

image not found or type unknown



Вирусы можно разделить на классы по следующим основным признакам:

1. среда обитания;
2. операционная система (ОС);
3. особенности алгоритма работы;
4. деструктивные возможности.

По СРЕДЕ ОБИТАНИЯ вирусы можно разделить на:

1. файловые;
2. загрузочные;
3. макро;
4. сетевые.

Файловые вирусы либо различными способами 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 винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макро-вирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

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 полиморфические технологии. Другой пример такого сочетания - сетевой макро-вирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

Заражаемая ОПЕРАЦИОННАЯ СИСТЕМА (вернее, ОС, объекты которой подвержены заражению) является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких ОС - DOS, Windows, Win95/NT, OS/2 и т.д. Макро-вирусы заражают файлы форматов Word, Excel, Office97. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

Среди ОСОБЕННОСТЕЙ АЛГОРИТМА РАБОТЫ вирусов выделяются следующие пункты:

1. резидентность;
2. использование стелс-алгоритмов;
3. самошифрование и полиморфичность;
4. использование нестандартных приемов.

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. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными.

Резидентными можно считать макро-вирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

В многозадачных операционных системах время «жизни» резидентного DOS-вируса также может быть ограничено моментом закрытия зараженного DOS-окна, а активность загрузочных вирусов в некоторых операционных системах

ограничивается моментом инсталляции дисковых драйверов ОС.

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. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макро-вирусов наиболее популярный способ -- запрет вызовов меню просмотра макросов. Один из первых файловых стелс-вирусов -- вирус «Frodo», первый загрузочный стелс-вирус -- «Brain».

САМОШИФРОВАНИЕ и ПОЛИМОРФИЧНОСТЬ используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования 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 ОС (как это делает вирус «ЗАРАЗА»), защитить от обнаружения свою резидентную копию (вирусы «TPVO», «Trout2»), затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т.д.

По ДЕСТРУКТИВНЫМ ВОЗМОЖНОСТЯМ вирусы можно разделить на:

1. безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
2. неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
3. опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
4. 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, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить

в резонанс и разрушать головки некоторых типов винчестеров.

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. Ведь вирус, как и всякая программа, имеет ошибки, в результате которых могут быть испорчены как файлы, так и сектора дисков (например, вполне безобидный на первый взгляд вирус «DenZuk» довольно корректно работает с 360К дискетами, но может уничтожить информацию на дискетах большего объема). До сих пор попадаются вирусы, определяющие «СОМ или ЕХЕ» не по внутреннему формату файла, а по его расширению. Естественно, что при несовпадении формата и расширения имени файл после заражения оказывается неработоспособным. Возможно также «заклинивание» резидентного вируса и системы при использовании новых версий DOS, при работе в Windows или с другими мощными программными системами. И так далее. Конец формы