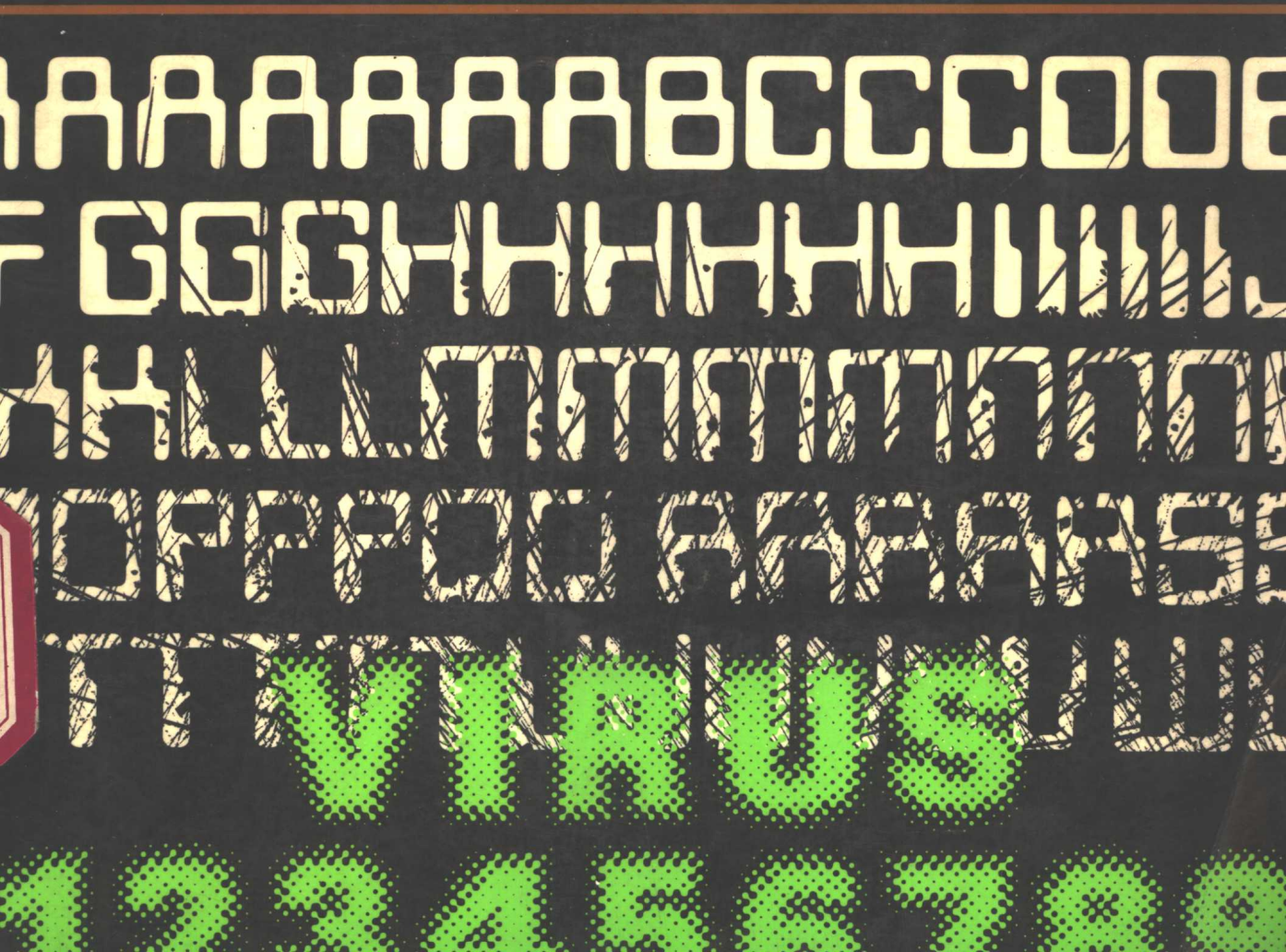
THE COMPUTER VIRUS CRISIS

Philip Fites / Peter Johnston / Martin Kratz



The Computer Virus Crisis

Philip Fites
Peter Johnston
Martin Kratz

VAN NOSTRAND REINHOLD
New York

Copyright (c) 1989 by Van Nostrand Reinhold

Library of Congress Catalog Card Number 88-13496
ISBN 0-442-28532-9

All rights reserved. No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means--graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems--without written permission of the publisher.

