УДК 004.49
ББК 32.973-018.2
К49

Климентьев К. Е.
К49 Компьютерные вирусы и антивирусы: взгляд программиста. – М.: ДМК Пресс, 2018. – 656 с.: ил.

ISBN 978-5-97060-576-9

Книга представляет собой курс компьютерной вирусологии, посвященный подробному рассмотрению феномена саморазмножающихся программ. Содержит неформальное и формальное введение в проблему компьютерных вирусов, описание принципов их работы, многочисленные примеры кода, методики обнаружения и удаления, а также лежащие в основе этих методик математические модели. Рассматривает все наиболее широко распространенные в прошлом и настоящем типы вирусов. Ориентирована на самую широкую аудиторию, но прежде всего на студентов и программистов – будущих и действующих специалистов в области защиты информации и разработки системного и прикладного программного обеспечения. Также может быть полезна и интересна «рядовым» пользователям, интересующимся проблемой компьютерных вирусов.

УДК 004.49
ББК 32.973-018.2

ISBN 978-5-97060-576-9

Содержание

Введение 12

ГЛАВА 1 ❖
Общие сведения о компьютерных вирусах 15

1.1. Что такое «компьютерный вирус» 15
1.2. Несколько исторических замечаний 17
1.3. Какие бывают вирусы 24
1.3.1. Классификация по способу использования ресурсов 25
1.3.2. Классификация по типу заражаемых объектов 25
1.3.3. Классификация по принципам активации 25
1.3.4. Классификация по способу организации программного кода 26
1.3.5. Классификация вирусов-червей 27
1.3.6. Прочие классификации 27
1.4. О «вредности» и «полезности» вирусов 28
1.5. О названиях компьютерных вирусов 31
1.6. Кто и зачем пишет вирусы 35
1.6.1. «Самоутверждающиеся» 36
1.6.2. «Честолюбцы» 36
1.6.3. «Игроки» 39
1.6.4. «Хулиганы и вандалы» 40
1.6.5. «Корыстолюбцы» 40
1.6.6. «Фемида» в борьбе с компьютерными вирусами 42
1.7. Общие сведения о способах борьбы с компьютерными вирусами 45

ГЛАВА 2 ❖
Загрузочные вирусы 49

2.1. Техническая информация 49
2.1.1. Загрузка с дискеты 53
2.1.2. Загрузка с винчестера 56
2.2. Как устроены загрузочные вирусы 58
2.2.1. Как загрузочные вирусы получают управление 58
2.2.2. Как загрузочные вирусы заражают свои жертвы 59
2.2.3. Как вирусы остаются резидентно в памяти 60
2.2.4. Как заподозрить и «изловить» загрузочный вирус 60
2.3. Охотимся за загрузочным вирусом 62
2.3.1. Анализ вирусного кода 62
2.3.2. Разработка антивируса 66

2.4. Редко встречающиеся особенности 70
2.4.1. Зашифрованные вирусы 70
2.4.2. Вирусы, не сохраняющие оригинальных загрузчиков 72
2.4.3. Механизмы противодействия удалению вирусов 74
2.4.4. Проявления загрузочных вирусов 77
2.4.5. Загрузочные вирусы и Windows 79
2.4.6. Буткиты 82
2.5. Советы по борьбе с загрузочными вирусами 85
2.5.1. Методы защиты дисков от заражения 86
2.5.2. Удаление загрузочных вирусов и буткитов «вручную» 87

ГЛАВА 3 ❖
Файловые вирусы в MS-DOS 89

3.1. Вирусы-«спутники» 89
3.2. «Оверлейные» вирусы 94
3.3. Вирусы, заражающие COM-программы 98
3.3.1. Внедрение в файл «жертвы» 98
3.3.2. Возврат управления «жертве» 102
3.4. Вирусы, заражающие EXE-программы 105
3.4.1. «Стандартный» метод заражения 107
3.4.2. Заражение в середину файла 109
3.4.3. Заражение в начало файла 110
3.5. Нерезидентные вирусы 111
3.5.1. Метод предопределенного местоположения файлов 112
3.5.2. Метод поиска в текущем каталоге 113
3.5.3. Метод рекурсивного обхода дерева каталогов 118
3.5.4. Метод поиска по «тропе» 119
3.6. Резидентные вирусы 122
3.6.1. Схема распределения памяти в MS-DOS 122
3.6.2. Способы выделения вирусом фрагмента памяти 126
3.6.3. Обработка прерываний 130
3.6.3.1. Перехват запуска программы 131
3.6.3.2. Перехват файловых операций 134
3.6.3.3. Перехват операций с каталогами 136
3.7. Вирусы-«невидимки» 137
3.7.1. «Психологическая» невидимость 140
3.7.2. Прямое обращение к системе 143
3.7.2.1. Метод предопределенных адресов 144
3.7.2.2. Метод трассировки прерывания 145
3.7.2.3. Прочие методы 149
3.7.3. Использование SFT 151

