Защита от компьютерных вирусов. Признаки заражения компьютера.

Вирус — программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

Как следует из определения, основная черта компьютерного вируса – способность распространяться при запуске.

Вредоносные программы — это программы, предназначенные для незаконного доступа к информации, для скрытого использования компьютера или для нарушения работы

Создание и распространение компьютерных вирусов и вредоносных программ – это уголовные преступление, которое предусматривает (в особо тяжких случаях) наказание до 7 лет лишения свободы

Признаки заражения вирусом:

- замедление работы компьютера;
- уменьшение объема оперативной памяти;
- зависание, перезагрузка или блокировка компьютера;
- ошибки при работе ОС или прикладных программ;
- изменение длины файлов, появление новых файлов (в том числе «скрытых»);
- рассылка сообщений по электронной почте без ведома автора.

Вирусы заражают не любые данные, а только программный код, который может выполняться.

Например:

- исполняемые программы (с расширениями .exe, .com);
- загрузочные сектора дисков;
- пакетные командные файлы (.bat);
- драйверы устройств;
- библиотеки динамической загрузки (.dll), функции из которых вызываются из прикладных программ;
- документы, которые могут содержать *макросы* – небольшие программы, выполняющиеся при нажатии на клавиши или выборе пункта меню; например, макросы нередко используются в документах пакета *Microsoft Office*;
- веб-страницы (в них можно внедрить программу-*скрипт*, которая выполнится при просмотре страницы на компьютере пользователя).

Сейчас существуют два основных источника заражения вредоносными программами – флэш-диски и компьютерные сети.

Компьютер может быть заражен при:

- запуске зараженного файла;
- загрузке с зараженного CD(DVD)-диска или флэш-диска;
- автозапуске зараженного CD(DVD)-диска или флэш-диска (вирус автоматически запускается из файлаautorun.inf в корневом каталоге диска);
- открытии зараженного документа с макросами;
- открытии сообщения электронной почты с вирусом или запуске зараженной программы, полученной в приложении к сообщению;
- открытии веб-страница с вирусом;
- установке активного содержимого для просмотра веб-страницы.

Типы вредоносных программ

К вредоносным программам относятся компьютерные вирусы, черви, троянские программы и др. По «среде обитания» обычно выделяют следующие типы вирусов:

- файловые – внедряются в исполняемые файлы, системные библиотеки и т.п.;
- загрузочные – внедряются в загрузочный сектор диска или в главную загрузочную запись винчестера (англ. *MBR = Master Boot Record*); опасны тем, что загружаются в память раньше, чем ОС и антивирусные программы;
- макровирусы – поражают документы, в которых могут быть макросы;
- скриптовые вирусы – внедряются в командные файлы или в веб-страницы (записывая в них код на языке *VBScript* или *JavaScript*);

Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС.

Файловые вирусы :

- *различными способами внедряются в исполняемые файлы (наиболее распространенный тип вирусов);*
- *создают файлы-двойники (компаньон-вирусы);*
- *создают свои копии в различных каталогах;*
- *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. Данный тип вирусов был достаточно распространён в 1990-х, но практически исчез с переходом на 32-битные операционные системы и отказом от использования дискет как основного способа обмена информацией. Теоретически возможно появление загрузочных вирусов, заражающих CD-диски и USB-флешек, но на текущий момент такие вирусы не обнаружены.

Многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макро-языки для автоматизации выполнения повторяющихся действий. Эти макро-языки часто имеют сложную структуру и развитый набор команд. Макро-вирусы являются программами на макро-языках, встроенных в такие системы обработки данных. Для своего размножения вирусы этого класса используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Скрипт-вирусы, также как и макро-вирусы, являются подгруппой файловых вирусов. Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы (командные и служебные файлы MS Windows или Linux), либо являются частями многокомпонентных вирусов. Также, данные вирусы могут заражать файлы других форматов (например, HTML), если в них возможно выполнение скриптов.

Некоторые вирусы при создании новой копии немного меняют свой код, для того чтобы их было труднее обнаружить. Такие вирусы называют «полиморфными» (от греч. *πολυ* — много, *μορφη* — форма, внешний вид).

Червь *(сетевой червь) - это вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом.*

Наиболее опасны *сетевые черви*, которые используют «дыры» (ошибки в защите, уязвимости) операционных систем и распространяются очень быстро без участия человека. Зараженные компьютеры используются для рассылки *спама* (нежелательных рекламных сообщений) или массовых *DOS*-атак на сайты в Интернете.

Почтовые черви распространяются как приложения к сообщениям электронной почты. Они представляют собой программы, которые при запуске заражают компьютер и рассылают свои копии по всем адресам из адресной книги пользователя.

Еще одна группа вредоносных программ – троянские программы или «троянцы» (трояны).

Троян *(троянский конь) - программа, основной целью которой является вредоносное воздействие по отношению к компьютерной системе. Трояны отличаются отсутствием механизма создания собственных копий.*

Троянские программы проникают на компьютер под видом «полезных» программ, например, кодеков для просмотра видео или экранных заставок (которые включаются, если некоторое время не работать на компьютере). В отличие от вирусов и червей, они не могут распространяться самостоятельно и часто «путешествуют» вместе с червями.

Клавиатурные шпионы, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору.

Похитители паролей предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат.

Утилиты скрытого удаленного управления - это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Перечень действий, которые позволяет выполнять тот или иной троян, определяется его функциональностью, заложенной автором. Обычно это возможность скрыто загружать, отсылать, запускать или уничтожать файлы. Такие трояны могут быть использованы как для получения конфиденциальной информации, так и для запуска вирусов, уничтожения данных.

Логические бомбы характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов.