

Вирусы

Вирусы можно разделить на классы по следующим основным признакам:

- **Среда обитания**
- **Особенности алгоритма работы**
- **Разрушительные действия**

Среда обитания

- Файловые
- Загрузочные
- Макро-вирусы
- Скрипт-вирусы
- Смешанного типа

Особенности алгоритма работы

- Резидентные и нерезидентные
- Стелс-вирусы
- Полиморфик-вирусы

Разрушительные действия

- Безвредные
- Неопасные
- Опасные
- Очень опасные

Вирусы

```
graph TD; A[Вирусы] --> B[Среда обитания]; A --> C[Особенности алгоритма работы]; A --> D[Разрушительные действия]; B --> B1[Файловые]; B --> B2[Загрузочные]; B --> B3[Макровирусы]; B --> B4[Скрипт-вирусы]; B --> B5[Смешанного типа]; C --> C1[Резидентные]; C --> C2[Нерезидентные]; C --> C3[Стелс-вирусы]; C --> C4[Полиморфик-вирусы]; D --> D1[Безвредные]; D --> D2[Неопасные]; D --> D3[Опасные]; D --> D4[Очень опасные];
```

Среда обитания

Файловые
Загрузочные
Макровирусы
Скрипт-вирусы
Смешанного типа

Особенности алгоритма работы

Резидентные
Нерезидентные
Стелс-вирусы
Полиморфик-вирусы

Разрушительные действия

Безвредные
Неопасные
Опасные
Очень опасные

Файловые вирусы

- Файловые вирусы- это вирусы, которые внедряются в файлы операционной системы, активизируются при запуске зараженной программы и распространяются при копировании файлов с компьютера на компьютер.
- Этот тип вирусов самый старый и самый распространенный.
- Внедрение возможно во все операционные системы: DOS, Windows, OS/2, Unix

Классификация файловых вирусов

- Обычные
- Overwriting
- Паразитические
- Компаньон-вирусы
- Link-вирусы
- Файловые черви

Загрузочные вирусы

- Загрузочные (бутовые) вирусы – это вирусы, заражающие загрузочный boot-сектор. Активизируются при запуске операционной системы.

Макровирусы

- Макровирусы - это небольшие программы, написанные на языках (макроязыках), встроенных в различные системы документооборота (текстовые редакторы, электронные таблицы и т. д.)

Резидентные вирусы

- Вирусы, которые находятся в оперативной памяти, перехватывают обращения операционной системы к тем или иным объектам и внедряются в них. Активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу.

Нерезидентные вирусы

- Активны непродолжительное время – только в момент запуска зараженной программы. Файлы зараженные нерезидентными вирусами, значительно проще вылечить, при этом вирус не заразит их повторно.

Стелс-вирусы (невидимки)

- Компьютерные вирусы, которые помимо негативных действий, присущих вирусам, пытаются скрыть факт своего присутствия в зараженных объектах. Например, вирус перехватывает команды чтения зараженного сектора и подставляет вместо него незараженный оригинал.

Полиморфик-вирусы

- Вирусы, предпринимающие специальные меры для затруднения их поиска и анализа путем шифрования основного тела вируса и модификациями программы-расшифровщика. Полиморфность – это способность вируса изменять свой код при каждом новом запуске зараженной программы. Это ведет к отсутствию постоянных байтовых сигнатур у вируса.

Сигнатура вируса

- Сигнатура вируса – это последовательность байтов, имеющаяся в любом экземпляре вируса и только в нем. По сигнатурам вирусов создается антивирусная база.

Основные методы определения вирусов

- Сканирование сигнатур
- Проверка целостности
- Эвристический анализ
- Полиморфный анализ
- Анализатор макровирусов

Сканирование сигнатур

- Метод представляет собой идентификацию вирусов по неизменным кодам (эталонам). Он опирается на базу, содержащую сигнатуры вирусов.
- Метод хорошо для поиска вирусов с неизменным кодом, но не справляется с полиморфными вирусами и вирусами-невидимками

Проверка целостности

- Метод основывается на сравнении «контрольной суммы» проверяемого файла и контрольной суммы этого же файла, хранящегося в некоторой базе. Несовпадение сумм свидетельствует о возможном заражении файла.
- Метод неэффективен для вирусов —невидимок.

Эвристический анализ

- Чтобы размножиться, вирус совершает действия: копирование в память, запись загрузочные сектора и пр. Эвристический анализатор содержит список таких действий, просматривает код программы и определяет, что она делает.

Полиморфный анализ

- Использует технологию эмуляции процессора для того, чтобы проанализировать исполняемый код вируса. Эмулятор как бы воспроизводит работу программы в некотором виртуальном пространстве или реконструирует её оригинальное содержимое и всегда способен прервать её выполнение, не давая ничего испортить.

Анализатор макровирусов

- Метод основан на поиске макроопределений в файлах офисных приложений и проверке их на наличие вирусов.

Типы антивирусных программ

- Сканеры
- CRC-сканеры (ревизоры)
- Мониторы (блокировщики)
- Иммунизаторы

Антивирусный сканер

- Программа, осуществляющая проверку файлов, секторов и системной памяти на наличие в них известных и новых (неизвестных сканеру) вирусов. Для поиска используется сигнатура вируса. В сканерах иногда используется алгоритм эвристического анализа.
- Достоинства сканеров – универсальность
- Недостатки- большие размеры антивирусных баз.

CRC – сканеры (ревизоры)

- Программы-ревизоры, осуществляющие контроль над всеми изменениями, которые происходят в файловой системе компьютера. Принцип работы основан на подсчете контрольных сумм. Используют анти-стелс алгоритмы. Недостаток CRC-сканера: не способны поймать вирус в момент его появления в системе, т.е. в новом файле.

