{jcomments on}

Компьютерный вирус – это вредоносный программный код, способный к самораспространению.

Классифицируют вирусы по:

1. По признаку операционной системы:

1.1 Вирусы для ОС семейства Windows.

1.2 Вирусы для ОС UNIX-подобных систем.

2. Среде обитания:

2.1 Файловые: вирус, присоединяется к программным файлам, например к текстовому редактору или компьютерным играм. При запуске инфицированной программы этот вирус размещается в памяти так, чтобы заразить другие приложения, запускаемые пользователем. Таким способом вирус распространяется по компьютеру пользователя, а если пользователь даст кому-то дискету или «флешку» с инфицированным приложением или пошлет это приложение по сети, то зараженным окажется и другой компьютер.

2.2 Загрузочные (бутовые): называются так потому, что заражают загрузочный (boot) сектор – записывают себя в загрузочный сектор диска (boot - сектор) либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record). Загрузочные вирусы замещают код программы, получающей управление при загрузки системы. Таким образом, при перезагрузке управление передается вирусу. При этом, оригинальный -

сектор обычно переносится в какой – либо другой сектор диска.

2.3 Файловые – загрузочные: вирусы, заражающие как файлы, так и загрузочные сектора дисков.

3. Структуре (сигнатуре):

3.1 Полиморфные (мутанты): вирусы способные к самомодификации. Две версии одной программы могут не совпадать ни в одном байте. Обычно свойство полиморфизма в чистом виде у компьютерных вирусов не встречается и идет в комплексе с другими.

3.2 Стелс - вирусы (невидимки): скрывают факт своего присутствия в системе. Они изменяют информацию таким образом, что файл появляется перед пользователем в не зараженном виде.

3.3 Спутники: вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE файлов файлы-спутники, имеющие такое же имя, но с расширением COM. Вирус записывается в COM файл и никак не изменяет EXE файл. При запуске такого файла DOS первым обнаружит и выполнит COM файл, то есть вирус, который затем запустит и EXE файл.

3.4 Черви: разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. В отличие от других типов компьютерных вирусов червь является самостоятельной программой. Черви могут использовать различные механизмы распространения. Некоторые черви требуют определенного действия пользователя для распространения (например, открытия инфицированного сообщения в клиенте электронной почты). Другие черви могут распространяться автономно, выбирая и атакуя компьютеры в полностью автоматическом режиме.

3.5 Троянские: вирусы, целью которых являются шпионские действия и информация пользователя. «Трояны» не имеют собственного механизма распространения, и этим

отличаются от вирусов, которые распространяются, прикрепляя себя к безобидному ПО или документам.

3.5.1 Троянцы - вымогатели: парализуют работу пользователя размещая на рабочем столе баннер, в котором указывается, что пользователь нарушил законодательство и для снятие баннера необходима оплата. Примечание: оплату производить не стоит, необходимо обратиться к специалистам или воспользоваться данным решением

3.5.2 Троянцы - шифровальщики: так же размещают баннер на рабочем столе, но при этом шифруют файлы пользователя. При заражении необходимо обратиться в антивирусные лаборатории.

3.6 Макровирусы: вирусы, написанные на макроязыках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т. д.). Они заражают документы и электронные таблицы ряда офисных редакторов. Для размножения они используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла в другие. Наибольшее распространение получили макровирусы для Microsoft Word, Excel. Вирусы этого типа получают управление при открытии зараженного файла и инфицируют файлы, к которым впоследствии идет обращение из соответствующего офисного приложения – Word, Excel и пр.

4. Резидентным и нерезидентным

Вирус находится в оперативной памяти и перехватывает сообщения ОС. Если нерезидентные вирусы активны только в момент запуска зараженной программы, то резидентные вирусы находятся в памяти и остаются активными вплоть до выключения компьютера или перезагрузки операционной системы. Резидентные вирусы находятся в оперативной памяти, перехватывают обращения операционной системы к тем или иным объектам и внедряются в них. Такие вирусы активны не только в момент работы зараженной программы, но и после завершения ее работы.

5. По деструктивным возможностям

5.1 Безвредные: т.е. никак не влияющие на работу компьютера, кроме уменьшения свободной памяти на диске в результате своего распространения.

5.2 Неопасные: вирусы, не ведущие к потере информации. Их влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами.

5.3 Опасные: вирусы способные повредить информацию или привести к серьезным сбоям в работе компьютера.

5.4 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.