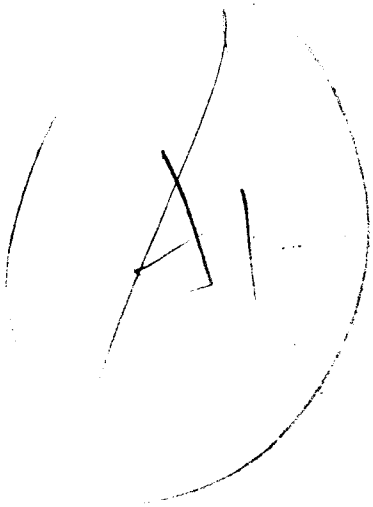
The Computer Virus Handbook



The Computer Virus Handbook

Richard B. Levin

Osborne McGraw-Hill

Berkeley New York St. Louis San Francisco
Auckland Bogotá Hamburg London Madrid
Mexico City Milan Montreal New Delhi Panama City
Paris São Paulo Singapore Sydney
Tokyo Toronto

FOREWORD

On October 12, 1985, the *New York Times* carried a story about a man who had downloaded a program from a computer bulletin board system on Long Island. The program was called EGABTR and was supposedly designed to significantly enhance the performance of any IBM compatible with an EGA graphics card. Instead, while distracting the user with an on-screen display, the program systematically wiped out every file on the hard disk. Adding insult to injury, the program finished up by throwing the phrase "Arf! Arf! Got You!" up on the hapless victim's screen.

As a longtime follower of the personal computer communications field, I was naturally drawn to this story. But what struck me as odd was not the story itself, but the fact that the *New York Times* ran it on the *front page*. October 12th of that year fell on a Saturday, and all I could figure was that it must have been a slow news day. I didn't realize it at the time, but that October day not only marked the discovery of America by Columbus, it also marked the discovery of "computer viruses" by the press at large.

Three days later the *Wall Street Journal* ran the story as well. Only it placed it in the lower-left corner of the second section, a box known inside the company as "the orphan." I nodded in approval since in my professional estimation that gave it about the emphasis it deserved. An interesting story, a little tidbit, but nothing to get excited about.

After all, programs with embedded code designed to do unexpected things have been around as long as there have been computers. And they haven't always been the product of some wan, wild-eyed programmer. In 1983, for example, *Popular Computing* reported on the technique Digital Equipment Corporation (DEC) employed to discourage illegal copies of its Decmate II software. In 1980 the company installed a number of Decmate II micros at selected test sites and offered customers at those sites special deals and incentives to keep the company informed about system bugs.

The Decmate II was one of the better word processing systems of the day, and the software provided to these test sites was of particular

interest. Evidence exists of people selling bootleg copies to friends and, of course, keeping copies for their own use. "But DEC had a surprise in store for these thieves," the magazine reported. "In a unique software protection scheme, DEC had embedded into the word processing source code the statement, IF DATE$ = APRIL 1, 1983 THEN DELETE ALL FILES." All across the country on April Fool's Day of that year there were muffled cries of despair. Muffled, because calling DEC customer support would be tantamount to an admission of piracy.

So computer viruses are nothing new. What's new is that the press has discovered them and in doing so has found that the story strikes a responsive chord in the public at large. And like any good business, the media gives the public what it wants. So we have had more coverage, with each story feeding upon itself.

It reminds me of the airplane hijacking phenomenon of the 1970s. That story, too, caught fire, and with each new incident dozens of twisted minds were inspired to add their names to the list of those who are infamous for 15 minutes.

There are other similarities as well. Many people are afraid of flying anyway, and thoughts of being hijacked add greatly to those fears. Many people have a similar unreasoning fear of computers, and the thoughts that "these machines that control our lives" could be vulnerable to a devastating "infection" provokes both irrational terror and secret smiles of satisfaction.

