Игорь Гульев

Создаем вирус и антивирус

2-е издание, стереотипное



Москва

Гульев Игорь
Г94 Создаем вирус и антивирус / Гульев Игорь — 2-е изд., стереотипное. – М.: ДМК. — 304 с.: ил.

Virus Warning!

С этим сообщением, хоть раз в жизни, сталкивался любой пользователь компьютера. Вирмейкеры с упорством маньяков плодят все новые и новые разновидности вирусов. Бытует мнение, что избавиться от них можно лишь с помощью сложных и дорогостоящих новейших антивирусных программ. Это не совсем верно – знание принципов действия и способов внедрения вирусов поможет вовремя их обнаружить и локализовать, даже если под рукой не окажется подходящей антивирусной «вакцины».

В этой книге вы найдете обширный материал, посвященный проблеме защиты информации, рассмотренной с обеих сторон баррикад (как от лица вирмейкера, так и создателя антивирусов).

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Информация, представленная автором книги, предназначена исключительно для удовлетворения любопытства уважаемых читателей. Издательство не несет ответственности за возможные негативные последствия в результате ее использования в целях, запрещенных Законодательством РФ.

ISBN 978-5-519-67705-9

© ДМК

КРАТКОЕ СОДЕРЖАНИЕ

ГЛАВА 1
COM-ВИРУСЫ 9

ГЛАВА 2
EXE-ВИРУСЫ 25

ГЛАВА 3
ВИРУСЫ ПОД WINDOWS 55

ГЛАВА 4
МАКРО-ВИРУСЫ 95

ГЛАВА 5
МАСКИРОВКА ВИРУСОВ 107

ГЛАВА 6
МЕТОДЫ БОРЬБЫ С ВИРУСАМИ 149

ГЛАВА 7
BBS И FTN-СЕТИ 181

ГЛАВА 8
ХАКЕРСКИЕ ШТУЧКИ, ИЛИ КАК ОНИ ЭТО ДЕЛАЮТ 193

ПРИЛОЖЕНИЯ 210

АЛФАВИТНЫЙ УКАЗАТЕЛЬ 302

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 8

ГЛАВА 1

COM-ВИРУСЫ 9
Структура и процесс загрузки COM-программы 10
Простейший COM-вирус 11
Способы внедрения COM-вирусов 22

ГЛАВА 2

EXE-ВИРУСЫ 25
Структура и процесс загрузки EXE-программы 26
Классификация EXE-вирусов 27
Вирусы, замещающие программный код (Overwrite) 27
Вирусы-спутники (Companion) 27
Вирусы, внедряющиеся в программу (Parasitic) 28
Способы заражения EXE-файлов 29
Вирусы, замещающие программный код (Overwrite) .30
Вирусы-спутники (Companion) 36
Инфицирование методом создания COM-файла спутника 36
Инфицирование методом переименования EXE-файла 40
Вирусы, внедряющиеся в программу (Parasitic) 46
Стандартное заражение EXE-файлов 46
Внедрение способом сдвига 52
Внедрение способом переноса 53

ГЛАВА 3

ВИРУСЫ ПОД WINDOWS 55
Вирусы под Windows 3.11 56
Вирусы под Windows 95 69

Вызов Windows 95 API 69
Адреса и номера функций 70
Соглашения о вызовах 71
Заражение файлов формата PE-executable 71
Пример вируса под Windows 95 72

ГЛАВА 4

МАКРО-ВИРУСЫ 95
Инструментарий 96
Общие сведения 96
Процедура SaveAs 103
Специальные процедуры 103
Пример макро-вируса 104

ГЛАВА 5

МАСКИРОВКА ВИРУСОВ 107
Protected Mode – укрытие для вируса 108
Обход резидентных антивирусных мониторов 119
Определение адреса оригинального обработчика DOS 120
Борьба с антивирусными мониторами 129
Конструирование неотслеживаемого обращения к DOS 130
Пример реализации 131
Flash BIOS 135
Новое место для вирусов 135
AMI Flash вирус 135

ГЛАВА 6

МЕТОДЫ БОРЬБЫ С ВИРУСАМИ 149
Стандартные программы защиты 151
Поиск вируса 152
Как исследовать алгоритм работы вируса 161
Эвристические анализаторы кода 167
Блокировщик вируса 169

Пример антивируса 172

ГЛАВА 7

BBS И FTN-СЕТИ 181
Взлом BBS 182
Получение пароля BBS без взлома 186
Взлом FTN-сетей 187
Безопасность вашей BBS 191

