Оглавление

Внимание! ... 12

Об авторах ... 13
О техническом редакторе ... 13
О соавторах ... 14

Предисловие ... 15

Благодарности ... 18
Отдельное спасибо ... 18

Введение ... 19
В чем заключается анализ вредоносного ПО ... 20
Необходимая квалификация ... 20
Изучение на примерах ... 21
Структура книги ... 21

Глава 0. Анализ вредоносных программ для начинающих ... 24
Цель анализа вредоносных программ ... 24
Методики анализа вредоносного ПО ... 25
Типы вредоносного ПО ... 26
Общие правила анализа вредоносного ПО ... 28

Часть I. Базовый анализ

Глава 1. Основные статические методики ... 30
Сканирование антивирусом: первый шаг ... 30
Хеширование: отпечатки пальцев злоумышленника ... 31
Поиск строк ... 32
Упакованное и обфусцированное вредоносное ПО ... 34
Формат переносимых исполняемых файлов ... 36
Компонуемые библиотеки и функции ... 36
Статический анализ на практике ... 40
Заголовки и разделы PE-файла ... 43
Итоги главы ... 49

Глава 2. Анализ вредоносных программ в виртуальных машинах 52
Структура виртуальной машины 53
Запуск виртуальной машины для анализа вредоносного ПО 54
Использование виртуальной машины для анализа безопасности 57
Риски при использовании VMware для анализа безопасности 60
Запись/воспроизведение работы компьютера 60
Итоги главы 61

Глава 3. Основы динамического анализа 62
Песочницы: решение на скорую руку 62
Запуск вредоносных программ 65
Мониторинг с помощью Process Monitor 66
Просмотр процессов с помощью Process Explorer 70
Сравнение снимков реестра с помощью Regshot 74
Симуляция сети 75
Перехват пакетов с помощью Wireshark 78
Использование INetSim 79
Применение основных инструментов для динамического анализа 81
Итоги главы 84

Часть II. Продвинутый статический анализ

Глава 4. Ускоренный курс по ассемблеру для архитектуры x86 88
Уровни абстракции 88
Обратное проектирование 90
Архитектура x86 91
Итоги главы 110

Глава 5. IDA Pro 111
Загрузка исполняемого файла 112
Интерфейс IDA Pro 113
Использование перекрестных ссылок 119
Анализ функций 121
Схематическое представление 122
Повышение эффективности дизассемблирования 124
Плагины к IDA Pro 129
Итоги главы 132

Глава 6. Распознавание конструкций языка C в ассемблере 135
Переменные: локальные и глобальные 136
Дизассемблирование арифметических операций 138
Распознавание выражений if 139
Распознавание циклов 142
Соглашения, касающиеся вызова функций 144
Анализ выражений switch 148
Дизассемблирование массивов 152
Распознавание структур 153
Анализ обхода связного списка 156
Итоги главы 158

Глава 7. Анализ вредоносных программ для Windows 160
Windows API 160
Реестр Windows 164
API для работы с сетью 169
Отслеживание запущенной вредоносной программы 171
Сравнение режимов ядра и пользователя 185
Native API 186
Итоги главы 188

Часть III. Продвинутый динамический анализ

Глава 8. Отладка 192
Сравнение отладки на уровне исходного и дизассемблированного кода 192
Отладка на уровне ядра и пользователя 193
Использование отладчика 193
Исключения 201
Управление выполнением с помощью отладчика 202
Изменение хода выполнения программы на практике 203
Итоги главы 204

Глава 9. OllyDbg 205
Загрузка вредоносного ПО 205
Пользовательский интерфейс OllyDbg 207
Карта памяти 208
Просмотр потоков и стеков 211
Выполнение кода 212
Точки останова 214
Загрузка динамических библиотек 218
Трассировка 219
Обработка исключений 222
Редактирование кода 222
Анализ кода командной оболочки 224
Вспомогательные возможности 224
Подключаемые модули 225
Отладка с использованием скриптов 228
Итоги главы 229

Глава 10. Отладка ядра с помощью WinDbg 232
Драйверы и код ядра 232
Подготовка к отладке ядра 234
Использование WinDbg 237
Отладочные символы Microsoft 239
Отладка ядра на практике 242
Руткиты 248
Загрузка драйверов 253
Особенности ядра в Windows Vista, Windows 7 и 64-битных версиях 254
Итоги главы 255

Часть IV. Возможности вредоносного ПО

Глава 11. Поведение вредоносных программ ... 258
Программы для загрузки и запуска ПО ... 258
Бэкдоры ... 258
Похищение учетных данных ... 262
Механизм постоянного присутствия ... 269
Повышение привилегий ... 274
Заметая следы: руткиты, работающие в пользовательском режиме ... 276
Итоги главы ... 279