Clearly, the computer nasties the press and public now loosely refer to as "viruses" are real. They do exist, and they do pose a threat to any computer system. But so too does a power company blackout—or worse, a brownout. Indeed, the files in most computer systems are much more likely to be erased by an untrained user than they are by a virus, Trojan horse, or logic bomb.

What's needed is considerably less heat and a lot more light. And I'm happy to report that that's exactly what you'll find here. Rich Levin has done a masterful job of putting the virus phenomenon in its proper perspective. He separates the facts from the media hype and fiction. He tells you what to look for, and what to do (and not do) should you find a virus. Most important of all, he gives you practical, well considered advice on how to *prevent* viral infections.

Viruses and other deliberately destructive programs are a well-established fact of computer life. It is only prudent to guard against them. But let reason rule. The hysteria is not only unfounded, it is counterproductive. Rich Levin will show you what to do. You simply couldn't ask for a more comprehensive, common sense guide than this. It is *must* reading for every computer owner.

– Alfred Glossbrenner

ACKNOWLEDGMENTS

I would like to thank everyone who influenced or otherwise contributed to the creation of this book; however, space and memory limitations prohibit me from doing so. I will therefore limit my acknowledgments to those persons directly involved in the production and management of this project. To those not formally acknowledged—thank you for your help.

First and foremost, I want to thank my editor at Osborne/McGraw-Hill, Roger Stewart, for sharing his management and editorial expertise, and for believing in the concept and viability of this project. Thanks also to my agent, Nick Anis, for his guidance and support.

Thanks are due to Chuck Guzis of Sydex for his impeccable technical editing of the manuscript, and to Judy Berkowitz, who did a superb job with the copyediting of the book. Thanks to Laurie Beaulieu, Associate Editor, whose reasoned opinions, patience, and unending good humor speeded the process of reviewing Judy's edits. And thanks to Judith Brown, Project Editor, for rewarding me with her informed opinions and helpful guidelines as we readied the final proofs for the presses.

I am grateful for the talents of Kendal Andersen, Marketing Services Manager, and Ann Kameoka, Publicity Coordinator at Osborne, for their on-going efforts. Thanks also to Carie DeRuiter and Suellen Ehnebuske at Graphic Eye, Inc., for the book's cover design, and to David Kerper at Kerper Studio, for the cover photograph.

Special thanks to my friends John Blumberg, David Bushong, Nelson Ford, Ross Greenberg, Mary Hughes, John McAfee, David Moskowitz, Don Watkins, and the folks at CompuServe Corporation and Symantec Corporation for providing valuable software, documentation, commentary, and reference materials. Thanks to Brian Proffit and IBM Corporation, and to Kurt Ebert for valuable remarks. Thanks as well to all the programmers who contributed their software development efforts on behalf of *The Computer Virus Handbook* disk. A note of appreciation is also

due to Katherine Margolis, for her efforts, and to my friends at I/O Corporation in Conshohocken, Pennsylvania, for their support.

Thanks to Gene Spafford for the quote and the conversation. Thanks to both Alfred Glossbrenner and Philippe Kahn for taking time out of their busy schedules to preview the manuscript and provide the book's foreword and back cover commentary, respectively.

Thanks to Charles Bowen, James Moran, Cathryn Conroy, Daniel Janal, and J. Scott Orr for their consistently evenhanded and well-researched reporting in the pages of *CompuServe Magazine* on the rogue software events of recent years.

Thanks also to the callers of the Mother Board BBS in Philadelphia, Pennsylvania (215-333-8275; give it a call) and to users of the CHECKUP virus detection system. Your ideas and encouragement are, as always, irreplaceable.

A big, warm note of thanks to my friend and co-author, Kathy Ivens, whose support and hard work were invaluable to the completion of this project and to the maintenance of my sanity. Thanks for everything, Kathy.

Finally, I would like to thank my family—Mom, Dad, Mark, and Michele, my wife, Carol, and my baby daughter, Rachel; Mom and Dad Fink, and Michael, and cousins Steven and Bruce—for their love, strength, support, and encouragement.

