Файловые вирусы, компьютерные вирусы

Ф.А.К. (F.A.Q., ЧАВО, ЧаВо, ЧаВО, ЧЗВ, FAQ)

«ФастФлюкс», FastFlux

Фишинг

Флейм

Флеш-память, флешка, flash-память

Флуд

«Фотошоп», Photoshop

**Файловые вирусы, компьютерные вирусы** — разновидность компьютерных программ, отличительной особенностью которых является способность к размножению (саморепликация).

*«Википедия»*[1]

*Файловый вирус* (англ. File Infector) — самореплицирующаяся вредоносная программа, внедряющая свой код в легитимный файл для выполнения вредоносного функционала или использования имен легитимных файлов.

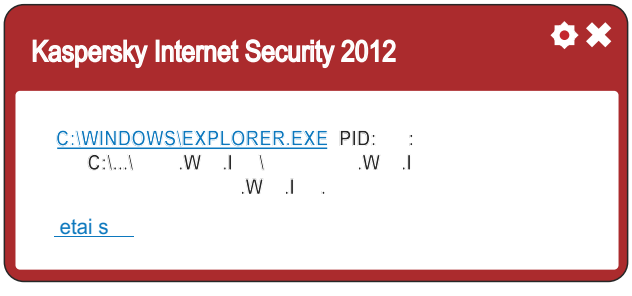
Вирусы-спутники, или вирусы-компаньоны, не внедряются в исполняемые программы. Такие вирусы используют особенность системы MS-DOS, позволяющую программному файлу с тем же названием, но другим расширением действовать с разными приоритетами. Под приоритетом понимают присваиваемый задаче, программе или операции признак, который определяет очередность их выполнения вычислительной системой. Большинство вирусов-спутников создают COM-файл, который обладает

[1] Адрес русскоязычной части «Википедии» — http://ru.wikipedia.org.

более высоким приоритетом, чем EXE-файлы с тем же самым названием. При запуске файла по имени (без указания расширения) будет запущен файл с расширением COM. Такие вирусы могут быть резидентными и маскировать файлы-двойники.

Некоторые файловые вирусы могут изменять или формировать свой код в процессе заражения очередного файла. Постоянное изменение кода программы не позволяет создать для них универсальную сигнатуру. Такое поведение программы называется полиморфизмом. В качестве методов защиты от вирусов такого рода применяются эвристический анализ (подробнее об этом читайте в статье «Эвристический анализ» данного выпуска) и эмуляция.

Файловые вирусы, постоянно находящиеся в оперативной памяти, могут фальсифицировать считываемую с диска информацию и передавать ложные данные запрашивающим программам.




**Kaspersky Internet Security обнаружил на компьютере файловый вирус**

*Егор Котельников и Давид Азнауров, участники проекта AV-School*


## ФАЙЛОВЫЕ ВИРУСЫ

Файловые вирусы — вид вредоносного программного обеспечения (ПО), отличительной чертой которого является способность к заражению исполняемых (PE) файлов.

Файловые вирусы ранее были популярны у вирусописателей, сейчас же осталось всего несколько распространенных файловых вирусов — Virut и Sality. Пример вредоносной активности одного из них мы рассмотрим позже.

Существует несколько методик заражения исполняемых файлов, которые используют файловые вирусы.

**Перезапись существующих файлов.** Это самый простой тип заражения, запись кода вируса вместо кода файла. Такой способ имеет два недостатка для вирусописателей:

- заражение легко может обнаружить даже пользователь, так как программы просто перестают работать;
- для лечения системы не нужно применять сложных процедур, а можно просто удалять файлы, поскольку исходный код этих файлов уже был уничтожен вирусом.

**Паразитический тип заражения.** При этом типе файл после заражения может работать так, как работал раньше, и пользователь может даже не замечать, что система заражена.