3.8. Зашифрованные и полиморфные вирусы 154
3.8.1. Зашифрованные и полиморфные вирусы для MS-DOS 155
3.8.2. Полиморфные технологии 168
3.9. Необычные файловые вирусы для MS-DOS 170
3.9.1. «Не-вирус» Eicar 171
3.9.2. «Двуполый» вирус 172
3.9.3. Файлово-загрузочные вирусы 173
3.9.4. Вирусы-«драйверы» 174
3.9.5. Вирусы с «неизвестной» точкой входа 175
3.9.6. Самый маленький вирус 176
3.10. Подробный пример обнаружения, анализа и удаления 179
3.10.1. Способы обнаружения и выделения вируса в чистом виде 179
3.10.2. Анализ вирусного кода 180
3.10.3. Пишем антивирус 183
3.11. MS-DOS-вирусы в эпоху Windows 184

ГЛАВА 4 ❖
Файловые вирусы в Windows 186

4.1. Системная организация Windows 186
4.1.1. Особенности адресации 187
4.1.1.1. Сегментная организация адресного пространства 188
4.1.1.2. Страничная организация адресного пространства 191
4.1.2. Механизмы защиты памяти 192
4.1.3. Обработка прерываний и исключений 193
4.1.4. Механизмы поддержки многозадачности 198
4.1.5. Распределение оперативной памяти 199
4.1.6. Файловые системы 203
4.1.7. Запросы прикладных программ к операционной системе 204
4.1.7.1. Системные сервисы в MS-DOS 204
4.1.7.2. Системные сервисы в Windows 3.X 205
4.1.7.3. Системные сервисы в Windows 9X 207
4.1.7.4. Системные сервисы в Windows NT 208
4.1.8. Конфигурирование операционной системы 209
4.1.8.1. Конфигурационные файлы Windows 3.X 209
4.1.8.2. Конфигурационные файлы и структуры Windows 9X 210
4.1.8.3. Конфигурационные файлы и структуры Windows NT 212
4.1.9. Исполняемые файлы Windows 213
4.2. Вирусы для 16-разрядных версий Windows 216
4.2.1. Формат файла NE-программы 217
4.2.1.1. Таблица описания сегментов 218
4.2.1.2. Таблица описания перемещаемых ссылок 219

4.2.1.3. Таблицы описания импорта 221
4.2.2. Организация вирусов для Windows 3X 221
4.2.3. Анализ конкретного вируса и разработка антивирусных процедур 225
4.3. Вирусы для 32-разрядных версий Windows 227
4.3.1. Формат файлов PE-программ 229
4.3.1.1. PE-программы на диске и в памяти 231
4.3.1.2. Таблица секций 234
4.3.1.3. Импорт объектов 236
4.3.1.4. Экспорт объектов 241
4.3.2. Где располагаются вирусы 243
4.3.2.1. Файловые «черви» 243
4.3.2.2. Вирусы-«спутники» 244
4.3.2.3. «Оверлейные» вирусы 245
4.3.2.4. Вирусы в расширенной последней секции 245
4.3.2.5. Вирусы в дополнительной секции 246
4.3.2.6. Вирусы, распределенные по секциям 247
4.3.2.7. Вирусы в файловых потоках NTFS 249
4.3.3. Как вирусы получают управление 250
4.3.3.1. Изменение адреса точки входа 250
4.3.3.2. Изменение кода в точке входа 251
4.3.3.3. Использование технологии EPO 251
4.3.4. Как вирусы обращаются к системным сервисам 252
4.3.4.1. Метод предопределенных адресов 253
4.3.4.2. Самостоятельный поиск адреса KERNEL32.DLL 258
4.3.4.3. Использование «нестандартных» сервисов 260
4.3.5. Нерезидентные вирусы 264
4.3.6. «Резиденты» 3-го кольца защиты 265
4.3.6.1. Вирусы – автономные процессы 266
4.3.6.2. «Полурезидентные» вирусы 266
4.3.6.3. Вирусы, заражающие стандартные компоненты Windows 266
4.3.6.4. Вирусы, анализирующие список процессов 268
4.3.7. «Резиденты» 0-го кольца защиты 269
4.3.7.1. Переход в 0-е кольцо защиты методом создания собственных шлюзов 269
4.3.7.2. Переход в 0-е кольцо защиты подменой обработчика исключений 270
4.3.7.3. Инсталляция в неиспользуемые буферы VMM 272
4.3.7.4. Инсталляция в динамически выделяемую системную память 273

