенно, что хвост бутового вируса всегда содержит копию оригинального (исходного) бут-сектора.

Механизм инфицирования, реализуемый бутовыми вирусами, например, при загрузке ОС, таков. При загрузке ОС с инфицированного носителя вирус, в силу своего положения на нем (независимо от того, с CD, флеш-карты или с винчестера производится загрузка), получает управление и копирует себя в оперативную память. Затем он модифицирует вектор прерываний таким образом, чтобы прерывания при обращении к диску обрабатывались собственным обработчиком прерываний вируса, и запускает загрузчик ОС. Посредством перехвата прерываний бутовые вирусы могут реализовывать столь же широкий набор способов инфицирования и целевых функций, сколь и файловые резидентные вирусы.

***Stealth-вирусы*** пользуются слабой защищенностью некоторых операционных систем и заменяют некоторые их компоненты (драйверы дисков, прерывания) таким образом, что вирус становится невидимым (прозрачным) для других программ.

***Полиморфные вирусы*** содержат алгоритм порождения дешифрованных тел вирусов, непохожих друг на друга. При этом в алгоритмах дешифрования могут встречаться обращения практически ко всем командам процессора Intel и даже использоваться некоторые специфические особенности его реального режима функционирования.

***Макровирусы*** распространяются под управлением прикладных программ, что делает их независимыми от операционной системы. Наибольшее число макровирусов функционируют под управлением системы ОС Windows. В то же время известны макровирусы, работающие под управлением и других операционных систем.

***Вирусные «скрипты» (скрипт-вирусы)*** – вирусы, написанные на языках Visual Basic Script, Java Script, BAT и др. Эти вредоносные программы могут как располагаться в отдельных файлах, так и встраиваться в HTML-документ и в таком случае интерпретироваться браузером (причем не только с удаленного сервера, но и с локального диска).

Различают:

- ✓ *VBS-вирусы, написанные на языке Visual Basic Script;*
- ✓ *JS-вирусы, написанные на языке Java Script;*
- ✓ *BAT-вирусы, написанные на языке командного интерпретатора MS-DOS (на BAT-языке);*
- ✓ *PIF-еирус в формате PIF (Program Information File);*
- ✓ *WScript-черви, как правило, встроенные в HTML-файлы;*
- ✓ *PHP-скрипт-вирусы, написанные на языке PHP, либо вирусы, заражающие PHP-файлы;*
- ✓ *HTML-вирусы, встраиваемые в HTML-страницы;*
- ✓ *Perl-вирусы, написанные на языке Perl.*

***Сетевые вирусы*** наиболее просто реализуют размножение в тех случаях, когда сетевыми протоколами предусмотрен обмен программами. Однако размножение возможно и в тех случаях, когда указанные протоколы ориентированы только на обмен сообщениями. Классическим примером реализации процесса размножения с использованием только стандартных средств электронной почты является репликатор Морриса. Текст репликатора передается от одного компьютера к другому, как обычное сообщение, постепенно заполняющее буфер, выделенный в оперативной памяти компьютера-адресата. В результате переполнения буфера, инициированного передачей, адрес возврата в программу, вызвавшую программу приема сообщения, замещается на адрес самого буфера, где к

моменту возврата уже находится текст вируса. Тем самым вирус получает управление и начинает функционировать на компьютере-адресате.

***Сетевые черви*** – вредоносные программы, самостоятельно распространяющиеся через локальные и глобальные компьютерные сети. Классификация программ-червей включает:

- ✓ *почтовые программы-черви (Email-Worms) – вредоносные программы, использующие для своего распространения электронную почту. При этом червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо веб-сервере;*
- ✓ *программы-черви, использующие интернет-пейджеры (IM-Worms) – вредоносные программы, использующие для своего распространения рассылку на обнаруженные контакты из контакт-листа интернет-пейджера (программы ICQ, MSN Messenger, Yahoo Messenger, Google Talk, AOL Instant Messenger, Trillian, Miranda, QIP и др.) сообщений, содержащих ссылку на свой файл;*
- ✓ *программы-черви в IRC-каналах (IRC-Worms) – вредоносные программы, которые распространяются, используя среду IRC каналов CInternet Relayed Chat channels);*
- ✓ *классические сетевые программы-черви (Net-Worms) – вредоносные программы, использующие для своего распространения уязвимости в операционных системах и прикладном ПО или распространяющиеся с помощью копирования себя на сетевые ресурсы;*
- ✓ *программы-черви для файлообменных сетей (P2P-Worms) – вредоносные программы, использующие для своего распространения P2P-сети (распространяющиеся с помощью программ eMule, eDonkey, Kazzaa, DC++, BitTorrent, Gnutella, FastTrack и др.);*
- ✓ *вирусные черви – вредоносные программы, которые незаметно перемещаются между узлами вычислительной сети, не нанося никакого вреда до тех пор, пока не доберутся до целевого узла. В нем программа размещается и перестает размножаться.*

***Методы противодействия антивирусным программам.*** Поскольку цель компьютерных злоумышленников – внедрить вредоносный код в компьютеры-жертвы, то для этого им необходимо не только вынудить пользователя запустить зараженный файл или проникнуть в систему через какую-либо уязвимость, но и незаметно проскочить мимо установленного антивирусного фильтра. Поэтому злоумышленники целенаправленно борются с антивирусными программами. Используемые ими технические приемы весьма разнообразны, но чаще всего встречаются следующие.

***Упаковка и шифрование кода.*** Значительная часть (если не большинство) современных компьютерных червей и троянских программ упакованы или зашифрованы тем или иным способом. Более того, для этого специально создаются утилиты упаковки и шифровки. Для детектирования подобных программ-червей и троянских программ антивирусным программам приходится добавлять либо новые методы распаковки и расшифровки, либо сигнатуры на каждый образец ВП, что снижает качество детектирования, поскольку не всегда все возможные образцы модифицированного кода оказываются в руках антивирусной компании.

***Мутация кода*** – разбавление троянского кода «мусорными» инструкциями. В результате функционал троянской программы сохраняется, но значительно меняется ее «внешний вид». Периодически встречаются случаи, когда мутация кода происходит в режиме реального времени – при каждом скачивании троянской программы с зараженного веб-сайта. То есть все или значительная часть попадающих с такого сайта на компьютеры образцы троянской программы разные.

***Скрытие своего присутствия*** – так называемые руткит-технологии, обычно используемые в троянских программах. В этом случае осуществляется перехват и подмена системных функций, в результате чего зараженный файл не виден ни штатными средствами

операционной системы, ни антивирусными программами. Иногда так же скрываются ветки реестра, в которых регистрируется копия троянской программы, и другие системные области компьютера.

***Остановка работы антивирусной программы и системы получения обновлений антивирусных баз данных.*** Многие троянские программы и сетевые черви предпринимают специальные действия против антивирусных программ: ищут их в списке активных приложений и пытаются остановить их работу, «портят» антивирусные базы данных, блокируют получение обновлений и т.п. Антивирусным программам приходится защищать себя соответствующими способами: следить за целостностью баз данных, «прятать» от троянцев свои процессы и т.п.

***Сокрытие своего кода на веб-сайтах.*** Адреса веб-страниц, на которых присутствуют троянские файлы, рано или поздно становятся известны антивирусным компаниям. Естественно, что подобные страницы попадают под пристальное внимание антивирусных аналитиков: содержимое страницы периодически скачивается, новые версии троянских программ заносятся в антивирусные обновления. Для противодействия этому веб-страница модифицируется специальным образом: если запрос идет с адреса антивирусной компании, то скачивается какой-нибудь нетроянский файл вместо троянского.

***Атака количеством*** – генерация и распространение в Интернете большого количества новых версий троянских программ за короткий промежуток времени. В результате антивирусные компании оказываются «завалены» новыми образцами, на анализ которых требуется время, что дает вредоносному коду дополнительный шанс для успешного внедрения в компьютеры.