Глава 12. Скрытый запуск вредоносного ПО ... 282
Загрузчики ... 282
Внедрение в процесс ... 283
Подмена процесса ... 286
Внедрение перехватчиков ... 288
Detours ... 291
Внедрение асинхронных процедур ... 292
Итоги главы ... 294

Глава 13. Кодирование данных ... 297
Зачем нужно анализировать алгоритмы кодирования ... 297
Простые шифры ... 298
Распространенные криптографические алгоритмы ... 309
Нестандартное кодирование ... 314
Декодирование ... 318
Итоги главы ... 324

Глава 14. Сетевые сигнатуры, нацеленные на вредоносное ПО ... 327
Сетевые контрмеры ... 327
Безопасное расследование вредоносной деятельности в Интернете ... 330
Контрмеры, основанные на сетевом трафике ... 332
Углубленный анализ ... 334
Сочетание динамических и статических методик анализа ... 338
Понимание психологии злоумышленника ... 353
Итоги главы ... 354

Часть V. Противодействие обратному проектированию

Глава 15. Антидизассемблирование ... 358
Понимание антидизассемблирования ... 358
Искажение алгоритмов дизассемблирования ... 360
Методики антидизассемблирования ... 364
Скрытие управления потоком ... 371
Срыв анализа слоя стека ... 377
Итоги главы ... 379

Глава 16. Антиотладка 382
Обнаружение отладчика в Windows 382
Распознавание поведения отладчика 387
Искажение работы отладчика 390
Уязвимости отладчиков 395
Итоги главы 397

Глава 17. Методы противодействия виртуальным машинам 400
Признаки присутствия VMware 400
Уязвимые инструкции 404
Изменение настроек 411
Побег из виртуальной машины 412
Итоги главы 412

Глава 18. Упаковщики и распаковка 415
Анатомия упаковщика 415
Распознавание упакованных программ 419
Способы распаковки 420
Автоматизированная распаковка 420
Ручная распаковка 421
Советы и приемы для работы с распространенными упаковщиками 430
Анализ без полной распаковки 434
Упакованные DLL 435
Итоги главы 435

Часть VI. Специальные темы

Глава 19. Анализ кода командной оболочки 438
Загрузка кода командной оболочки для анализа 438
Позиционно-независимый код 439
Определение адреса выполнения 440
Поиск символов вручную 444
Окончательная версия программы Hello World 450
Кодировки кода командной оболочки 452
NOP-цепочки 454
Поиск кода командной оболочки 454
Итоги главы 456

Глава 20. Анализ кода на C++ 458
Объектно-ориентированное программирование 458
Обычные и виртуальные функции 463
Создание и уничтожение объектов 467
Итоги главы 468

Глава 21. Шестидесятичетырехбитные вредоносные программы 471
Какой смысл в 64-битном вредоносном ПО? 471
Особенности архитектуры x64 472
WOW64 477
Признаки вредоносного кода на платформе x64 478
Итоги главы 479

Приложения

Приложение А. Важные функции Windows 482

Приложение Б. Инструменты для анализа вредоносного ПО 491

Приложение В. Решения лабораторных работ 502

Работа 1.1 502
Работа 1.2 504
Работа 1.3 505
Работа 1.4 506
Работа 3.1 507
Работа 3.2 511
Работа 3.3 516
Работа 3.4 518
Работа 5.1 520
Работа 6.1 528
Работа 6.2 530
Работа 6.3 534
Работа 6.4 538
Работа 7.1.....541
Работа 7.2.....545
Работа 7.3.....547
Работа 9.1 558
Работа 9.2 568
Работа 9.3 574
Работа 10.1.....578
Работа 10.2.....583
Работа 10.3.....590
Работа 11.1.....596
Работа 11.2.....601
Работа 11.3.....611
Работа 12.1.....617
Работа 12.2.....621
Работа 12.3.....629
Работа 12.4.....631
Работа 13.1.....639
Работа 13.2.....644
Работа 13.3.....650
Работа 14.1.....660
Работа 14.2.....666
Работа 14.3.....671
Работа 15.1.....679
Работа 15.2.....680
Работа 15.3.....686
Работа 16.1.....689
Работа 16.2.....695
Работа 16.3.....700
Работа 17.1.....705
Работа 17.2.....708
Работа 17.3.....713
Работа 18.1.....720
Работа 18.2.....721
Работа 18.3.....722
Работа 18.4.....725
Работа 18.5.....727
Работа 19.1.....731
Работа 19.2.....734
Работа 19.3.....739
Работа 20.1.....748
Работа 20.2.....749
Работа 20.3.....753
Работа 21.1.....759
Работа 21.2.....764