4.3.7.5. Встраивание в файловую систему 274
4.3.8. Вирусы – виртуальные драйверы 278
4.3.8.1. VxD-вирусы 279
4.3.8.2. SYS-вирусы и WDM-вирусы 282
4.3.9. «Невидимость» Windows-вирусов 286
4.3.9.1. Маскировка присутствия в файле 287
4.3.9.2. Маскировка присутствия в памяти 289
4.3.9.3. Маскировка ключей Реестра 296
4.3.10. Полиморфные вирусы в Windows 296
4.3.11. Вирусы и подсистема безопасности Windows 301
4.4. Пример анализа и нейтрализации конкретного вируса 305
4.4.1. Первичный анализ зараженных программ 305
4.4.2. Анализ кода 307
4.4.3. Алгоритм поиска и лечения 307
4.4.4. Дополнительные замечания 308

ГЛАВА 5 ❖
Макровирусы 310

5.1. Вирусы в MS Word 310
5.1.1. Общие сведения о макросах 313
5.1.2. Вирусы на языке WordBasic 315
5.1.2.1. Проблема «локализации» 322
5.1.2.2. Активация без «автоматических макросов» 323
5.1.2.3. Копирование макросов без «MacroCopy» 324
5.1.2.4. Запуск бинарного кода 324
5.1.2.5. Обеспечение «невидимости» 325
5.1.3. Вирусы на языке VBA 326
5.1.4. О проявлениях макровирусов 333
5.1.5. Простейшие приемы защиты от макровирусов 336
5.1.5.1. Манипуляции с «NORMAL.DOT» 336
5.1.5.2. Удаление вируса средствами «Организатора» 336
5.1.5.3. Антивирусные макросы 337
5.1.5.4. Встроенная «защита» MS Word 339
5.2. Вирусы в других приложениях MS Office 342
5.2.1. Макровирусы в MS Excel 342
5.2.2. «Многоплатформенные» макровирусы 344
5.3. Полиморфные макровирусы 346
5.4. Прямой доступ к макросам 349
5.4.1. Формат структурированного хранилища 350
5.4.2. «Правильный» доступ к структурированному хранилищу 357
5.4.3. Макросы в Word-документе 358

5.4.3.1. Макросы на языке WordBasic 358
5.4.3.2. Макросы на языке VBA 361
5.4.3.3. Вид и расположение VBA-макросов 362
5.4.3.4. Поиск VBA-макросов 363
5.4.3.5. Распаковка VBA-текста макросов 364
5.4.3.6. Удаление VBA-макросов 366
5.5. Пример анализа и удаления конкретного макровируса 367
5.5.1. Получение и анализ исходного текста 367
5.5.2. Распознавание и удаление макровируса 370

ГЛАВА 6 ❖
Сетевые и почтовые вирусы и черви 371

6.1. Краткая история сетей и сетевой «заразы» 371
6.2. Архитектура современных сетей 375
6.2.1. Топология сетей 375
6.2.2. Семиуровневая модель ISO OSI 377
6.2.3. IP-адресация 378
6.2.4. Символические имена доменов 380
6.2.5. Клиенты и серверы. Порты 382
6.2.6. Сетевое программирование. Интерфейс сокетов 384
6.3. Типовые структура и поведение программы-червя 386
6.4. Как вирусы и черви распространяются 391
6.4.1. Черви в локальных сетях 392
6.4.2. Почтовые вирусы 398
6.4.2.1. Первые почтовые вирусы. Интерфейс MAPI 401
6.4.2.2. Прямая работа с почтовыми серверами 408
6.4.3. «Интернет»-черви 414
6.5. Как черви проникают в компьютер 417
6.5.1. «Социальная инженерия» 423
6.5.2. Ошибки при обработке почтовых вложений 427
6.5.3. Ошибки в процессах SVCHOST и LSASS 429
6.5.4. Прочие «дыры» 435
6.5.5. Брандмауэры 438
6.6. Как черви заражают компьютер 442
6.7. Пример обнаружения, исследования и удаления червя 445
6.7.1. Проявления червя 445
6.7.2. Анализ алгоритма работы 448
6.7.2.1. Установка в памяти 448
6.7.2.2. Борьба с антивирусами 449
6.7.2.3. Модификация Реестра 451
6.7.2.4. Поиск адресов 451

6.7.2.5. Распространение по электронной почте 451
6.7.3. Методы удаления 452
6.8. Современные сетевые вирусы и черви....454
6.8.1. Модульное построение 456
6.8.2. Множественность способов распространения 457
6.8.3. Борьба червей с антивирусами 458
6.8.4. Управляемость. Ботнеты....458

