Компьютерные вирусы

Компью́терный ви́рус — разновидность компьютерной программы, отличительной особенностью которой является **способность к размножению** (саморепликация). В дополнение к этому он *может* повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени которого была запущена заражённая программа.

Немного об истории

Интересно, что идея компьютерных вирусов появилась намного раньше самих персональных компьютеров. Точкой отсчета можно считать труды известного ученого Джона фон Неймана по изучению самовоспроизводящихся математических автоматов, о которых стало известно в 1940-х годах. В 1951 году он предложил способ создания таких автоматов. А в 1959 году журнал Scientific American опубликовал статью Л.С. Пенроуза, посвященную самовоспроизводящимся механическим структурам. В ней была описана простейшая двумерная модель самовоспроизводящихся механических структур, способных к активации, размножению, мутациям, захвату. Позднее другой ученый Ф.Ж. Шталь реализовал данную модель на практике с помощью машинного кода на IBM 650.

Прообраз компьютерного вируса

В 1962 г. инженеры из американской компании Bell Telephone Laboratories - В.А. Высотский, Г.Д. Макилрой и Роберт Моррис - создали игру "Дарвин". Игра предполагала присутствие в памяти вычислительной машины так называемого супервизора, определявшего правила и порядок борьбы между собой программ-соперников, создававшихся игроками. Программы имели функции исследования пространства, размножения и уничтожения. Смысл игры заключался в удалении всех копий программы противника и захвате поля битвы.

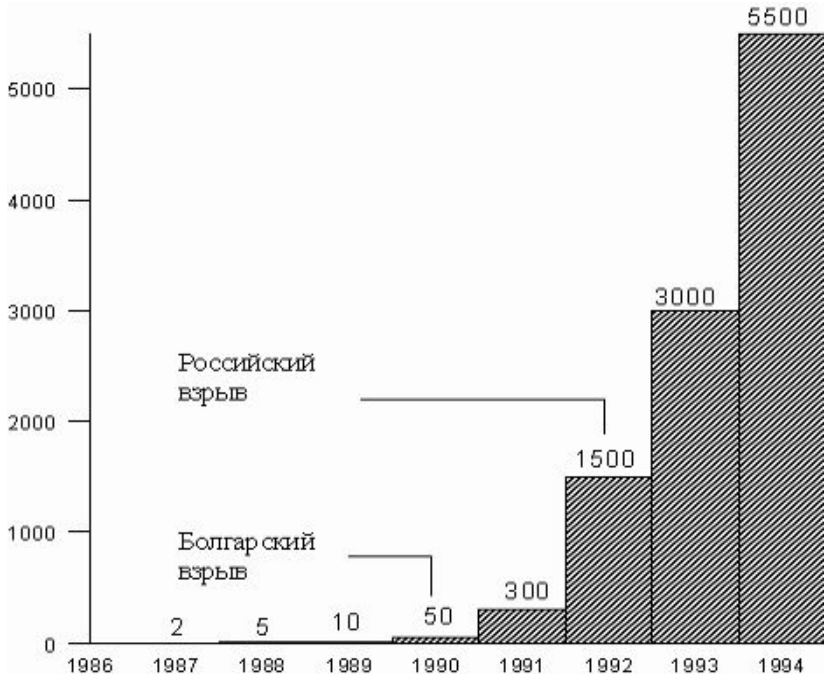
Грегори Бенфорд

Одни считают, что впервые слово вирус по отношению к программе было употреблено Грегори Бенфордом (Gregory Benford) в фантастическом рассказе «Человек в шрамах» (*The Scarred Man*), опубликованном в журнале Venture в мае 1970 года.

Другие считают, что идею создания компьютерных вирусов подбросил писатель-фантаст Т. Дж. Райн, который в одной из своих книг, опубликованной в США в 1977 г., описал эпидемию, за короткое время поразившую более 7000 компьютеров.

