Компьютерные вирусы

Классификация компьютерных вирусов

1. **По среде "обитания"** компьютерные вирусы делятся на:
    1) Файловые
    2) Загрузочные
    3) Макровирусы
    4) Сетевые

- ***Файловые вирусы*** внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

- ***Загрузочные вирусы*** записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик жесткого диска (Master Boot Record), либо меняют указатель на активный boot-сектор.

- ***Макровирусы*** заражают файлы-документы и электронные таблицы популярных офисных приложений.

- ***Сетевые вирусы*** используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

- Существует большое количество сочетаний – например, ***файлово-загрузочные вирусы***, заражающие как файлы, так и загрузочные сектора дисков.

Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс- и полиморфик-технологии.

- Другой пример такого сочетания – ***сетевой макровирус***, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Классификация компьютерных вирусов

2. **Заражаемая операционная система** является вторым уровнем деления вирусов на классы (по видам ОС).

- Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких OS – DOS, Windows, и т. д.

- Макровирусы заражают файлы форматов Word, Excel, пакета Office.

- Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Классификация компьютерных вирусов

3. **По особенностям алгоритма работы** вирусы делятся на:

– Резидентные;

– Стелс-вирусы;

– Полиморфик-вирусы;

– Вирусы, использующие нестандартные приемы.

Резидентный вирус при инфицировании компьютера оставляет в

- оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них.
- Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы.

Нерезидентные вирусы не заражают память компьютера и сохраняют

- активность ограниченное время

Использование ***стелс-алгоритмов*** позволяет вирусам полностью или частично скрыть себя в системе.

- Наиболее распространенным стелс-алгоритмом является перехват запросов операционной системы на чтение/запись зараженных объектов.
- Стелс-вирусы при этом либо временно лечат их, либо "подставляют" вместо себя незараженные участки информации.
- В случае макровирусов наиболее популярный способ – запрет вызовов меню просмотра макросов.

Самошифрование и полиморфичность используются практически

- всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования (обнаружения) вируса.

Полиморфик-вирусы (polymorphic) – это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т. е. не содержащие ни одного постоянного участка кода.

- В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения.
- Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные ***нестандартные приемы*** часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре операционной системы,защи тить от обнаружения свою резидентную копию, затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т. д.

Классификация компьютерных вирусов

4. По **деструктивным возможностям** вирусы можно разделить на:

– ***безвредные***, т. е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

– ***неопасные***, влияние которых ограничивается уменьшением свободной памяти на диске;

– ***опасные вирусы***, которые могут привести к серьезным сбоям в работе компьютера;

– ***очень опасные***, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже повредить аппаратные средства компьютера.

- Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия.
- К "***троянским***" программам относятся программы, наносящие какие-либо разрушительные действия в зависимости от каких-либо условий.
- Например, уничтожение информации на дисках при каждом запуске или по определенному графику и т. д.
- К "троянским" программам также относятся так называемые "дропперы" вирусов – зараженные файлы, код которых подправлен таким образом, что известные версии антивирусов не определяют присутствие вируса в файле.

Отметим еще один тип программ (программы – "злые шутки"), которые используются для устрашения пользователя, предупреждают о возможном заражении вирусом или о каких либо предстоящих действиях с этим связанных, т. е. сообщают о несуществующих опасностях, вынуждая пользователя к активным действиям.

- ***Утилиты скрытого администрирования*** являются разновидностью "логических бомб" ("троянских программ"), которые используются злоумышленниками для удаленного администрирования компьютеров в сети.
- По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов.
- Внедренные в операционную систему утилиты скрытого управления позволяют делать с компьютером все, что в них заложил их автор: принимать/отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т. д.
- В результате эти программы могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и т. п.

- ***К "Intended" - вирусам*** относятся программы, которые, на первый взгляд, являются стопроцентными вирусами, но не способны размножаться по причине ошибок.
- Например, вирус, который при заражении не помещает в начало файла команду передачи управления на код вируса, либо записывает в нее неверный адрес своего кода, либо неправильно устанавливает адрес перехватываемого прерывания (в большинстве приводит к «зависанию» компьютера) и т. д.
- К категории "intended" также относятся вирусы, которые по приведенным выше причинам размножаются только один раз – из "авторской" копии.

- ***Конструкторы вирусов***
- К данному виду "вредных" программ относятся утилиты, предназначенные для изготовления новых компьютерных вирусов.
- Известны конструкторы вирусов для DOS, Windows и макровирусов.
- Они позволяют генерировать исходные тексты вирусов, объектные модули, и/или непосредственно зараженные файлы.

Полиморфные 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.

СПАСИБО ЗА ВНИМАНИЕ!