ГЛАВА 7 ❖
Философские и математические аспекты 461

7.1. Строгое определение вируса 461
7.1.1. Модели Ф. Коэна 462
7.1.2. Модель Л. Адлемана....469
7.1.3. «Французская» модель 472
7.1.4. Прочие формальные модели 475
7.1.4.1. Модель китайских авторов Z. Zuo и M. Zhou 475
7.1.4.2. Векторная модель Д. Зегжды 475
7.1.4.3. Модели на основе абстрактных «вычислителей» 476
7.2. «Экзотические» вирусы....478
7.2.1. Мифические вирусы 479
7.2.2. Batch-вирусы 482
7.2.3. Вирусы в исходных текстах 486
7.2.4. Графические вирусы 490
7.2.5. Вирусы в иных операционных системах....492
7.2.5.1. Вирусы в UNIX-подобных системах 492
7.2.5.2. Вирусы для мобильных телефонов....501
7.2.6. Прочая вирусная «экзотика» 506
7.3. Распространение вирусов....508
7.3.1. Эпидемии сетевых червей 508
7.3.1.1. Простая SI-модель экспоненциального размножения 510
7.3.1.2. SI-модель размножения в условиях ограниченности ресурсов 514
7.3.1.3. SIS-модель примитивного противодействия 516
7.3.1.4. SIR-модель квалифицированной борьбы 517
7.3.1.5. Прочие модели эпидемий 519
7.3.1.6. Моделирование мер пассивного противодействия 521
7.3.1.7. Моделирование «контрчервя» 522
7.3.2. Эпидемии почтовых червей, файловых и загрузочных вирусов 527
7.3.3. Эпидемии мобильных червей 530
7.4. Обнаружение вирусов 532

7.4.1. Анализ косвенных признаков 533
7.4.2. Простые сигнатуры 535
7.4.3. Контрольные суммы 541
7.4.4. Вопросы эффективности 544
7.4.4.1. Выбор файловых позиций 545
7.4.4.2. Фильтр Блума 547
7.4.4.3. Метод половинного деления 548
7.4.4.4. Разбиение на страницы 549
7.4.5. Использование сигнатур для детектирования полиморфиков 551
7.4.5.1. Аппаратная трассировка 552
7.4.5.2. Эмуляция программ 556
7.4.5.3. Противодействие эмуляции 560
7.4.5.4. «Глубина» трассировки и эмуляции 563
7.4.6. «Рентгеноскопия» полиморфных вирусов 564
7.4.7. Метаморфные вирусы и их детектирование 567
7.4.7.1. Этап «выделения и сбора характеристик» 569
7.4.7.2. Этап «обработки и анализа» 571
7.4.8. Анализ статистических закономерностей 578
7.4.9. Эвристические методы детектирования вирусов 580
7.4.9.1. Выделение характерных признаков 582
7.4.9.2. Логические методы 586
7.4.9.3. Синтаксические методы 588
7.4.9.4. Методы на основе формулы Байеса 588
7.4.9.5. Методы, использующие искусственные нейронные сети 590
7.4.10. Концепция современного антивирусного детектора 592
7.5. Борьба с вирусами без использования антивирусов 596
7.5.1. Файловые «ревизоры» 596
7.5.2. Политики разграничения доступа 597
7.5.3. Криптографические методы 601
7.5.4. Гарвардская архитектура ЭВМ 604
7.6. Перспективы развития и использования компьютерных вирусов 605
7.6.1. Вирусы как «кибероружие» 606
7.6.2. Полезные применения вирусов 613

ЗАКЛЮЧЕНИЕ 623

Литература 625

ПРИЛОЖЕНИЕ ❖
Листинги вирусов и антивирусных процедур 630

1. Листинги компьютерных вирусов 630
1.1. Листинг загрузочного вируса Stoned.AntiExe 630
1.2. Листинг вируса Eddie, заражающего программы MS-DOS 634
1.3. Листинг вируса Win16.Wintiny.b, заражающего NE-программы 637
1.4. Листинг вируса Win32.Barum.1536, заражающего PE-программы 639
2. Исходные тексты антивирусных процедур 641
2.1. Процедуры рекурсивного сканирования каталогов 641
2.2. Процедуры детектирования и лечения вируса Boot.AntiExe 642
2.3. Процедуры детектирования и лечения вируса Eddie.651.a 642
2.4. Процедуры детектирования и лечения вируса Win.Wintiny.b 644
2.5. Процедуры детектирования и лечения вируса Win32.Barum.1536 645
2.6. Процедуры детектирования и лечения вирусов Macro.Word.Wazzu.gw и Macro.Word97.Wazzu.gw 646
2.7. Скрипт антивируса AVZ для детектирования и лечения почтового червя E-Worm.Avron.a 651

Предметный указатель 653