Вредоносное ПО и защита от него

Выполнил студент
Группы СБ-41
Логачев Сергей
Проверила:
Щучка Т.А.

Термин «компьютерный вирус» впервые употребил сотрудник Лехайского университета Ф. Коэн в 1984 году. Основная трудность, возникающая при попытках дать это определение, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и ..) либо присущи другим программам, которые никак вирусами не являются, либо существуют вирусы, которые не содержат выше отличительных черт.

Классификация вирусов

- Среда обитания
- Заражаемая операционная система
- Особенности алгоритма работы
- Деструктивные возможности

Деструктивные возможности вирусов:

1) безвредные – никак не влияющие на работу компьютера;

2) неопасные – влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми эффектами;

3) опасные – могут привести к серьезным сбоям в работе компьютера;

4) очень опасные – могут привести к потере программ, уничтожить данные, вывести из строя оборудование.

Среди особенностей алгоритма работы вирусов выделяются следующие пункты:

- резидентность
- использование стелс-алгоритмов
- самошифрование и полиморфичность
- метаморфичность

Резидентность

- Под резидентностью понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события и вызывать при этом процедуры заражения обнаруженных объектов. Резидентные копии вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы. Резидентными можно считать макро-вирусы, поскольку они постоянно присутствуют в памяти компьютера во время работы зараженного редактора.

Стелс-алгоритмы

- Использование стелс-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение, запись зараженных объектов.

Самошифрование и полиморфичность

- Такие типы используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вирусов. Шифрующийся вирус – вирус, который при заражении новых файлов и системных областей диска шифрует собственный код, пользуясь для этого случайными паролями.
- К полиморфик-вирусам относятся те из них, детектирование которых невозможно осуществить при помощи участков постоянного кода, специфичных для конкретного вируса.

Метаморфичность

- Метаморфные вирусы, так же изменяют свой код, но не используют алгоритмы шифрования. Различие проявляется в виде изменений внутри кода вируса.

Загрузочные вирусы

- Принцип действия основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера – после необходимых тестов установленного оборудования (памяти, дисков). Существуют нерезидентные загрузочные вирусы – при загрузке они заражают дискеты, если те присутствуют в дисководах.

Макро-вирусы

- Макро-вирусы являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла в другие.

Сетевые вирусы (черви)

- К ним относятся вирусы, которые для своего распространения используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию и захватить управление.

Почтовые вирусы

- Этот вирус использует для своего распространения каналы электронной почты. Заражение почтовым вирусом происходит в результате действий пользователей, просматривающих почту, а также из-за ошибок в почтовых программах и операционных системах.

Файловые вирусы

- К данной группе относятся вирусы, которые при своем размножении используют файловую систему какой-либо ОС. Внедрение файлового вируса возможно практически во все исполняемые файлы всех популярных ОС.

Программные закладки. Троянский конь

- Троянский конь:
- – 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, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие действия.

Типы троянских объектов:

1) троянские программы
2) троянские веб-сайты
3) троянские сообщения электронной почты

Модели воздействия программных закладок на компьютеры

- - Перехват
- Искажение:

1) Статическое
2) Динамическое

Защита от программных закладок

- Универсальным средством защиты является создание изолированного компьютера. Компьютер называется изолированным, если выполнены условия:

1) В нем установлена система BIOS, не содержащая закладок
2) ОС проверена на наличие закладок
3) Достоверно установлена неизменность BIOS и ОС для данного сеанса
4) На компьютере не запускалось и не запускается никаких иных программ, кроме уже прошедших проверку на присутствие в них заклакдок
5) Исключен запуск проверенных программ в каких-либо иных условиях, кроме перечисленных выше.

Клавиатурные шпионы

- Клавиатурные шпионы (кейлоггеры) - нацелены на перехват паролей пользователей ОС, а также на определение их легальных полномочий и прав доступа к компьютерным ресурсам.

Типы клавиатурных шпионов:

1) имитаторы
2) фильтры
3) заместители

Антивирусное ПО

- Методы обнаружения вирусов:
  - Сканирование
  - Блокирование подозрительных действий
  - Обнаружение изменений
  - Анализ сетевого трафика
  - Анализ базы данных почтовых программ
  - Обнаружение вирусов в системе автоматизации документооборота.