Презентация на тему: Способы заражения программ

Выполнил: Кайдалов Максим

Понятие вредоносного программного обеспечения

К вредоносному программному обеспечению относятся сетевые черви, компьютерные вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие какой-либо вред компьютеру, на они запускаются, или компьютерам в сети.

Классификация вредоносного программного обеспечения

Классические компьютерные вирусы

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью: последующего запуска своего кода при каких-либо действиях пользователя; дальнейшего внедрения в другие ресурсы компьютера.

Троянские программы

В данную категорию входят программы, осуществляющие несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

.

Сетевые черви

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

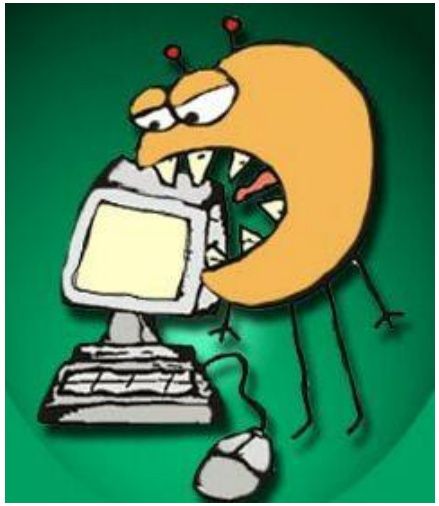
- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры сети.

Прочие вредоносные программы

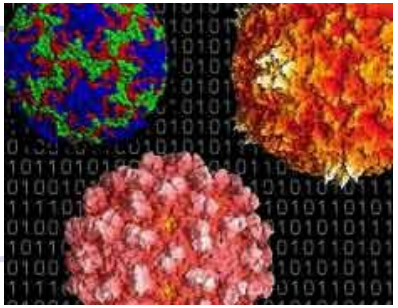
К данной категории относятся:

утилиты автоматизации создания сетевых червей, вирусов и троянских программ

- библиотеки, разработанные для создания вредоносного ПО;
- утилиты скрытия кода зараженных файлов от антивирусной проверки



Компьютерные вирусы



Существует несколько определений компьютерных вирусов.

- «Компьютерный вирус — это специально написанная, небольшая по размерам программа (т. е. некоторая совокупность выполняемого кода), которая может «приписывать» себя к другим программам «заражать» их), создавать свои копии и внедрять их в файлы, системные области компьютера и т. д., а также выполнять различные нежелательные действия на компьютере»
- «Компьютерным вирусом называется способная к самовоспроизводству и размножению программа, внедряющаяся в другие программы»
- «Компьютерный вирус - фрагмент исполняемого кода, который копирует себя в другую программу (главную программу), модифицируя ее при этом. Дублируя себя, вирус заражает другие программы. Вирус выполняется только при запуске главной программы и вызывает ее непредсказуемое поведение, приводящее к уничтожению и искажению данных и программ».
- «Компьютерный вирус - программа, имеющая возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие объекты с целью искажения и уничтожения данных и программ.
- При этом дубликаты сохраняют способность к дальнейшему распространению. Такие программы, как правило, составляются на языке ассемблера, никаких сообщений на экран дисплея не выдают. Переносятся при копировании с диска на диск либо по сети Интернет.

Первый вирус для PC

- Первый вирус для PC был обнаружен в январе 1986 года. Назывался он Brain.A и распространялся "перекрестным опылением" - через дискеты.
- Инфицируя загрузочный сектор машины, вирус приступал к копированию себя во все доступные файлы. Вирус был безопасен, не причинял никакого особого вреда, но именно он стал родоначальником длинной вереницы своих последователей, за прошедшие 20 лет успевших "эволюционировать" в порой весьма агрессивные "особи".
- Вирусы же, поражающие загрузочный сектор, благополучно "вымерли" уже с 1995 года, когда против них появились достаточно эффективные средства борьбы, а сами дискеты почти перестали использоваться - появилась технология оптических носителей.

Классификация вирусов

Один из авторитетнейших «вирусологов» страны Евгений Касперский предлагает условно классифицировать вирусы по следующим признакам:

- по среде обитания вируса;
- по способу заражения среды обитания;
- по деструктивным возможностям;
- по особенностям алгоритма вируса.

KASPERSKY lab

Классификация вирусов

- ***Среда обитания***
  - *Сетевые* - распространяются по компьютерной сети;
  - *Файловые* - внедряются в выполняемые файлы;
  - *Загрузочные* - внедряются в загрузочные области носителей информации (boot-сектор).

