Защита информации, антивирусная защита информации

Компьютерный вирус

Первая массовая эпидемия компьютерного вируса произошла в 1986 году, когда вирус Brain «заражал» дискеты для первых массовых персональных компьютеров.

Компьютерный вирус

Компьютерный вирус - это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Признаки заражения

- замедление работы компьютера
- перезагрузка или зависание компьютера
- неправильная работа ОС или прикладных программ
- изменение длины файлов
- появление новых файлов
- уменьшение объема оперативной памяти
- рассылка сообщений e-mail без ведома автора

Способы заражения

- запустить зараженный файл;
- загрузить компьютер с зараженной дискеты или диска;
- при автозапуске CD(DVD)-диска или флэш-диска;
- открыть зараженный документ с макросами (Word или Excel);
- открыть сообщение e-mail с вирусом;
- открыть Web-страницу с вирусом;
- разрешить установить активное содержимое на Web-странице.

Жизненный цикл вируса

1. Проникновение на чужой компьютер
2. Активация
3. Поиск объектов для заражения
4. Подготовка копий
5. Внедрение копий

Классификация вирусов

По величине вредных воздействий:

- ***Неопасные*** – их влияние ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и другими внешними эффектами.
- ***Опасные*** – могут привести к сбоям и зависаниям при работе компьютера.
- ***Очень опасные*** – их активизация может привести к потере программ и данных, форматированию винчестера и т.д.

Классификация вирусов

По среде обитания:

- ***Загрузочные вирусы*** - заражают загрузочные сектора жестких дисков и мобильных носителей.
- ***Файловые вирусы*** - заражают файлы. Отдельно по типу среды обитания в этой группе также выделяют:
  - ***Классические файловые вирусы*** - различными способами внедряются в исполняемые файлы (внедряют свой вредоносный код или полностью их перезаписывают), создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы.
  - ***Макровирусы*** - написаны на внутреннем языке, так называемых макросах какого-либо приложения. Подавляющее большинство макровирусов используют макросы текстового редактора Microsoft Word.
  - ***Скрипт-вирусы*** – написаны в виде скриптов для определенной командной оболочки.

Вирусы

При подготовке своих вирусных копий для маскировки от антивирусов могут применять такие технологии как:

- ***Шифрование*** - в этом случае вирус состоит из двух частей: сам вирус и шифратор.
- ***Метаморфизм*** - вирусные копии создаются путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительного, обычно ничего не делающих команд.

Черви

Червь (сетевой червь) - это вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом.

Жизненный цикл червей

1. Проникновение в систему
2. Активация
3. Поиск объектов для заражения
4. Подготовка копий
5. Распространение копий

Классификация червей

В зависимости от типа проникновения в систему:

- ***Сетевые черви*** - используют для распространения локальные сети и Интернет
- ***Почтовые черви*** - распространяются с помощью почтовых программ
- ***IM-черви*** - используют системы мгновенного обмена сообщениями
- ***IRC-черви*** - распространяются по каналам IRC
- ***P2P-черви*** - при помощи пиринговых файлообменных сетей

Троянские программы

Троянские программы - позволяют получать управление удаленным компьютером, распространяются через компьютерные сети, часто при установке других программ (зараженные инсталляторы).

Жизненный цикл троянских программ

1. Проникновение в систему
2. Активация
3. Выполнение вредоносных действий

Классификация троянских программ

По типу вредоносной нагрузки:

- ***Клавиатурные шпионы*** - постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору.
- ***Похитители паролей*** - предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат.
- ***Утилиты скрытого удаленного управления*** - это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером.
- ***Анонимные SMTP-сервера и прокси-сервера*** - такие трояны на зараженном компьютере организовывают несанкционированную отправку электронной почты, что часто используется для рассылки спама.
- ***Утилиты дозвона*** - в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернет.
- ***Модификаторы настроек браузера*** - меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т. п.
- ***Логические бомбы*** - характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие.

Антивирусы-сканеры

- Умеют находить и лечить известные им вирусы в памяти и на диске;
- Используют базы данных вирусов;
- Ежедневное обновление баз данных через Интернет.

- лечат известные им вирусы

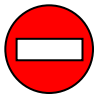
- не могут предотвратить заражение
- чаще всего не могут обнаружить и вылечить неизвестный вирус

Антивирусы-мониторы

Постоянно находятся в памяти в активном состоянии.

- перехватывают действия, характерные для вирусов и блокируют их (форматирование диска, замена системных файлов);
- блокируют атаки через Интернет;
- проверяют запускаемые и загружаемые в память файлы (например, документы Word);
- проверяют сообщения электронной почты;
- проверяют Web-страницы.

- непрерывное наблюдение
- блокируют вирус в момент заражения
- могут бороться с неизвестными вирусами



- замедление работы компьютера
- в случае ошибки ОС может выйти из строя

Антивирусные программы

Коммерческие:

- **DrWeb (www.drweb.com)**
- **Norton Antivirus (www.symantec.com)**
- **NOD32 (www.eset.com)**

Бесплатные:

- **Security Essential (http://www.microsoft.com/security_essentials/)**
- **Avast Home (www.avast.com)**
- **Antivir Personal (free-av.com)**
- **AVG Free (free.grisoft.com)**

Антивирус Касперского

- Файловый антивирус (проверка файлов в момент обращения к ним)
- Почтовый антивирус (проверка входящих и выходящих сообщений)
- Веб-антивирус (Интернет, проверка Web-страниц)
- Проактивная защита (попытки обнаружить неизвестные вредоносные программы):
  - слежение за реестром
  - проверка критических файлов
  - сигналы о «подозрительных» обращениях к памяти
- Анти-шпион (борьба с Интернет-мошенничеством)
- Анти-хакер (обнаружение сетевых атак)
- Анти-спам (фильтр входящей почты)

Другие виды антивирусной защиты

брандмауэры (файрволы, сетевые экраны)

- блокируют «лишние» обращения в сеть и запросы из сети

аппаратные антивирусы

- защита от изменения загрузочного сектора
- запрет на выполнение кода из области данных
- аппаратный брандмауэр (Лаборатории Касперского)

онлайновые (on-line) антивирусы

- устанавливают на компьютер модуль ActiveX, который проверяет файлы или файл пересылается на сайт разработчика антивирусов

Профилактика

- делать резервные копии важных данных на CD и DVD
- использовать антивирус-монитор, особенно при работе в Интернете
- при работе в Интернете включать брандмауэр (программу, запрещающую обмен по некоторым каналам связи, которые используют вирусы)
- проверять с помощью антивируса-доктора все новые программы и файлы
- не открывать сообщения e-mail с неизвестных адресов, особенно файлы-приложения
- иметь загрузочный диск с антивирусом