- **1959 г.** - на ЭВМ IBM 650 обнаружен вирус, который «съедал» часть слов.
- Первая «эпидемия» компьютерного вируса произошла в **1986** году, когда вирус по имени Brain (англ. «мозг») заражал дискеты персональных компьютеров.
- **1988 г**. - Роберт Моррис в США написал вирус, поразивший 2000 компьютеров.
- **В середине августа 1995 г.** в США и ряде стран Западной Европы появился вирус, который использует возможность представления информации в виде конгломерата данных и программ. Он заражает документы, подготовленные в системе MS Word for Windows-файлы типа *.doc.
- **26 апреля 1999 г.** Новым словом в вирусологии стал вирус под названием «Чернобыль» или WIN95.CIN. Данный вирус в отличии от своих собратьев в зависимости от модификации мог уничтожить MBR жесткого диска, таблицу размещения данных и не защищенную от перезаписи Flash-память. Волна эпидемии этого вируса прокатилась по всему миру. Громадный материальный ущерб был нанесен в Швеции. Пострадало большое количество пользователей и в России.

Начиная с конца 1990г, появилась новая тенденция, получившая название «экспоненциальный вирусный взрыв». Количество новых вирусов, обнаруженных в месяц, стало исчисляться сотнями. Поначалу эпицентром взрыва была Болгария, затем он переместился в Россию.



В настоящее время известно более 50 тысяч вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям.

Классификация вирусов

В настоящее время нет единой классификации вирусных программ, но их можно выделить по следующим признакам:

- **по среде обитания;**
- **по способу заражения среды обитания;**
- **по особенностям алгоритма;**
- **по степени воздействия.**

В зависимости от среды обитания вирусы можно разделить:

Сетевые вирусы – распространяются по различным компьютерным сетям;

Файловые вирусы – внедряются в файлы, имеющие расширение COM и EXE;

Загрузочные вирусы – внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска;

Файлово-загрузочные вирусы – заражают файлы и загрузочные сектора дисков.

По способу заражения вирусы делятся на:

1. Резидентные – при заражении оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения и внедряется в них.
2. Нерезидентные вирусы – не заражают память компьютера и являются активными ограниченное время.

По особенностям алгоритма вирусы имеют большое разнообразие

1. Простейшие вирусы – не изменяют содержимое файлов, могут быть легко обнаружены и уничтожены.
2. Черви – распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и рассылают свои копии по этим адресам.
3. Вирусы – невидимки (стелс-вирусы) – трудно обнаружить и обезвредить, подставляют вместо своего тела незараженные участки диска.
4. Вирусы-мутанты – содержат алгоритмы шифровки/расшифровки, наиболее трудно обнаружить.
5. Трояны – маскируются под полезную программу, разрушают загрузочный сектор и файловую систему, воруют пароли.
6. Макровирусы – заражают файлы документов, например, текстовых документов. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы.

Пример макровируса

Первый из них – DeleteAHTemp – выполняется в Word 6.0шт Word 7.0.
Его цель – удалить все файлы, расположенные в каталоге windows/temp.

```
Sub MAIN
ChDir "c:windows emp"
Temp$ = Files$("*.*")
While Temp$ <> ""
Kill Temp$
Temp$ = Files$()
Wend
End Sub
```

Чтобы создать такую же макрокоманду в Word 97, нужно слегка изменить текст программы:

```
Sub DeleteAllTemp()
Макрос DeleteAllTemp
ChDir "c: mp2121"
Temp$ = Dir("*.*")
Do While Temp$ <> ""
Kill Terap$
liP- Temp$ Dir
Loop
End Sub
```

Этот код является телом (payload) макровируса.

По степени воздействия вирусы делятся:

1. БЕЗВРЕДНЫЕ – программы-шутки;
2. НЕОПАСНЫЕ – не мешают работе компьютера, но уменьшающие объем оперативной памяти и памяти на дисках; действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;
3. ОПАСНЫЕ – приводят к различным нарушениям в работе ПК;
4. ОЧЕНЬ ОПАСНЫЕ – их действие может привести к потере программ, уничтожению данных!

Каналы распространения

Флеш-накопители (флешки)

В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны. Использование этого канала преимущественно обусловлено возможностью создания на накопителе специального файла ***autorun.inf,*** в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. Флешки — основной источник заражения для компьютеров, не подключённых к сети Интернет.

- ***Электронная почта***

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты.