Эти и другие методы используются хакерами для противодействия антивирусным программам. При этом их активность растет год от года, и сейчас можно говорить о настоящей «гонке технологий», которая развернулась между антивирусной и вирусной индустрией. Одновременно растет не только количество хакеров-индивидуалов и преступных групп, но и профессионализм последних. Все это значительно увеличивает сложность и объем работы, необходимой антивирусным компаниям для разработки средств защиты достаточного уровня.

***Прочие вредоносные программы***

Существуют вредоносные программы, которые занимаются уничтожением, блокированием, модификацией или копированием информации, нарушением работы компьютеров или компьютерных сетей и при этом не значатся ни в одной из классификаций, приведенных выше. К таким вредоносным программам относятся разнообразные программы, не представляющие угрозы непосредственно компьютеру, на котором исполняются: они разработаны для создания других вирусов или троянских программ, организации DoS-атак на удаленные серверы, взлома других компьютеров и т.п. Все вредоносные действия такие программы (в отличие от вирусов, программ-червей и троянских программ) совершают по прямому указанию пользователя.

***Классификация программ с вредоносной составляющей.*** Основным признаком, по которому различают такие программы, являются совершаемые ими действия.

***DoS-утилиты*** – программы, предназначенные для проведения DoS-атаки (Denial of Service) с ведома пользователя на компьютер-жертву. Суть атаки сводится к посылке жертве многочисленных запросов, что приводит к отказу в обслуживании, если ресурсы атакуемого удаленного компьютера недостаточны для обработки всех поступающих запросов.

***DDoS-программы*** (Distributed DoS) реализуют распределенные атаки с разных компьютеров, причем без ведома пользователя зараженного компьютера. Для этого DDoS-программа засылается любым способом на компьютер «жертв-посредников» и после запуска в зависимости от текущей даты или по команде «хозяина» начинает DoS-атаку на указанный сервер в сети.

***Программы класса HackTools.*** Хакерские утилиты данного класса предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими (используя методы троянских программ класса «бэкдор») или для внедрения во взломанную систему других вредоносных программ.

***Хакерские утилиты класса Exploit*** используют уязвимости в ОС или приложениях, установленных на атакуемом компьютере.

***Программы класса VirTools*** – программы, позволяющие злоумышленнику модифицировать другие вредоносные программы таким образом, чтобы они не детектировались антивирусным программным обеспечением.

***Программы класса Flooders.*** Данные хакерские утилиты используются для «забивания мусором» (бесполезными сообщениями) каналов Интернета: IRC-каналов, компьютерных пейджинговых сетей, электронной почты и т.д.

***Конструкторы***. Конструкторы вирусов и троянских программ – это утилиты, предназначенные для изготовления новых компьютерных вирусов и троянских программ. Известны конструкторы вирусов для ОС Windows и макровирусов. Они позволяют генерировать исходные тексты вирусов, объектные модули и/или непосредственно зараженные файлы.

Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать:

- ✓ *тип вируса;*
- ✓ *поражаемые объекты;*
- ✓ *наличие утилиты самошифрования внутренних текстовых строк для противодействия отладчику;*
- ✓ *эффекты, сопровождающие работу вируса, и т.п.*

Прочие конструкторы не имеют интерфейса и считывают информацию о типе вируса из конфигурационного файла.

***Программы класса «злые шутки»*** - программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К «злым шуткам» относятся, например, программы, которые «пугают» пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), выводят странные вирусоподобные сообщения и т.д. – в зависимости от «чувства юмора» автора такой программы.

***Подозрительные программы.*** Описанные выше вредоносные программы используются в основном для сокрытия вредоносного кода или для его генерации. Приведенная классификация охватывает большую часть всех известных программ с вредоносной составляющей. Однако нужно учитывать возможность создания новых ВП, а также программ, нацеленных на осуществление вредоносной деятельности в специфических системах.

Так как определение неполезной составляющей нельзя однозначно возложить на программу или на уже имеющеюся базу знаний о ВП, определим еще один класс вредоносных программ – программы, определенные как вредоносные самим пользователем, – и назовем его классом подозрительных программ. Учитывая, что все вышеописанные классы можно определить, как классы, описанные специалистами антивирусных компаний, новый класс описывается пользователями, осуществляющими непосредственную работу со своим определенным набором программ.