ГЛАВА 8

ХАКЕРСКИЕ ШТУЧКИ, ИЛИ КАК ОНИ ЭТО ДЕЛАЮТ 193
Проверка на отсутствие АОН 194
Советы по регистрации 194
Что «помнит» компьютер 195
К вопросу о CMOS SETUP 196
Программы, авторизующиеся в Online 197
Клавиатурные шпионы 197
Защита от ПЭМИН 198
Пейджинговая безопасность 198
Электронная почта 199
Получение E-mail 199
Отправление E-mail 201
Второй адрес 203
Идентификация пользователя по E-mail 205
Защита от SPAM 207
На FTP-сервер под чужим IP-адресом 208

ПРИЛОЖЕНИЯ 210

ПРИЛОЖЕНИЕ А
Форматы заголовков EXE-файлов 211
ПРИЛОЖЕНИЕ Б
Функции DOS (INT 21h) 223

ПРИЛОЖЕНИЕ В
Функции программирования Flash в AMIBIOS 273
ПРИЛОЖЕНИЕ Г
Функции DPMI (INT 31h) 281
ПРИЛОЖЕНИЕ Д
Коды ошибок DOS 299
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ 300
БЛАГОДАРНОСТИ 301
АЛФАВИТНЫЙ УКАЗАТЕЛЬ 302

ВВЕДЕНИЕ

Вряд ли стоит напоминать, что компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Однако в связи с этим особенно обострилась проблема защиты информации.

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность...

Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных саморазмножающихся программ. Совсем недавно заражение вирусом текстовых файлов считалось абсурдом – сейчас этим уже никого не удивишь. Достаточно вспомнить появление «первой ласточки», наделавшей много шума – вируса WinWord.Concept, поражающего документы в формате текстового процессора Microsoft Word for Windows 6.0 и 7.0.

Хочется сразу заметить, что слишком уж бояться вирусов не стоит, особенно если компьютер приобретен совсем недавно, и много информации на жестком диске еще не накопилось. Вирус компьютер не взорвет. Ныне известен только один вирус (Win95.CIH), который способен испортить «железо» компьютера. Другие же могут лишь уничтожить информацию, не более того.

В литературе весьма настойчиво пропагандируется, что избавиться от вирусов можно лишь при помощи сложных (и дорогостоящих) антивирусных программ, и якобы только под их защитой вы можете чувствовать себя в полной безопасности. Это не совсем так – знакомство с особенностями строения и способами внедрения компьютерных вирусов поможет вовремя их обнаружить и локализовать, даже если под рукой не окажется подходящей антивирусной программы.

Глава 1

COM-ВИРУСЫ

Структура и процесс загрузки COM-программы 10
Простейший COM-вирус 11
Способы внедрения COM-вирусов 22

В этой главе рассказано об алгоритмах работы вирусов, заражающих COM-файлы, и способах их внедрения. Представлен исходный текст одного из таких вирусов с подробными комментариями. Также приведены основные сведения о структуре и принципах работы COM-программы.

Компьютерные вирусы могут «гнездиться» в самых неожиданных местах, например, в записи начальной загрузки MBR (master boot record), в исполняемых файлах типа COM и EXE, в файлах динамических библиотек DLL и даже в документах текстового процессора Microsoft Word for Windows. В этом разделе подробно рассматривается строение вируса, поражающего COM-файлы.

Структура и процесс загрузки COM-программы

Что же представляет собой COM-программа, как она загружается в память и запускается?

Структура COM-программы предельно проста – она содержит только код и данные программы, не имея даже заголовка. Размер COM-программы ограничен размером одного сегмента (64Кбайт).

И еще два понятия, которые часто будут встречаться:

Program Segment Prefix (PSP) – область памяти размером 256 (0100h) байт, предшествующая программе при ее загрузке. PSP содержит данные командной строки и относящиеся к программе переменные.

Disk Transfer Address (DTA) – блок данных, содержащий адреса обмена данными с файлом (чтение или запись). Область DTA для работы с файлом используют многие функции, в том числе и не производящие чтение или запись в файл. Примером может служить функция 4Eh (найти первый файл по шаблону), которая будет неоднократно встречаться в листингах программ.

Загрузка COM-программы в память и ее запуск происходят так:

1. Определяется сегментный адрес свободного участка памяти достаточного для размещения программы размера.
2. Создается и заполняется блок памяти для переменных среды.
3. Создается блок памяти для PSP и программы (сегмент:0000h – PSP; сегмент:0100h – программа). В поля PSP заносятся соответствующие значения.
4. Устанавливается адрес DTA равным PSP:0080h.
5. Загружается COM-файл с адреса PSP:0100h.