Computer viruses are not the only problem facing computer users and systems managers today. Many people are now wrestling with the problem of choosing their next operating system—be it OS/2, UNIX, a DOS extender or a non-IBM-compatible solution. Managers are trying to decide which side to root for in the spreadsheet wars, where even venerable Lotus Development Corporation now offers a multitude of spreadsheets, each called 1-2-3, each with different features and abilities. Nowadays it is no longer sufficient to evaluate programs on the basis of their individual merits alone; we must decide which interface to standardize all of our software on—GUI or character-based? Life in the fast-track world of computing grows more confusing every day.

Complicating matters immensely is the issue of rogue software—programs designed with no other purpose than to destroy your hard-earned data. Software bombs, Trojan horses, worms, computer viruses, and other fiendish software devices have entered the fray of personal computing with a vengeance. Hundreds, perhaps thousands of personal computers have been affected and infected by rogue computer software. The loss to businesses, both large and small, in time, money, and data is unaccountable. And no end is in sight.

But the sky is not falling. The end is not near. With a little work, computer viruses and other rogue code can be understood and managed by all users, from sophisticated power users to budding novices. The trick is to have accurate, straightforward information at your disposal—*information that's in this book.*

ABOUT THIS BOOK

This book was written for people who take their personal computing seriously; people who are concerned about the problem of rogue soft-

ware; people who want to know what they can do to help stop the spread of this troublesome breed of software.

Fighting computer viruses is a practical problem, the responsibility for which lies in the hands of end users—your hands. Before you can begin fighting the spread of computer viruses, you must first understand what they are, how they work, and how you can protect yourselves against them.

All of the material in this book is written so everyone, regardless of their level of proficiency, will understand and benefit from it. Educating the scholars and professional programmers is not the answer to the computer virus problem. Educating the computing masses, of which scholars and programmers are a part, is the answer. Therefore, where possible, overly technical dissertations have been waived in favor of accessible, serviceable solutions.

This is not a book that you will keep beside your computer as a point of reference for years to come. Rather, *The Computer Virus Handbook* will serve as your guide on a tour of the extraordinary world of computer viruses. Readers will, hopefully, come away with a new awareness of safe computing habits, a better comprehension of virus and antivirus capabilities, and a sense of objectivity for dealing with viral infections.

HOW THIS BOOK IS ORGANIZED

This book is divided into four parts. Part One, "What Are Computer Viruses and Where Do They Come From?" explains the nature of computer viruses and other rogue program types, virus capabilities and limitations, how and why viruses are created, how they work and how average users help them spread. Part One also features an overview of computer virus types and infection methods.

Part Two, "Preventing the Spread of Computer Viruses," focuses on ways to evaluate and implement antivirus software, and on erecting barriers against viral infections and other rogue software attacks. General instructions for eradicating viral infections are also presented. The section is wrapped up with a psychological profile of rogue software developers along with some comments from Don Watkins, a leader in the field of public computerized information services.

Part Three, "User Guides," contains the edited documentation for a number of well-known antivirus software programs, all of which are available on disk through a coupon offer featured at the back of the book.

Part Four concludes the book with a collection of appendixes that are well worth reading in their own right. From a comprehensive history of viral attacks to an in-depth review of viruses and the law, to detailed listings of IBM- and Macintosh-class computer viruses, the appendixes contain a wealth of material that augments and complements the balance of *The Computer Virus Handbook*.

Finally, the back pages contain an assortment of coupon offers for select antivirus, security-related, and data integrity maintenance software.

SOFTWARE AND HARDWARE USED TO CREATE THIS BOOK

This book was written using Microsoft Word 5.0 running on an MS-DOS 4.01-based ALR (Advanced Logic Research) PowerFlex 286 with the 386sx module installed. The manuscript was output as "Text only," archived using Yoshi's LHarc 1.13c, and posted on our BBS, the Mother Board, running BBSX software 2.44.B in a multitasked, DESQView-386 virtual 8086 partition.