## 2 Защита от вредоносных программ

Антивирусные программы (антивирусы) – наиболее распространенное средство обнаружения и нейтрализации вредоносных программ.

Антивирусы, исходя из реализованного в них подхода к выявлению и нейтрализации вирусов, принято делить на следующие группы:

- ✓ *детекторы;*
- ✓ *фаги;*
- ✓ *вакцины;*
- ✓ *прививки;*
- ✓ *ревизоры;*
- ✓ *мониторы.*

***Детекторы*** обеспечивают выявление вирусов посредством просмотра исполняемых файлов и поиска так называемых сигнатур – устойчивых последовательностей байтов, имеющихся в телах известных вирусов. Наличие сигнатуры в каком-либо файле свидетельствует о его заражении соответствующим вирусом. Антивирус, обеспечивающий возможность поиска различных сигнатур, называют полидетектором.

***Фаги*** выполняют функции, свойственные детекторам, и «излечивают» инфицированные программы посредством «выкусывания» вирусов из их тел. По аналогии с полидетекторами, фаги, ориентированные на нейтрализацию различных вирусов, именуют полифагами.

***Вакцины***, в отличие от детекторов и фагов, по своему принципу действия подобны вирусам. Вакцина имплантируется в защищаемую программу и запоминает ряд количественных и структурных характеристик последней. Если вакцинированная программа не была к моменту вакцинации инфицированной, то при первом же после заражения запуске произойдет следующее. Активизация вирусоносителя приведет к получению управления вирусом, который, выполнив свои целевые функции, передаст управление вакцинированной программе. В последней, в свою очередь, сначала управление получит вакцина, которая выполнит проверку соответствия запомненных ею характеристик аналогичным характеристикам, полученным в текущий момент. Если указанные наборы характеристик не совпадают, то делается вывод об изменении текста вакцинированной программы вирусом. Характеристиками, используемыми вакцинами, могут быть длина программы, ее контрольная сумма и т.д.

***Прививки***. Принцип действия прививок основан на учете того, что любой вирус, как правило, помечает инфицируемые программы каким-либо признаком, чтобы не выполнять их повторное заражение. В ином случае имело бы место многократное инфицирование, сопровождаемое существенным и поэтому легко обнаруживаемым увеличением объема зараженных программ. Прививка, не внося никаких других изменений в текст защищаемой программы, помечает ее тем же признаком, что и вирус, который, в свою очередь, после активизации и проверки наличия указанного признака, считает ее инфицированной и «оставляет в покое».

***Ревизоры*** обеспечивают слежение за состоянием файловой системы, используя для этого подход, аналогичный реализованному в вакцинах. Программа-ревизор в процессе своего функционирования выполняет применительно к каждому исполняемому файлу сравнение его текущих характеристик с аналогичными характеристиками, полученными в ходе предшествующего просмотра файлов. Если при этом обнаруживается, что, согласно имеющейся системной информации, файл с момента предшествующего просмотра не обновлялся пользователем, а сравниваемые наборы характеристик не совпадают, то файл считается инфицированным. Характеристики исполняемых файлов, получаемые в ходе очередного просмотра, запоминаются в отдельном файле (файлах), в связи с чем увеличение длин исполняемых файлов, имеющее место при вакцинации, в данном случае не происходит. Другое отличие ревизоров от вакцин состоит в том, что каждый просмотр исполняемых файлов ревизором требует его повторного запуска.

***Монитор*** представляет собой резидентную программу, обеспечивающую перехват потенциально опасных прерываний, характерных для вирусов, и запрашивающую у пользователей подтверждение на выполнение операций, следующих за прерыванием. В случае запрета или отсутствия подтверждения монитор блокирует выполнение пользовательской программы.

***Технологии проактивной защиты.*** Антивирусы рассмотренных типов существенно повышают вирусозащищенность отдельных компьютеров и сетей в целом, однако, в силу свойственных им ограничений, естественно, не являются панацеей. В связи с этим необходима реализация альтернативных подходов к нейтрализации вирусов: создание операционных систем, обладающих высокой вирусозащищенностью по сравнению с наиболее «вирусодружественной» MS Windows, разработка аппаратных средств защиты от вирусов и соблюдение технологии защиты от вирусов.

