

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ	5
ГЛАВА 1. ЗАКОУЛКИ ИСТОРИИ	9
Первые ласточки	10
Эпоха вирусов	13
Новое время	18
Наши дни	22
ГЛАВА 2. СРАВНИТЕЛЬНАЯ ВИРУСОЛОГИЯ	27
Классификация по типу операционной системы.	28
Классификация по вредоносным функциям.	33
Вирусы	33
Черви	35
Троянские программы (трояны или троянцы).	37
Бэкдоры	38
Бугкиты	39
Руткиты	41
Биоскиты	42
Боты	42
Шпионы (Spyware).	44
Нежелательные и нерекомендуемые приложения	45
Классификация по степени опасности	46
ГЛАВА 3. ВНИМАНИЕ, ОПАСНОСТЬ!	49
Троянцы-блокировщики (вин-локеры).	51
Троянцы-шифровальщики (энкодеры)	53
Банковские троянцы	60
Веб-инъекты	65
Троянцы-загрузчики	70
Майнеры	71
Клиперы	72
Стилеры	73
Троянцы для любителей игр	73
Фишинг	78
Рекламные троянцы	80
Узкоспециализированные вредоносные программы.	81
ГЛАВА 4. МОБИЛЬНЫЕ ВРЕДОНОСНЫЕ ПРОГРАММЫ	83
Уязвимости в Android.	84
Мобильные банковские троянцы.	84
Первенцы	85
Как работают мобильные банкиры	87
Банкботы.	91
Криминальная индустрия.	92
Вредоносные программы для iOS	94

Немного теории	94
Шпионские игры	96
Технология MDM	98
Технология DRM	100

ГЛАВА 5. ВРЕДОНОСНЫЕ ПРОГРАММЫ

ДЛЯ «ИНТЕРНЕТА ВЕЩЕЙ» 103

Матчасть	105
Mirai	108
«Наследники» и модификации	111
HaJime	114
Взлом устройства	114
Исследование устройства	116
Инфектор	116
Основной модуль трояна	117
Ботнет	118
Цели и выводы	119

ГЛАВА 6. БОТНЕТЫ 120

История вопроса	121
Архитектура ботнетов	123
Простые ботнеты	123
Ботнеты, использующие DGS	124
P2P-ботнеты	126
Ботнеты смешанного типа	128
Ботнеты с использованием TOR и «облаков»	131
Нетрадиционные схемы	132
Командная система ботнетов	135
Методика перехвата управления ботнетами (sinkhole)	137

ГЛАВА 7. ТЕХНОЛОГИИ ПРОНИКНОВЕНИЯ 140

Сменные носители информации	141
Вредоносные почтовые рассылки	142
Уязвимости	144
Эксплойты	153
Загрузчики	158
Социальная инженерия	159
Поддельные сайты	164
Бесплатные и взломанные приложения	164
Системы TDS	165
Ресурсы «для взрослых»	166
Взломанные сайты	167
Атаки типа MITM	168

ГЛАВА 8. ТЕХНОЛОГИИ ЗАРАЖЕНИЯ	170
Дроппер171
Инфектор171
Инжектор172
Лоадер172
Процесс заражения.172
Инфицирование файловых объектов174
Методы обеспечения	
автоматического запуска176
Инжекты177
Перехват вызовов функций.179
ГЛАВА 9. КТО ПИШЕТ И РАСПРОСТРАНЯЕТ ВИРУСЫ?	183
Хакеры и киберпреступники.184
На чем зарабатывает	
компьютерный андеграунд?186
Так кто все-таки	
распространяет вирусы?191
Как вычислить вирусописателя?193
ГЛАВА 10. МЕТОДЫ БОРЬБЫ	199
Немного истории200
Как антивирусные компании	
пополняют базы?202
Компоненты антивирусной	
программы203
Сигнатурное детектирование205
Поведенческий анализ206
Эвристический анализ.207
Проактивная защита (HIPS)208
Методики противодействия	
антивирусам209
Переупаковка209
Обфускация210
Антиотладка.211
Заключение212
ГЛОССАРИЙ	213