



Валентин Холмогоров

PRO Вирусы



Версия 4.0

Автор идеи и научный редактор серии
С. Л. Деменок

НАУЧНО-ПОПУЛЯРНОЕ
ИЗДАТЕЛЬСТВО
«СТРСТ»

Санкт-Петербург. 2020

УДК 681.3.06(075)

ББК 32.973-01я2

X72

Холмогоров В.

X72 ПРО ВИРУСЫ. Издание четвертое, переработанное и дополненное / Валентин Холмогоров. — СПб.: Страта, 2020. — 224 с., ил.

ISBN 978-5-907314-12-2

Время энтузиастов-одиночек, создававших компьютерные вирусы на заре информационной эпохи, давно прошло: в наши дни разработкой и распространением вредоносных программ занимаются хорошо организованные преступные группировки, имеющие жесткую иерархию и напоминающие по своей структуре настоящие мафиозные кланы. Объем этого подпольного рынка составляет сотни миллионов долларов.

Книга рассказывает об истории возникновения и развития технологий компьютерных вирусов, их разновидностях, внутренней архитектуре, способах распространения и принципах действия. Книга позволит читателям познакомиться с таинственным теневым миром киберпреступности, представители которого ежедневно осуществляют атаки на компьютеры простых пользователей по всему миру.

Все права защищены. Никакая часть настоящей книги не может быть воспроизведена или передана в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование и запись на магнитный носитель, а также размещение в Интернете, если на то нет письменного разрешения владельцев.

All rights reserved. No parts of this publication can be reproduced, sold or transmitted by any means without permission of the publisher.

УДК 681.3.06(075)

ББК 32.973-01я2

ISBN 978-5-907314-12-2

© Холмогоров В., 2020, текст

© ООО «Страта», 2020

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
Буткиты	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 (винлокеры)	51
Троянцы-шифровальщики (энкодеры)	53
Банковские троянцы	60
Веб-инжекты	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 ВРЕДНОСНЫЕ 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 теории94
Шпионские игры.96
Технология MDM98
Технология DRM100

ГЛАВА 5. ВРЕДОНОСНЫЕ ПРОГРАММЫ

ДЛЯ «ИНТЕРНЕТА ВЕЩЕЙ» 103

Матчасть105
Mirai108
«Наследники» и модификации.111
Najime.114
Взлом устройства114
Исследование устройства116
Инфектор116
Основной модуль трояна117
Ботнет.118
Цели и выводы119

ГЛАВА 6. БОТНЕТЫ 120

История вопроса121
Архитектура ботнетов123
Простые ботнеты123
Ботнеты, использующие DGS.124
P2P-ботнеты.126
Ботнеты смешанного типа128
Ботнеты с использованием TOR и «облаков»131
Нетрадиционные схемы132
Командная система ботнетов135
Методика перехвата управления ботнетами (sinkhole).137

ГЛАВА 7. ТЕХНОЛОГИИ ПРОНИКНОВЕНИЯ 140

Сменные носители информации141
Вредоносные почтовые рассылки142
Уязвимости144
Эксплойты153
Загрузчики.158
Социальная инженерия159
Поддельные сайты164
Бесплатные и взломанные приложения164
Системы TDS165
Ресурсы «для взрослых».166
Взломанные сайты.167
Атаки типа MITM168

ГЛАВА 8. ТЕХНОЛОГИИ ЗАРАЖЕНИЯ 170

Дроппер	171
Инфектор	171
Инжектор	172
Лоадер	172
Процесс заражения.	172
Инфицирование файловых объектов	174
Методы обеспечения	
автоматического запуска	176
Инжекты	177
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 истории	200
Как антивирусные компании	
пополняют базы?	202
Компоненты антивирусной	
программы	203
Сигнатурное детектирование	205
Поведенческий анализ	206
Эвристический анализ.	207
Проактивная защита (HIPS)	208
Методики противодействия	
антивирусам	209
Переупаковка	209
Обфускация	210
Антиотладка.	211
Заключение	212

ГЛОССАРИЙ 213