Сегодня можно выделить в отдельный класс методов антивирусной защиты методы проактивной защиты – защиты, основанной не на поиске сигнатурных данных вируса, уже имеющихся в базе, а на непосредственной проверке действий, выполняемых приложением.

Существуют следующие технологии проактивной защиты:

- ✓ *эвристический анализ – технология, позволяющая на основе анализа кода программы осуществлять поиск участков, отвечающих за вредоносные действия;*
- ✓ *эмуляция кода – технология, позволяющая запустить приложение в среде, эмулирующей поведение ОС и центрального процессора. При выполнении приложения в этой среде оно не сможет нанести вред системе, но вредоносное воздействие будет обнаружено;*
- ✓ *анализ поведения – технология, обеспечивающая перехват всех важных системных событий, установку собственных фильтров, которые позволяют отслеживать всю системную активность. Данная технология оценивает не только единичное действие, но и всю цепочку действий. Именно на такой технологии основывается работа большинства поведенческих блокираторов;*
- ✓ *песочница – технология, обеспечивающая ограничение возможностей подозрительного приложения таким образом, чтобы оно не могло повлиять на важные системные функции. Данные ограничения достигаются путем запуска приложения в специальной ограниченной среде, из которой приложение не может получить доступ к системным функциям, файлам, реестру и т.д.;*
- ✓ *виртуализация рабочего приложения – технология, которая с помощью специального системного драйвера обеспечивает перехват запросов на запись информации на жесткий диск и запись этой информации на виртуальный жесткий диск (временный буфер), очистка которого по умолчанию будет произведена при отключении компьютера.*

Рассмотрим поведенческий блокиратор как конкурент традиционным антивирусным решениям, основанным на вирусных сигнатурах. Это два разных, не исключающих друг друга подхода к проверке на вирусы. Сигнатура – это небольшой кусок вирусного кода, который прикладывается к файлам, и антивирус смотрит, подходит он или нет. Поведенческий блокиратор следит за действиями программ при их запуске и прекращает работу программы в случае ее подозрительных или явно вредоносных действий (для этого есть специальный набор правил). У обоих методов есть и достоинства, и недостатки.

Достоинство сигнатурных сканеров – гарантированный «отлов» тех вирусов, для которых известны их сигнатуры. Недостатки:

- ✓ *пропуск вирусов, сигнатуры которых сканерам пока неизвестны:*
- ✓ *большой объем антивирусных баз;*
- ✓ *ресурсоемкое.*

Достоинство поведенческого блокиратора – детектирование даже неизвестных вредоносных программ. Недостатки:

- ✓ *пропуск некоторых уже давно известных вариантов. Поведение современных вирусов и троянских программ настолько разнообразно, что покрыть их все единым набором правил просто нереально;*
- ✓ *ложные срабатывания, поскольку иногда вполне легальные программы ведут себя «подозрительно». То есть поведенческий блокиратор будет гарантированно*

*пропускать что-то вредное и периодически блокировать работу чего-то весьма полезного.*

Это справедливо также и в отношении другого проактивного метода защиты – эвристического анализатора. Работа последнего заключается в анализе предполагаемого поведения программы до ее запуска и вынесении вердикта, подозрительная программа или нет.

Следует отметить, что, как только подобные антивирусные технологии начинают мешать хакерам атаковать свои жертвы, практически сразу появляются новые вирусные технологии, позволяющие «обходить» эвристические методы защиты.

**Заключение**

Таким образом, вновь изобретенные проактивные технологии работают довольно короткое время. Это, конечно, не означает, что проактивные методы защиты бесполезны. Они прекрасно справляются со своей частью работы и могут обнаруживать некоторое количество компьютерных вирусов, разработанных не «слишком» умелыми хакерами-программистами. И по этой причине они могут являться хорошим дополнением к традиционным сигнатурным сканерам, однако полагаться на них целиком и полностью нельзя.

**Контрольные вопросы**

Смотри руководство по организации самостоятельной работы магистрантов.