Вредоносное программное обеспечение и защита информации

1. Исторические данные о первых вирусах, антивирусах и вирусных эпидемиях

Первые вирусы:

1) Brain

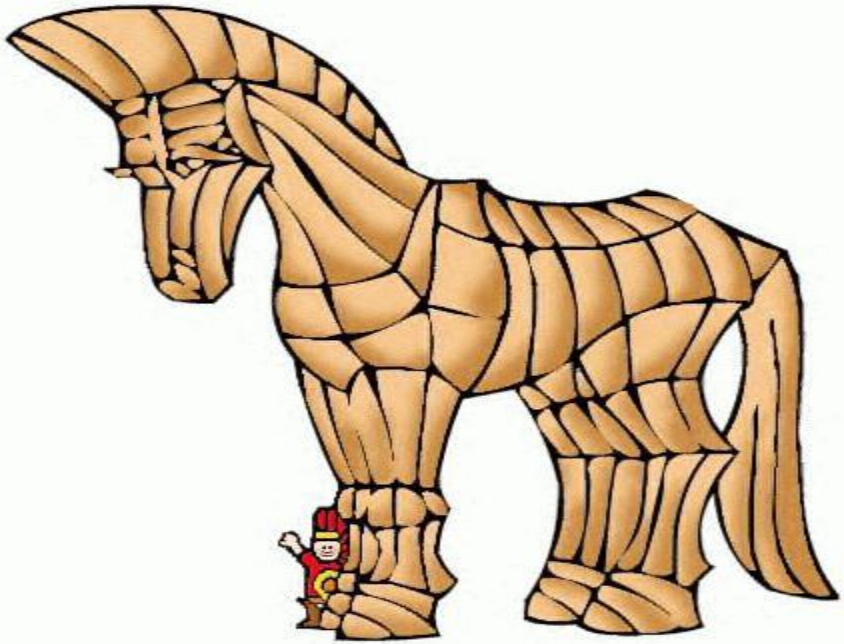
Первая эпидемия 1987 года была вызвана вирусом Brain (также известен как Пакистанский вирус), который был разработан братьями Амджатом и Базитом Алви (Amdjat и Basit Faroog Alvi) в 1986 и был обнаружен летом 1987. По данным McAfee, вирус заразил только в США более 18 тысяч компьютеров. Программа должна была наказать местных пиратов, ворующих программное обеспечение у их фирмы. В программке значились имена, адрес и телефоны братьев. Однако неожиданно для всех The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру. Вирус Brain являлся также и первым стелс-вирусом — при попытке чтения заражённого сектора он «подставлял» его незаражённый оригинал.

2) Червь Морриса

- В 1988 году Робертом Моррисом-младшим был создан первый массовый сетевой червь. 60 000-байтная программа разрабатывалась с расчётом на поражение операционных систем UNIX Berkeley 4.3. Вирус изначально разрабатывался как безвредный и имел целью лишь скрытно проникнуть в вычислительные системы, связанные сетью ARPANET, и остаться там необнаруженным. Вирусная программа включала компоненты, позволяющие раскрывать пароли, имеющиеся в инфицированной системе, что, в свою очередь, позволяло программе маскироваться под задачу легальных пользователей системы, на самом деле занимаясь размножением и рассылкой копий. Вирус не остался скрытым и полностью безопасным, как задумывал автор, в силу незначительных ошибок, допущенных при разработке, которые привели к стремительному неуправляемому саморазмножению вируса.

3) Троянский конь

В 1989 году появился первый «троянский конь» AIDS.[] Вирус делал недоступными всю информацию на жёстком диске и высвечивал на экране лишь одну надпись: «Пришлите чек на $189 на такой-то адрес». Автор программы был арестован в момент обналичивания чека и осуждён за вымогательство.



Первые антивирусы:

1) CHK4BOMB, BOMBSQAD

Первые антивирусные утилиты появились зимой 1984. Анди Хопкинс (Andy Hopkins) написал программы CHK4BOMB и BOMBSQAD. CHK4BOMB позволяла проанализировать текст загрузочного модуля и выявляла все текстовые сообщения и «подозрительные» участки кода (команды прямой записи на диск и др.). Благодаря своей простоте (фактически использовался только контекстный поиск) и эффективности CHK4BOMB получила значительную популярность. Программа BOMBSQAD.COM перехватывает операции записи и форматирования, выполняемые через BIOS. При выявлении запрещенной операции можно разрешить её выполнение.

2) DPROTECT

В начале 1985 Ги Вонг (Gee Wong) написал программу DPROTECT — резидентную программу, перехватывающую попытки записи на дискеты и винчестер. Она блокировала все операции (запись, форматирование), выполняемые через BIOS. В случае выявления такой операции программа требовала рестарта системы.

2. Вирусы. Антивирусы. И их классификация

Вредоносной программой называется любое программное обеспечение, предназначенное для получения несанкционированного доступа к информации, хранимой на компьютере, с целью причинения вреда владельцу информации, хранимой на компьютере, с целью причинения вреда владельцу информации или владельцу компьютера.

Компьютерный вирус — программа способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере

Признаки заражения:

· Прекращение работы или неправильная работа ранее успешно функционировавших программ;
· Медленная работа компьютера;
· Невозможность загрузки операционной системы;
· Исчезновение файлов и каталогов,искажение их содержимого;
· Изменение даты и времени модификации файлов;
· Изменение размеров файлов;
· Неожиданное увеличение количества файлов на диске;
· Существенное уменьшение размера свободной оперативной памяти;
· Вывод на экран непредусмотренных звуковых сигналов;
· Частые зависания и сбои в работе компьютера;

Схема работы компьютерных вирусов :

— ***Заражение.***

Происходит при запуске инфицированной программы или при обращении к носителю, имеющему вредоносный код в системной области; обычно код вируса сначала поступает в оперативную память работающего компьютера, откуда он копируется на запоминающие устройства.

— ***Размножение.***

Вирусный код может воспроизводить себя в теле других программ. Происходит как серия последовательных заражений; в первую очередь поражаются файлы самой операционной системы, чем чаще срабатывает механизм, тем больше файлов поражается.

— ***Атака.***

Последняя фаза развития вируса; во время атаки вирус производит более или менее разрушительные действия. После создания достаточного числа копий программный вирус начинает осуществлять разрушение: нарушение работы программ и ОС, удаление информации на жестком диске, самые разрушительные вирусы вызывают форматирование жесткого диска.

Классификация компьютерных вирусов:

По среде обитании:

· *файловые вирусы.*

Внедряются в файлы, имеющие расширение COM и EXE. Внедряются в программу и активизируются при их запуске. После запуска заражённой программы вирусы находятся в оперативной памяти компьютера и могут заражать другие файлы до момента выключения компьютера или перезагрузки операционной системы.

· *загрузочные вирусы.*

Располагаются в служебных секторах носителей данных и поступают в оперативную память только при загрузке компьютера с этого носителя. Внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска.

· *файлово-загрузочные вирусы.*

Заражают файлы и загрузочные сектора дисков.

· *сетевые вирусы.*

Обитают только в оперативной памяти компьютеров и не копируют себя на носители данных. Распространяются по различным компьютерным сетям. Могут передавать по компьютерным сетям свой программный код и запускать его на компьютерах, подключенных к этой сети. Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной паутине.

· *Макровирусы.*

Заражают файлы документов, например, текстовых документов. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы. Угроза заражения прекращается только после закрытия текстового документа.

По способу заражения :

· ***Резидентные*** .

При заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения

· ***Нерезидентные*** .

Не заражают оперативную память и активны ограниченное время.

По воздействию .

· ***Неопасные*** .

Не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках. Занимаются только размножением.

· ***Опасные*** .

Приводят к различным нарушениям в работе компьютера. Беспокоят неожиданными сообщениями, экранными и звуковыми эффектами.

· ***Очень опасные*** .

Могут приводить к потере программ, данных, стиранию информации в системных областях дисков.

По особенностям алгоритма:

· ***Паразиты*** .

Не изменяют содержимое файлов и секторов, легко обнаруживаются.

· ***Черви*** .

Вычисляют адреса сетевых компьютеров и отправляют по ним свои копии.

· ***Стелсы*** .

Перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области.

· ***Мутанты*** .

Содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую.

· ***Трояны*** .

Не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему.

Правила защиты от компьютерных вирусов:

- Регулярно тестируйте компьютер на наличие вирусов с помощью антивирусных программ
- Перед считыванием информации с дискет проверяйте их на наличие вирусов
- Всегда защищайте свои дискеты от записи при работе на других компьютерах
- Делайте архивные копии ценной для вас информации
- Не оставляйте дискету в дисководе
- Не используйте программы, поведение
- которых непонятно

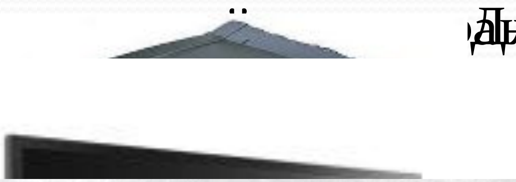
Методы борьбы с компьютерными вирусами:

- 1. Резервное копирование всех программ, файлов и системных областей дисков на дискеты, чтобы можно было восстановить данные в случае вирусной атаки. Создание системной и аварийной дискеты.
- 2. Ограничение доступа к машине путем введения пароля, администратора, закрытых дисков.
- 3. Использование только лицензионного программного обеспечения, а не пиратских копий, в которых могут находиться вирусы.
- 4. Проверка всей поступающей извне информации на вирусы, как на дискетах, CD-ROM, так и по сети.
- 5. Применение антивирусных программ и обновление их версий.
- 6. Периодическая проверка компьютера на наличие вирусов при помощи антивирусных программ.

Классификация антивирусного программного обеспечения:

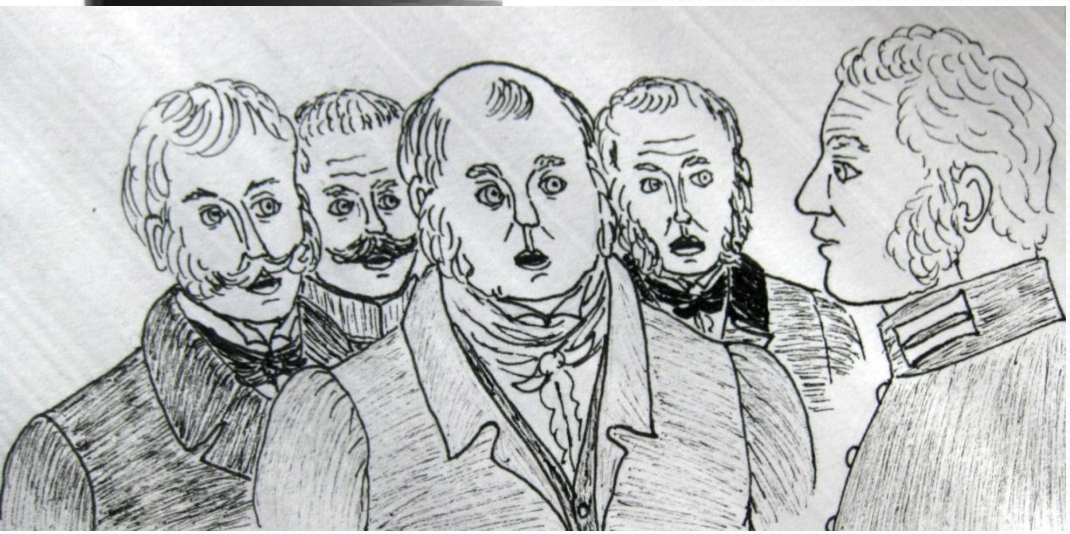
Сканеры

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов.



роверяют созданные ими образы и производят

стоянием.




Как не пострадать фигней?