Kathy Ivens downloaded the text and imported it into her DOS-based ACER 1100/25 under WordPerfect 5.1 or Xywrite III+, depending on her mood. The final manuscript was output on a Hewlett-Packard LaserJet III using Glyphix fonts from Swfte International.

Source code was developed using the Norton Editor. Code was assembled and compiled using products developed by Microsoft Corporation and Borland International.

ADDITIONAL HELP FROM OSBORNE/McGRAW-HILL

Osborne/McGraw-Hill provides top-quality books for computer users at every level of computing experience. To help you build your skills, we suggest that you look for the books in the following Osborne/McGraw-Hill series that best address your needs.

The "Teach Yourself" series is perfect for people who have never used a computer before or who want to gain confidence in using program

basics. These books provide a simple, slow-paced introduction to the fundamentals of popular software packages and programming languages. The Mastery Skills Check format ensures that you understand concepts thoroughly before you progress to new material. Plenty of examples and exercises are used throughout the text, and answers are provided at the back of the book.

The "Made Easy" series is also for beginners or users who may need a refresher on the new features of an upgraded product. These in-depth introductions guide users step-by-step from program basics to intermediate use. Every chapter includes a number of hands-on exercises and examples.

The "Using" series presents fast-paced guides that quickly cover beginning concepts and move on to intermediate techniques and some advanced topics. These books are written for users already familiar with computers and software who want to get up to speed fast with a certain product.

The "Advanced" series assumes that the reader is a user who has reached at least an intermediate skill level and is ready to learn more sophisticated techniques and refinements.

The "Complete Reference" series provides handy desktop references for popular software and programming languages that list every command, feature, and function of a product along with brief but detailed descriptions of how they are used. Books are fully indexed and often include tear-out command cards. The "Complete Reference" series is ideal for both beginners and pros.

The "Pocket Reference" series is a pocket-sized, shorter version of the "Complete Reference" series. It provides the essential commands, features, and functions of software and programming languages for users of every level who need a quick reminder.

The "Secrets, Solutions, Shortcuts" series is for beginning users who are already somewhat familiar with the software and for experienced users at intermediate and advanced levels. This series provides clever tips, points out shortcuts for using the software to greater advantage, and indicates traps to avoid.

Osborne/McGraw-Hill also publishes many fine books that are not included in the series described here. If you have questions about which Osborne books are right for you, ask the salesperson at your local book or computer store, or call us toll-free at 1-800-262-4729.

OTHER OSBORNE/McGRAW-HILL BOOKS OF INTEREST TO YOU

We hope that *The Computer Virus Handbook* will assist you in overcoming and preventing computer viruses in your workplace, and will also pique your interest in learning more about other ways to better use your computer.

If you're interested in expanding your skills so you can be even more "computer efficient," be sure to take advantage of Osborne/M-H's large selection of top-quality computer books that cover all varieties of popular hardware, software, programming languages, and operating systems. While we cannot list every title that may relate to your special computing needs, here are just a few related books that may complement *The Computer Virus Handbook.*

Hard Disk Management: The Pocket Reference, by Kris Jamsa, is a handy little guide that helps users who already know DOS basics make the most of their hard disk's speed and capacity. It covers all versions of MS-DOS and PC-DOS through 3.3.

If you're looking for an encyclopedia of every DOS command and function, ask for *DOS: The Complete Reference, Second Edition* by Kris Jamsa. From an overview of the disk operating system to a reference for advanced programming and disk management techniques, this best-selling book has it all for DOS users at every skill level. Each chapter begins with a discussion of specific applications followed by a list of related commands.

For UNIX users with System V Release 3.1, from beginners who are somewhat familiar with the operating system to veteran users, see *UNIX: The Complete Reference,* by Stephen Coffin. This handy desktop encyclopedia covers all UNIX commands, text processing, editing, programming, communications, the shell, the UNIX file system, and more.

CONTENTS AT A GLANCE

CONTENTS