

# СОДЕРЖАНИЕ

<b>Предисловие .....</b>	<b>5</b>
<b>Глава 1. Закоулки истории .....</b>	<b>9</b>
Первые ласточки.....	9
Эпоха вирусов.....	12
Новое время .....	16
Наши дни.....	19
<b>Глава 2. Сравнительная вирусология .....</b>	<b>23</b>
Классификация по типу операционной системы .....	23
Классификация по вредоносным функциям.....	27
Вирусы.....	27
Черви.....	29
Троянские программы (троянцы) .....	30
Бэкдоры .....	31
Буткиты .....	32
Руткиты.....	33
Биоскиты .....	34
Боты .....	35
Шпионы (Spyware) .....	36
Нежелательные и нерекомендуемые приложения.....	36
Классификация по степени опасности .....	37
<b>Глава 3. Внимание, опасность! .....</b>	<b>41</b>
Троянцы-блокировщики (винлокеры) .....	42
Троянцы-шифровальщики (энкодеры).....	43
Банковские троянцы.....	45
Веб-инжекторы.....	50
Троянцы-загрузчики .....	54
Майнеры .....	55
Фишинг .....	55
Рекламные троянцы .....	57
Узкоспециализированные вредоносные программы .....	58
<b>Глава 4. Ботнеты.....</b>	<b>61</b>
История вопроса.....	61
Архитектура ботнетов.....	63
Простые ботнеты .....	63
Ботнеты, использующие DGS .....	64
P2P-ботнеты .....	66
Ботнеты смешанного типа .....	68
Ботнеты с использованием TOR и «облаков».....	70
Нетрадиционные схемы .....	71
Командная система ботнетов.....	74
Методика перехвата управления ботнетами (sinkhole) .....	75

<b>Глава 5. Технологии проникновения .....</b>	<b>79</b>
Сменные носители информации .....	79
Вредоносные почтовые рассылки.....	80
Уязвимости.....	82
Загрузчики .....	85
Социальная инженерия .....	86
Поддельные сайты .....	89
Бесплатные и взломанные приложения.....	90
Системы TDS .....	91
Ресурсы «для взрослых».....	91
Взломанные сайты .....	92
Атаки типа MITM .....	93
<b>Глава 6. Технологии заражения.....</b>	<b>95</b>
Дроппер .....	95
Инфектор .....	96
Инжектор .....	96
Лоадер.....	96
Процесс заражения .....	96
Инфицирование файловых объектов .....	98
Методы обеспечения автоматического запуска .....	100
Инжекты .....	101
Перехват вызовов функций .....	102
<b>Глава 7. Кто пишет и распространяет вирусы? .....</b>	<b>107</b>
Кто такие хакеры? .....	107
Категории компьютерных злоумышленников.....	109
На чем зарабатывает компьютерный андеграунд? .....	110
Так кто все-таки распространяет вирусы?.....	114
Как вычислить вирусописателя? .....	115
<b>Глава 8. Методы борьбы.....</b>	<b>121</b>
Немного истории.....	121
Компоненты антивирусной программы.....	123
Сигнатурное детектирование .....	124
Поведенческий анализ.....	125
Эвристический анализ .....	126
Проактивная защита (HIPS).....	127
Методики противодействия антивирусам.....	127
Переупаковка.....	127
Обfuscация.....	128
Антиотладка .....	128
Как защититься?.....	130
<b>Глоссарий .....</b>	<b>132</b>