Компьютерные вирусы

Вирус - *это программа, способная самовоспроизводиться, "приписывать" себя к другим программам (т.е "заражать" их), а также выполнять различные нежелательные действия на компьютере.*

Подробнее.

- Вирусы принято делить на классы по следующим основным признакам:

1. среда обитания;
2. операционная система;
3. алгоритм работы;
4. объем причиненного вреда;

По среде обитания :

1. файловые - это те, которые при своем размножении используют файловую систему определенной операционной системы.
2. загрузочные заражают загрузочный (Boot) сектор флоппи-диска и Boot-сектор или Master Boot Record (MBR) винчестер.
3. макро - вирусы на макроязыках различных приложений, вроде MS Excel (VB), MS Word (WB) и т.п. Для своего размножения они используют возможности макроязыков и с их помощью переносят себя из одного зараженного файла (документа или таблицы) в другие.
4. сетевые - такие вирусы, которые при своем распространении используют возможности Internet и локальных сетей.

По алгоритму работы:

1. резидентные;
2. с использованием стел-с – алгоритмов;
3. с самошифрованием и полиморфичностью;
4. с использованием нестандартных приемов;

По объему причиненного вреда:

1. безвредные, т.е. никак не влияющие на работу компьютера;
2. неопасные, т.е. те, которые просто себя распространяют, при этом, например, выдвигая CD-Rom или мигая лампочками на клавиатуре;
3. опасные, которые могут привести к серьезным сбоям компьютера;
4. очень опасные, которые могут привести к потере программ, уничтожить данные, стереть информацию, даже ту, которая находится в системной области данных!

История компьютерных вирусов.

Компьютерные вирусы являются одной из разновидностей компьютерного вандализма, получившего распространение в конце 80-х гг. Исторически их возникновение связано с идеей создания самовоспроизводящихся программ - концепции, уходящей своими корнями в пятидесятые годы.

– Троянские кони (логические бомбы).

К троянским коням относятся программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от каких-либо условий или при каждом запуске уничтожающая информацию на дисках, "завешивающая" систему и т.п.Большинство известных троянских коней являются программами, которые "подделываются" под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по BBS-станциям или электронным конференциям. По сравнению с вирусами "троянские кони" не получают широкого распространения по достаточно простым причинам - они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.

– Intended-вирусы

К таким вирусам относятся программы, которые на первый взгляд являются стопроцентными вирусами, но не способны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания. К категории "intended" также относятся вирусы, которые по приведенным выше причинам размножаются только один раз - из "авторской" копии. Заразив какой-либо файл, они теряют способность к дальнейшему размножению.

– Полиморфные генераторы

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т.е. открытия, закрытия и записи в файлы, чтения и записи секторов и т.д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика. Обычно полиморфные генераторы распространяются их авторами без ограничений в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор

– Конструкторы вирусов

Конструктор вирусов - это утилита, предназначенная для изготовления новых компьютерных вирусов. Известны конструкторы вирусов для DOS, Windows и макро-вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули, и/или непосредственно зараженные файлы.

Методы борьбы с вирусами.

Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов:

-Детекторы;
-Доктора (фаги);
-Ревизоры;
-Доктора-ревизоры;
-Фильтры;
-Вакцины (иммунизаторы).

ВНИМАНИЕ!!!

Создан первый компьютерный вирус, способный попасть в компьютер через фото-, видеокамеры и сканеры. Вирус VAZA существуют в видемодифицированных фигур Лиссажа на любом полиграфическом носителе, он способен проникать в систему при попытке отсканировать его или переснять вышеперечисленной периферией.

Подробнее…

После попадания в компьютер VAZA разрушает все графические файлы превращая их из цветных или полутоновых в черно-белые, после чего VAZA самоуничтожается. Через сетевые протоколы вирус не передается. Есть мнение, что создание вируса VAZA финансирует правительство США с целью усилить защиту национальной валюты. На данном этапе VAZA пока нельзя внедрить в уже готовое изображение, но разработки продолжаются. Не исключено и то, что вирус VAZA - это происки Алькаиды, стремящейся навязать миру черно-белое видение.

БУДЬТЕ ОСТОРОЖНЫ ! СТАРАЙТЕСЬ НЕ СКАНИРОВАТЬ И НЕ ПЕРЕСНИМАТЬ КАРТИНКИ СО СЛОЖНОПОВТОРЯЮЩИМСЯ РИСУНКОМ! ЭТО МОЖЕТ БЫТЬ ОПАСНО ДЛЯ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ НА ВАШЕМ КОМПЬЮТЕРЕ!

Резидентные вирусы.

Под термином "резидентность" (DOS'овский термин TSR - Terminate and Stay Resident) понимается способность вирусов оставлять свои копии в операционной системе, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов). Таким образом, резидентные вирусы активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу.

Подробнее…

Стелс-вирусы.

Стелс-вирусы теми или иными способами скрывают факт своего присутствия в системе.

Подробнее…

Полиморфик-вирусы и «вредные» программы.

– Полиморфик-вирусы.

К полиморфик-вирусам относятся те из них, детектирование которых невозможно (или крайне затруднительно) осуществить при помощи так называемых вирусных масок - участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами - шифрованием основного кода вируса с непостоянным ключем и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса.

– Прочие «вредные» программы.

К «вредным» программам, помимо вирусов, относятся также:

- троянские кони (логические бомбы);
- intended-вирусы;
- конструкторы вирусов;
- полиморфик-генераторы.

Подробнее…