ВИРУСЫ

Одной из главных причин уничтожения информации в настоящее время является распространение компьютерных вирусов.

Компьютерный вирус – это специальная компьютерная программа, как правило, небольшая по размерам, которая при своем запуске уничтожает или портит данные, хранящиеся на компьютере.

Компьютерный вирус может "приписывать" себя к другим программам, как говорят, "заражать" их. Такое "заражение" приводит к тому, что компьютерные вирусы могут самостоятельно распространяться и размножаться. Вследствие чего, большое число компьютеров может одновременно выйти из строя.

Признаки заражения:

- замедление работы компьютера
- перезагрузка или зависание компьютера
- неправильная работа ОС или прикладных программ
- изменение длины файлов
- появление новых файлов
- уменьшение объема оперативной памяти
- рассылка сообщений *e-mail* без ведома автора

Вредные действия вирусов

- звуковые и зрительные эффекты
- имитация сбоев ОС и аппаратуры
- перезагрузка компьютера
- разрушение файловой системы
- уничтожение информации
- шпионаж – передача секретных данных
- массовые атаки на сайты Интернет

Несмотря на возможность заражения компьютера вирусом, надо знать, что вирусом могут заразиться не все файлы компьютера.

ЗАРАЖАЮТСЯ:

- программы – ***.exe, *.com**
- загрузочные сектора дисков и дискет
- командные файлы – ***.bat**
- драйверы – ***.sys**
- библиотеки – ***.dll**
- документы с макросами – ***.doc, *.xls, *.mdb**
- *Web*-страницы со скриптами

НЕ ЗАРАЖАЮТСЯ:

- текст – ***.txt**
- рисунки – ***.gif, *.jpg, *.png, *.tif**
- звук (***.wav, *.mp3, *.wma**)
- видео (***.avi, *.mpg, *.wmv**)
- любые данные (без программного кода)

Непосредственное заражение компьютера вирусом может произойти в одном из следующих случаев:

- на компьютере была выполнена зараженная программа;
- компьютер загружался с дискеты, содержащей зараженный загрузочный сектор;
- на компьютере была установлена зараженная операционная система;
- на компьютере обрабатывались файлы, содержащие в своем теле зараженные макросы.

Классические вирусы

- **Файловые** – заражают файлы **`*.exe, *.sys, *.dll`** (редко – внедряются в тексты программ).
- **Загрузочные (бутовые, от англ. *boot – загрузка*) –** заражают загрузочные сектора дисков и дискет, при загрузке сразу оказываются в памяти и получают управление.
- **Полиморфные** – при каждом новом заражении немного меняют свой код.
- **Макровирусы** – заражают документы с макросами (**`*.doc, *.xls, *.mdb`**).
- **Скриптовые вирусы –** скрипт (программа на языке *Visual Basic Script*, *JavaScript*, BAT, PHP) заражает командные файлы (**`*.bat`**), другие скрипты и Web-страницы (**`*.htm, *.html`**).

Сетевые вирусы

распространяются через компьютерные сети, используют «дыры» – ошибки в защите *Windows, Internet Explorer, Outlook* и др.

- **Почтовые черви –** распространяются через электронную почту в виде приложения к письму или ссылки на вирус в Интернете; рассылают себя по всем обнаруженным адресам
- **Сетевые черви** – проникают на компьютер через «дыры» в системе, могут копировать себя в папки, открытые для записи (сканирование – поиск уязвимых компьютеров в сети)
- **IRC-черви, IM-черви –** распространяются через IRC-чаты и интернет-пейджеры (*ICQ*, *AOL*, *Windows Messenger*, *MSN Messenger*)
- **P2P-черви** – распространяются через файлообменные сети P2P (*peer-to-peer)*

Троянские программы

позволяют получать управление удаленным компьютером, распространяются через компьютерные сети, часто при установке других программ (зараженные инсталляторы)

- **Backdoor –** программы удаленного администрирования
- **воровство паролей** (доступ в Интернет, к почтовым ящикам, к платежным системам)
- **шпионы** (введенный с клавиатуры текст, снимки экрана, список программ, характеристики компьютера, промышленный шпионаж)
- **DOS-атаки** (англ. *Denial Of Service* – отказ в обслуживании) – массовые атаки на сайты по команде, сервер не справляется с нагрузкой
- **прокси-сервера** – используются для массовой рассылки рекламы (спама)
- **загрузчики** (англ. *downloader*) – после заражения скачивают на компьютер другие вредоносные программы

Антивирусы-сканеры

- умеют находить и лечить **известные им** вирусы в памяти и на диске;
- используют базы данных вирусов;
- ежедневное обновление баз данных через Интернет.

Антивирусы-мониторы

- постоянно находятся в памяти в активном состоянии
- блокируют их (форматирование диска, замена системных файлов);
- блокируют атаки через Интернет;
- проверяют запускаемые и загружаемые в память файлы (например, документы *Word*);
- проверяют сообщения электронной почты;
- проверяют *Web*-страницы;
- проверяют сообщения ICQ

Другие виды антивирусной защиты

брандмауэры (файрволы, сетевые экраны)

- блокируют «лишние» обращения в сеть и запросы из сети

аппаратные антивирусы

- защита от изменения загрузочного сектора
- запрет на выполнение кода из области данных
- аппаратный брандмауэр ZyWALL UTM (ZyXEL и Лаборатории Касперского)

онлайновые (*on-line*) антивирусы

- устанавливают на компьютер модуль *ActiveX,* который проверяет файлы…
- или файл пересылается на сайт разработчика антивирусов

Профилактика

- ✔ делать **резервные копии** важных данных на CD и DVD (раз в месяц? в неделю?)
- ✔ использовать **антивирус-монитор**, особенно при работе в Интернете
- ✔ при работе в Интернете включать **брандмауэр** (англ. *firewall*) – эта программа запрещает обмен по некоторым каналам связи, которые используют вирусы
- ✔ **проверять** с помощью антивируса-доктора все новые программы и файлы, дискеты
- ✔ **не открывать** сообщения e-mail с неизвестных адресов, особенно файлы-приложения
- ✔ иметь **загрузочный диск** с антивирусом

Если компьютер заражен…

- Отключить компьютер от сети.
- Запустить антивирус. Если не помогает, то…
- выключить компьютер и загрузить его с загрузочного диска (дискеты, CD, DVD). Запустить антивирус. Если не помогает, то…
- удалить *Windows* и установить ее заново. Если не помогает, то…
- отформатировать винчестер (**format.com**). Если сделать это не удается, то могла быть испорчена таблица разделов диска. Тогда …
- создать заново таблицу разделов (**fdisk.exe**). Если не удается (винчестер не обнаружен), то…
- можно нести компьютер в ремонт.