  Способ заражения
  - *Резидентные* - находятся в оперативной памяти компьютера, активны до выключения компьютера;
  - *Не резидентные* - не заражают память, являются активными ограниченное время.

  Деструктивные возможности
  - *Безвредные* - практически не влияют на работу; уменьшают свободную память на диске в результате своего распространения;
  - *Не опасные* - уменьшают свободную память, создают звуковые, графические и прочие эффекты;
  - *Опасные* - могут привести к серьезным сбоям в работе;
  - *Очень опасные* - могут привести к потере программ или системных данных.

Классификация вирусов

- ***Особенности алгоритма вируса***
  - *Вирусы - "спутники"* - вирусы, не изменяющие файлы, создают для EXE-файлов файлы-спутники с расширением COM;
  - *Вирусы - "черви"* - распространяются по сети, рассылают свои копии, вычисляя сетевые адреса;
  - *Паразитические* - изменяют содержимое дисковых секторов или файлов;
  - *"Студенческие"* - примитив, содержат большое количество ошибок;
  - *"Стелс" - вирусы* - перехватывают обращения DOS к пораженным файлам или секторам и подставляют вместо себя незараженные участки;
  - *Вирусы-"призраки"* или *Полиморфные вирусы* - не имеют ни одного постоянного участка кода, трудно обнаруживаемы, основное тело вируса зашифровано;
  - *Макровирусы* - пишутся не в машинных кодах, а на VBA и JS, живут в документах Word, переписывают себя в Normal.dot.

  Вид деструктивных действий
  - *Информационные вирусы* - уничтожают информацию;
  - *Аппаратные вирусы* - выводят из строя аппаратную часть компьютера;
  - *Психотропные вирусы* - способны убить человека.

Загрузочные вирусы

- Загрузочные вирусы заражают загрузочный (boot) сектор флоппи-диска и boot-сектор или Master Boot Record (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера.

Файловые вирусы

- К данной группе относятся вирусы, которые при своем размножении тем или иным способом используют файловую систему какой-либо ОС.
- Внедрение файлового вируса возможно практически во все исполняемые файлы всех популярных ОС, а также динамические и виртуальные библиотеки драйверов (dll,VxD) и многие другие файлы.
- Существуют вирусы, заражающие файлы, которые содержат исходные тексты программ, библиотечные или объектные модули. Возможна запись вируса и в файлы данных, но это случается либо в результате ошибки вируса, либо при проявлении его агрессивных свойств. Макро-вирусы также записывают свой код в файлы данных - документы или электронные таблицы, - однако эти вирусы настолько специфичны, что вынесены в отдельную группу.
- По способу заражения файлов вирусы делятся на переписчиков ("overwriting"), паразитические ("parasitic"), компаньон-вирусы ("companion"), "link"-вирусы, вирусы-черви и вирусы, заражающие объектные модули (OBJ), библиотеки компиляторов (LIB) и исходные тексты программ.

Переписчики - Overwriting вирусы

- Данный метод заражения является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.
- К разновидности overwriting-вирусов относятся вирусы, которые записываются вместо заголовка EXE-файлов. Основная часть файла при этом остается без изменений и продолжает нормально работать в соответствующей операционной системе, однако заголовок файла оказывается испорченным.

Вирусы паразиты (Parasitic)

- К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сими 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"). В свою очередь, внедрение вирусов в середину файлов происходит различными методами: путем переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла ("cavity"-вирусы).

Компаньон - вирусы

- К категории "компаньон" относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.
- Наиболее распространены компаньон - вирусы, использующие особенность DOS первым выполнять .COM-файл, если в одном каталоге присутствуют два файла с одним и тем же именем, но различными расширениями имени - .COM и .EXE. Такие вирусы создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением .COM, например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет EXE-файл. При запуске такого файла DOS первым обнаружит и выполнит COM-файл, т.е. вирус, который затем запустит и EXE-файл. Некоторые вирусы используют не только вариант COM-EXE, но также и BAT-COM-EXE.
- Вторую группу составляют вирусы, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл XCOPY.EXE переименовывается в XCOPY.EXD, а вирус записывается под именем XCOPY.EXE. При запуске управление получает код вируса, который затем запускает оригинальный XCOPY, хранящийся под именем XCOPY.EXD. Интересен тот факт, что данный метод работает, наверное, во всех операционных системах - подобного типа вирусы были обнаружены не только в DOS, но в Windows и OS/2.
- В третью группу входят так называемые "Path-companion" вирусы, которые "играют" на особенностях DOS PATH. Они либо записывают свой код под именем заражаемого файла, но "выше" на один уровень PATH (DOS, таким образом, первым обнаружит и запустит файл-вирус), либо переносят файл-жертву на один подкаталог выше и т.д.

Файловые черви

- Файловые черви (worms) являются, в некотором смысле, разновидностью компаньон - вирусов, но при этом никоим образом не связывают свое присутствие с каким-либо выполняемым 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.
- Существуют вирусы-черви, записывающие свои копии в архивы (ARJ, ZIP, RAR и прочие). К таким вирусам относятся "ArjVirus" и "Winstart". Некоторые вирусы записывают команду запуска зараженного файла в BAT-файлы.
- Не следует путать файловые вирусы-черви с сетевыми червями. Первые используют только файловые функции какой-либо операционной системы, вторые же при своем размножении пользуются сетевыми протоколами.

Link-вирусы

- Link-вирусы, как и компаньон - вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла "заставляют" ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.
- На сегодняшний день известен единственный тип Link-вирусов - вирусы семейства "Dir_II". При заражении системы они записывают свое тело в последний кластер логического диска. При заражении файла вирусы корректируют лишь номер первого кластера файла, расположенный в соответствующем секторе каталога. Новый начальный кластер файла будет указывать на кластер, содержащий тело вируса. Таким образом, при заражении файлов их длины и содержимое кластеров диска, содержащих эти файлы, не изменяется, а на все зараженные файлы на одном логическом диске будет приходиться только одна копия вируса.
- После заражения данные каталога указывают на вирус, т.е. при запуске файла управление получают не файлы, а вирус.

OBJ-, LIB-вирусы и вирусы в исходных текстах

- Вирусы, заражающие библиотеки компиляторов, объектные модули и исходные тексты программ, достаточно экзотичны и практически не распространены. Всего их около десятка. Вирусы, заражающие OBJ- и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, таким образом, не является выполняемым и неспособен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же "живого" вируса становится COM- или EXE-файл, получаемый в процессе линковки зараженного OBJ/LIB-файла с другими объектными модулями и библиотеками. Таким образом, вирус распространяется в два этапа: на первом заражаются OBJ/LIB-файлы, на втором этапе (линковка) получается работоспособный вирус.
- Заражение исходных текстов программ является логическим продолжением предыдущего метода размножения. При этом вирус добавляет к исходным текстам свой исходный код (в этом случае вирус должен содержать его в своем теле) или свой шестнадцатеричный дамп (что технически легче). Зараженный файл способен на дальнейшее распространение вируса только после компиляции и линковки.

Среда существования вирусов

- Операционная система или приложение может подвергнуться вирусному нападению в том случае, если она имеет возможность запустить программу, не являющуюся частью самой системы. Данному условию удовлетворяют все популярные «настольные» операционные системы, многие офисные приложения, графические редакторы, системы проектирования и прочие программные комплексы, имеющие встроенные скриптовые языки.

- Компьютерные вирусы, черви, троянские программы существуют для десятков операционных систем и приложений. В то же время существует огромное количество других операционных систем и приложений, для которых вредоносные программы пока не обнаружены. Что является причиной существования вредных программ в одних системах и отсутствия их в других?

- Причиной появления подобных программ в конкретной операционной системе или приложении является одновременное выполнение следующих условий:
  - популярность, широкое распространение данной системы;
  - наличие разнообразной и достаточно полной документации по системе;
  - незащищенность системы или существование известных уязвимостей в системе безопасности.

- Каждое перечисленное условие является необходимым, а выполнение всех трех условий одновременно является достаточным для появления разнообразных вредоносных программ.

Признаки появления и способы заражения вирусами

Непрофессионалу сложно обнаружить присутствие вирусов на компьютере, поскольку они умело маскируются среди обычных файлов.

Признаки заражения

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- произвольный, без вашего участия, запуск на компьютере каких-либо программ;
- при наличии на вашем компьютере межсетевого экрана, появление предупреждений о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя вы это никак не инициировали.

Способы заражения программ

- Можно выделить следующие способы заражения программ:
- - метод приписывания. Код вируса приписывается к концу файла заражаемой программы, и тем или иным способом осуществляется переход вычислительного процесса на команды этого фрагмента;
- - метод оттеснения. Код вируса располагается в начале зараженной программы, а тело самой программы приписывается к концу.
- - метод вытеснения. Из начала (или середины) файла "изымается" фрагмент, равный по объему коду вируса, и приписывается к концу файла. Сам вирус записывается в освободившееся место. Разновидность метода вытеснения - когда оригинальное начало файла не сохраняется вообще. Такие программы не могут быть восстановлены никаким антивирусом.
- - прочие методы. Сохранение вытесненного фрагмента программы в "кластерном хвосте" файла и пр.