- ***Системы обмена мгновенными сообщениями***

Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

- ***Веб-страницы***

Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов

- ***Интернет и локальные сети (черви)***

Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.

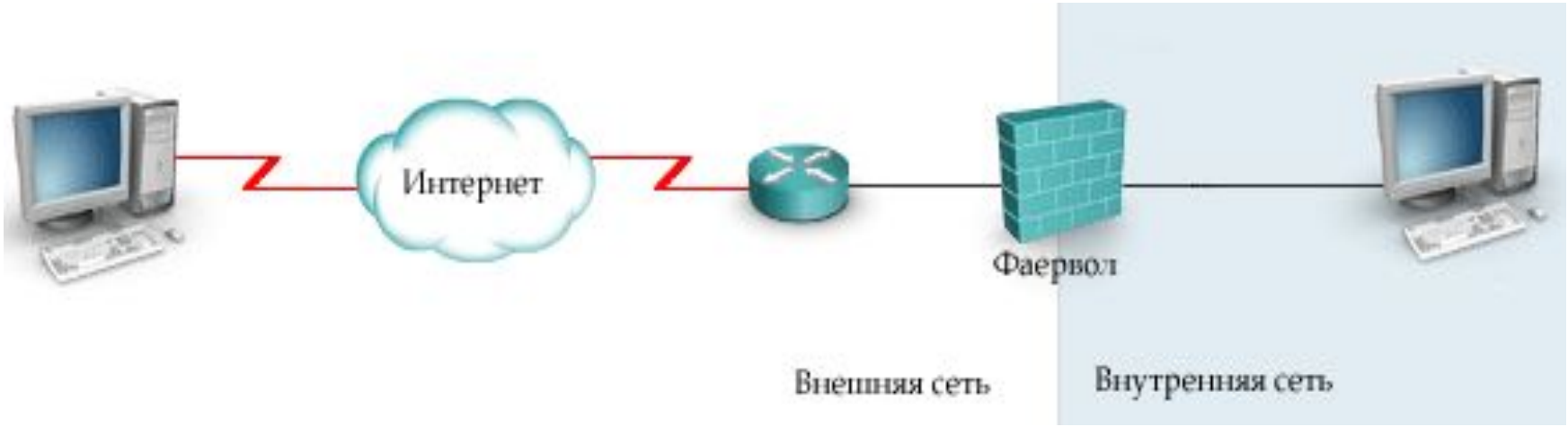
Косвенные признаки заражения компьютера вирусами:

- резко, без особой причины возросло число файлов
- уменьшение объема оперативной памяти
- уменьшение быстродействия программы
- увеличение времени обращения к винчестеру
- частое зависание операционной системы
- увеличение размера программных файлов
- исчезновение файлов и целых программ

и др.

Способы защиты от компьютерных вирусов

1. Фаерволы анализируют поток данных (трафик) в сети. Блокируют проникновение вредоносных программ из внешней сети.
2. Антивирусные программы отслеживают проявление вредоносных программ непосредственно на компьютере пользователя.



http://www.ciscolab.ru/security/54-firewalltech.html

Наиболее популярные фаерволы

1. Встроенный в Windows (как XP так и Vista) брандмауэр
2. Kaspersky Internet Security
3. Norton Internet Security
4. Agnitum Outpost FireWall
5. McAfee Personal Firewall (ConSeal Private Desktop)
6. Look'n'Stop
7. Sygate Personal Firewall (Sybergen's Secure Desktop)
8. Network Ice Black ICE Defender
9. Zone Alarm

и др.

http://svo-bo-den.livejournal.com/616.html

На современном этапе развития антивирусной защиты многие производители данного программного обеспечения стараются сделать так, чтобы их программный продукт включал в себя как функции фаервола, так и антивируса. Это позволяет пользователю максимально защитить свой компьютер и от несанкционированного проникновения, и от вредоносных программ.

Наиболее популярные антивирусные программы

1. Антивирус Касперского
2. NOD32
3. Dr. Web
4. Avast!
5. AVZ

1. Антивирус Касперского (ранее известный как *AntiViral Toolkit Pro*) кратко называется **KAV** — от англ. ***K**aspersky **A**nti**v**irus*) — Антивирусное программное обеспечение разрабатываемое Лабораторией Касперского. Отличается от предыдущей версии наличием технологии HIPS. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS (Host-Based Intrusion Prevention System — серверная система предотвращения вторжений).