Мониторы (блокировщики)

- Резидентные программы, перехватывающие вирусоопасные ситуации и сообщающие об этом пользователю. К вирусоопасным ситуациям относятся: изменение и переименование исполняемых файлов (СОМ и ЕХЕ), запись в загрузочные сектора, форматирование винчестера, попытки программ остаться резидентными и пр. Достоинства мониторов: способность обнаружить и заблокировать вирус в момент его появления в системе. Недостатки: ложные срабатывания, проблемы при их установке и настройке.

Иммунизаторы

- Программы, предназначенные для защиты системы от поражения вирусом определенного типа. В память компьютера заносится программа, имитирующая копию вируса. Файлы на дисках модифицируются таким образом, что вирус принимает их за зараженные. Вирус натывается на них и считает, что система уже заражена.

Сигнатура вируса

```
00000000: EB 3C 90 4D 53 44 4F 53 - 35 2E 30 00 02 01 01 00 ы<PMSDOS6.0.000.
00000010: 02 E0 00 60 09 F9 07 00 - 0F 00 02 00 00 00 00 00 0p.'0'.*.0.....
00000020: 00 00 00 00 00 00 29 E4 - 1B 00 00 00 00 00 00 00 .....>φ+.....
00000030: 00 00 00 00 00 00 46 41 - 54 31 32 20 20 20 FA 33 .....FAT12 -3
00000040: C0 8E D0 BC 00 7C 16 07 - BB 78 00 36 C5 37 1E 56 10Mj.i.*qx.6+7AU
00000050: 16 53 BF 3E 7C B9 0B 00 - FC F3 A4 06 1F C6 45 FE _S1>:|δ.№ед#|EИ
00000060: 0F 8B 0E 18 7C 88 4D F9 - 89 47 02 C7 07 3E 7C FB *лл†:ИМ-ИГ0||->|J
00000070: CD 13 72 79 33 C0 39 06 - 13 7C 74 08 8B 0E 13 7C =!!y3 19#!!it0л!!
00000080: 89 0E 20 7C A0 10 7C F7 - 26 16 7C 03 06 1C 7C 13 0л ia!|y&_!#*!!
00000090: 16 1E 7C 03 06 0E 7C 83 - D2 00 A3 50 7C 89 16 52 _▲!#*л:Γπ.rP!И_Р
000000A0: 7C A3 49 7C 89 16 4B 7C - B8 20 00 F7 26 11 7C 8B irI!И_K!з .y&<л
000000B0: 1E 0B 7C 03 C3 48 F7 F3 - 01 06 49 7C 83 16 4B 7C ▲δ!#Иyε0#I!Γ_K!
000000C0: 00 BB 00 05 8B 16 52 7C - A1 50 7C E8 92 00 72 1D .л.эл_Р:И6P!шI.r+
000000D0: B0 01 E8 AC 00 72 16 8B - FB B9 0B 00 BE E6 7D F3 0шм.r_лJ|δ.Јu)ε
000000E0: A6 75 0A 8D 7F 20 B9 0B - 00 F3 A6 74 18 BE 9E 7D му0!Δ |δ.εxt†!0)
000000F0: E8 5F 00 33 C0 CD 16 5E - 1F 8F 04 8F 44 02 CD 19 ш_3!_~^#л#И0=1
00000100: 58 58 58 EB E8 8B 47 1A - 48 48 8A 1E 0D 7C 32 FF XXXмшлG→HKKΔP12
00000110: F7 E3 03 06 49 7C 13 16 - 4B 7C BB 00 07 B9 03 00 yy#*I!!!_K!л. #|!#
00000120: 50 52 51 E8 3A 00 72 D8 - B0 01 E8 54 00 59 5A 58 PR ш.:r!@шI.YZX
00000130: 72 BB 05 01 00 83 D2 00 - 03 1E 0B 7C E2 E2 8A 2E rл@.Γπ.#▲δ:ттK.
00000140: 15 7C 8A 16 24 7C 8B 1E - 49 7C A1 4B 7C EA 00 00 S!K_!$!лΔI!6K!b..
00000150: 70 00 AC 0A C0 74 29 B4 - 0E BB 07 00 CD 10 EB F2 p.м0!t>|л!*.→м€
00000160: 3B 16 18 7C 73 19 F7 36 - 18 7C FE C2 88 16 4F 7C ;_†is!y6†!#γИ_0!
00000170: 33 D2 F7 36 1A 7C 88 16 - 25 7C A3 4D 7C F8 C3 F9 3пy6→!И_×!rM!°|_
00000180: C3 B4 02 8B 16 4D 7C B1 - 06 D2 E6 0A 36 4F 7C 8B |!0л_М:|#пш060л
00000190: CA 86 E9 8A 16 24 7C 8A - 36 25 7C CD 13 C3 0D 0A 4шшK_!$!K6%!:=!!J0
000001A0: 4E 6F 6E 2D 53 79 73 74 - 65 6D 20 64 69 73 6B 20 Non-System disk
000001B0: 6F 72 20 64 69 73 6B 20 - 65 72 72 6F 72 0D 0A 52 or disk errorJ0R
000001C0: 65 70 6C 61 63 65 20 61 - 6E 64 20 70 72 65 73 73 eplace and press
000001D0: 20 61 6E 79 20 6B 65 79 - 20 77 68 65 6E 20 72 65 any key when re
000001E0: 61 64 79 0D 0A 00 49 4F - 20 20 20 20 20 20 53 59 adyJ0.IO
000001F0: 53 4D 53 44 4F 53 20 20 - 20 53 59 53 00 00 55 AA SMSDOS SYS..UK
```