МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ПРОГРАММ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Раздел 1

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Компьютерный вирус (или просто **вирус**) - это автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Предшественниками вирусов принято считать так называемые ***троянские программы***, тела которых содержат скрытые последовательности команд(модули), выполняющие действия, наносящие вред пользователям.

Наиболее распространенной разновидностью троянских программ являются широко известные программы массового применения (редакторы, игры, трансляторы и т.д.), в которые встроены «логические бомбы», срабатывающие по наступлении некоторого события.

Троянские программы не являются саморазмножающимися.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

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

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

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.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

«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 (дискеты, CD-ROM, CD-RW, флэш-память и т.п.), так и каналы вычислительных сетей.

Вирусы, использующие для размножения сетевые средства, принято называть ***сетевыми***.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Цикл жизни вируса

Цикл жизни вируса обычно включает следующие периоды:

1. внедрение
2. инкубационный
3. репликации (саморазмножения)
4. проявления

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 магнитных носителях.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Физическая структура компьютерного вируса

Физическая структура компьютерного вируса достаточно проста. Он состоит из **головы** и, возможно, **хвоста**.

Под **головой вируса** понимается его компонента, получающая управление первой.
Хвост - это часть вируса, расположенная в тексте зараженной программы отдельно от головы.

Вирусы, состоящие из одной головы, называют ***несегментированными***, тогда как вирусы, содержащие голову и хвост - ***сегментированными***.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Классификация компьютерных вирусов

I. ***По режиму функционирования:***

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

II. ***По объекту внедрения:***

- *файловые вирусы* - вирусы, заражающие файлы с программами
- *загрузочные (бутовые) вирусы* - вирусы, заражающие программы, хранящиеся в системных областях дисков

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Классификация компьютерных вирусов

Файловые вирусы подразделяются на вирусы, заражающие:

- исполняемые файлы
- командные файлы и файлы конфигурации
- составляемые на макроязыках программирования, или файлы, содержащие макросы (*макровирусы*)
- файлы с драйверами устройств
- файлы с библиотеками исходных, объектных, загрузочных модулей

Загрузочные вирусы подразделяются на вирусы, заражающие:

- системный загрузчик, расположенный в загрузочном секторе дискет и логических дисков
- внесистемный загрузчик, расположенный в загрузочном секторе жестких дисков

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Классификация компьютерных вирусов

III. ***По степени и способу маскировки:***

- 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 делятся на:

- 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 тела, но и их дешифрованные тела

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Наиболее распространенные типы вирусов и их основные особенности

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

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Наиболее распространенные типы вирусов и их основные особенности

Файловый резидентный вирус отличается от нерезидентного логической структурой и общим алгоритмом функционирования.

Резидентный вирус состоит из инсталлятора и программ обработки прерываний.

Инсталлятор получает управление при активизации 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 описанной 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.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Наиболее распространенные типы вирусов и их основные особенности

Наиболее распространенными способами являются инфицирование запускаемых программ, а также файлов при их открытии или чтении. Отличительной особенностью последних является инфицирование загрузочного сектора (бут-сектора) магнитного носителя.
Голова ***бутового вируса*** всегда находится в бут-секторе (единственном для гибких дисков и одном из двух - для жестких), 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 следующий:
При загрузке операционной системы с инфицированного диска вирус, в силу своего положения на нем (независимо от того, с дискеты или с винчестера производится загрузка), получает управление и копирует себя в оперативную память. Затем он модифицирует вектор прерываний таким образом, чтобы прерывание по обращению к диску обрабатывались собственным обработчиком прерываний вируса, и запускает загрузчик операционной системы.

Благодаря перехвату прерываний бутовые вирусы могут реализовывать столь же широкий набор способов инфицирования и целевых функций, сколь и файловые резидентные вирусы.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Наиболее распространенные типы вирусов и их основные особенности

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

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Наиболее распространенные типы вирусов и их основные особенности

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.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Наиболее распространенные типы вирусов и их основные особенности

Макровирусы распространяются под управлением прикладных программ, что делает их независимыми от операционной системы.

Подавляющее число макровирусов функционируют под управлением системы Microsoft Word for Windows.

В то же время, известны макровирусы, работающие под управлением таких приложений как Microsoft Exel for Windows, Lotus Ami Pro, Lotus 1-2-3, Lotus Notes, в операционных системах фирм Microsoft и Apple.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Наиболее распространенные типы вирусов и их основные особенности

Сетевые вирусы, называемые также ***автономными репликативными программами***, или, для краткости, ***репликаторами***, используют для размножения средства сетевых операционных систем. Наиболее просто реализуется размножение в тех случаях, когда сетевыми протоколами предусмотрен обмен программами. Однако, размножение возможно и в тех случаях, когда протоколы ориентированы только на обмен сообщениями.

Классическим примером реализации процесса размножения с использованием только стандартных средств электронной почты является уже упоминаемый репликатор Морриса. Текст репликатора передается от одной ЭВМ к другой как обычное сообщение, постепенно заполняющее буфер, выделенный в оперативной памяти ЭВМ-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 ЭВМ-адресате.

ОБЩАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Наиболее распространенные типы вирусов и их основные особенности

«Лазейки», подобные описанной на предыдущем слайде и обусловленные особенностями реализации тех или иных функций в программном обеспечении, являются объективной предпосылкой для создания и внедрения репликаторов злоумышленниками.

Эффекты, вызываемые вирусами в процессе реализации ими целевых функций, принято делить на следующие группы:

- искажение информации в файлах, либо в таблице размещения файлов (FAT-таблице), которое может привести к разрушению файловой системы в целом
- имитация сбоев аппаратных средств
- создание звуковых и визуальных эффектов, включая, например, отображение сообщений, вводящих оператора в заблуждение или затрудняющих его работу
- инициирование ошибок в программах пользователей или операционной системе