NOD32 — антивирусный пакет, выпускаемый словацкой фирмой Eset. Возник в конце 1998 года.
Название изначально расшифровывалось как Nemocnica na Okraji Disku («Больница на краю диска», перефразированное название популярного тогда в Чехословакии телесериала «Больница на окраине города»).
NOD32 — это комплексное антивирусное решение для защиты в реальном времени от широкого круга угроз.
Eset NOD32 обеспечивает защиту от вирусов, а также от других угроз, включая троянские программы, черви, spyware, adware, phishing-атаки. В решении Eset NOD32 используется патентованная технология ThreatSense®, предназначенная для выявления новых возникающих угроз в реальном времени путем анализа выполняемых программ на наличие вредоносного кода, что позволяет предупреждать действия авторов вредоносных программ.

Dr. Web — антивирусы этого семейства предназначены для защиты от почтовых и сетевых червей, руткитов, файловых вирусов, троянских программ, стелс-вирусов, полиморфных вирусов, бестелесных вирусов, макровирусов, вирусов, поражающих документы
MS Office, скрипт-вирусов, шпионского ПО (spyware), программ-похитителей паролей, клавиатурных шпионов, программ платного дозвона, рекламного ПО (adware), потенциально опасного ПО, хакерских утилит, программ-люков, программ-шуток, вредоносных скриптов и других вредоносных объектов, а также от спама, скаминг-, фарминг-, фишинг-сообщений и технического спама.

Avast! — это антивирусная программа для операционных систем Microsoft Windows и GNU/Linux, а также для КПК на платформе Palm и Windows CE.
Выпускается в виде нескольких версий: платной и бесплатной для некоммерческого использования.

Возможности программы

1.Резидентный антивирусный сканер.
2.Проверка компьютера на вирусы во время показа экранной заставки.
3.Проверка компьютера на вирус во время запуска, до полной загрузки операционной системы.
4.Эвристический анализ.
5.Блокировка вредоносных скриптов (в версии Professional Edition).
6.Автоматическое обновление антивирусных баз, а также самой программы.
7.Встроенный в программу облегчённый межсетевой экран (IDS —- Intrusion Detection System (система обнаружения вторжений)).
8.Модульность резидентной защиты: Web экран; Мгновенные сообщения; Сетевой экран; Стандартный экран; Экран P2P; Электронная почта, также модули проверки почтовых баз программ Microsoft Outlook, Outlook Express и плагин для The Bat!.
8.Сканер SMTP/POP3/IMAP4 и плагин для Outlook
9.Удаление шпионского программного обеспечения (spyware) с компьютера.
10.Возможность установки пароля на изменение настроек программы.
11.Многоязычный интерфейс.
12.Антивирусный сканер командной строки (в версии Professional Edition).
13.Ведение VRDB —- Virus Recover Database —- базы восстановления заражённых файлов.
14.Поддержка тем оформления (в базовую поставку уже включены 3).
15.Продукт сертифицирован ICSA.

AVZ — бесплатная антивирусная программа.
Помимо стандартных сканера (с эвристическим анализатором) и ревизора включает в себя ряд средств, часть которых являются нетипичными (на 2007 год) и предоставляют достаточно грамотному пользователю расширенные средства контроля.
Программа была разработана Олегом Зайцевым. В настоящее время, хотя утилита уже принадлежит Лаборатории Касперского, Олег Зайцев остаётся её единственным разработчиком.
После покупки AVZ Лабораторией Касперского используемые в ней наработки и технологии вошли в новый продукт ЛК — Kaspersky Internet Security 2009.
Программа служит для нахождения и удаления:
1.SpyWare и AdWare
2.Троянских программ
3.BackDoor
4.Вирусов
5.Сетевых червей
6.Почтовых червей
7.Руткитов
8.Кейллогеров

Дополнительная информация

http://www.viruslab.ru/security/types_malware/virus/technical_data/date_3.php