Printed in the United States of America

Van Nostrand Reinhold
115 Fifth Avenue
New York, New York 10003

Van Nostrand Reinhold (International) Limited
11 New Fetter Lane
London EC4P 4EE, England

Van Nostrand Reinhold
480 La Trobe Street
Melbourne, Victoria 3000, Australia

Macmillan of Canada
Division of Canada Publishing Corporation
164 Commander Boulevard
Agincourt, Ontario, M1S 3C7, Canada

16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Library of Congress Cataloging in Publication Data

Fites, Philip E.
The computer virus crisis / Philip Fites, Peter Johnston, Martin Kratz
p. cm.
Bibliography: p.
Includes index.
ISBN: 0-442-28532-9 (pbk.)
1. Computer viruses. I. Johnston, Peter, 1948- . II. Kratz, Martin P. J. III. Title
QA76.76.C68F57 1989
005.8--dc19 88-13496

PREFACE

Do you worry about computer virus programs? If you use personal computers, and especially if you frequently use bulletin boards, perhaps you should. This book provides accurate information to help you learn what the whole virus phenomenon is about. You'll find checklists to help you cope with a virus problem, and lists of symptoms to help you diagnose your problem as a virus. We've provided practical tips to help you avoid virus programs in the first place. In the Appendix, there are brief reviews, with contact addresses, of antiviral products. If you're a professional, you'll find references to help you dig into technical details.

There's a party game called telephone or grapevine. People sit in a circle, one person whispers a message into the next person's ear, that person whispers the message into the next person's ear, and so on around the circle. The last listener then compares what was heard to what was whispered by the first person in the chain. Normally, the message is totally garbled by the time it gets back around the circle to the first person.

Some of the general press reports about computer virus programs in the past few months remind us of this party game. The first report, say in the *Wall Street Journal*, is reasonably detailed. (To a security professional, it shows evidence of a reporter who doesn't really understand the situation but takes good notes and writes well.) The story goes out over the wire services; it's edited to fit other newspapers' needs (often by people who have no technical knowledge at all), and by the time a local paper prints it, there's almost no resemblance to the original story.

The authors of this book all practice in areas that lead to advising clients on computer security or legal matters. During lunch one day, two of us were lamenting the garbled press reports and debating how we could serve our clients better by being ready to help them cope with computer virus programs. We knew of the *MacMag* virus on the Macintosh that startled users on March 2, 1988. Viruses had not been much of a problem in the past but with the sudden publicity we expected (and still expect) them to become a very big problem.

At some point in that discussion, one of us said, "Why don't we write a book." The book you are reading is the result.

We've compiled the available information into one book and written it using language understandable to people without in-depth technical backgrounds. By knowing the technical issues, we've avoided the inaccuracies sometimes found in articles written by people who don't really understand the technical issues but simply take notes.

The Computer Virus Crisis will help people who are, or think they are, or may soon be, coping with a computer virus. Although the level is relatively non-technical, we have included sufficient technical detail to help those who have some background to understand what some of the exposures are, how to recognize when they have a virus, and what to do about it if they do. If you need more information, refer to the Appendix, which is a review of some antiviral products. Some packages include detailed technical hints, along with instructions on how to use the tools provided. We recommend that you check out the vaccines and other protection software.

In *Through the Looking Glass and What Alice Found There*, Lewis Carroll has a character say, "When I use a word, it means just what I choose it to mean--neither more nor less." Since there's considerable confusion (even among professionals) about many words used in the area of computer security, we've included a Glossary. Use the definitions to help you in this book as well as others. It's ever so much more fruitful to talk about things when everyone's using the same words to mean the same things.

This book is not the last word on computer virus programs. Many vandals are working very hard to create viruses and many professionals are working to devise protection methods and products. Things change extremely quickly, far more quickly than a book can reflect. With this book as a base, you'll know enough about what the situation is to be able to follow the current material from magazines and journals.

In many places in this book, we present illustrative material designed to explain how a computer virus can do what it does. When we were creating these examples, we had a dilemma: If we made the examples absolutely complete and functional, we would in effect provide a "cookbook" that could very easily be used by vandals to produce a virus. That is not our desire or purpose. We do not want to promote the spread of viruses. The examples are therefore detailed and complete enough to illustrate the points, but not enough to produce a virus. What we want to do is help average computer users understand what computer virus programs are about and how to guard against them. When you understand what is going on, your use of computers will be safer.

The professionals and programmers who read this will easily identify the missing information *because they already have this background knowledge*--it is part of the working tools of our profession.

In creating this book, we have had considerable support from many people. Some of the software developers whose products are reviewed in the Appendix provided not only copies of their products for review, but also information their own research staffs have accumulated. Mr. Ian Fraser, owner of Microcomputer And Graphic Image Consultants Inc., helped out with much of the technical de-

此为试读,需要完整PDF请访问: www.ertongbook.com

tail in Chapter 5 and reviews of the DOS antiviral programs in the Appendix. Dr. H. Highland, editor-in-chief of *Computers and Security*, is working at a very technical level and helped us with numerous references and some reports of what his team is discovering. Dianne Littwin and Maud Keisman of Van Nostrand Reinhold have worked closely with us to accomplish publishing a quality book as quickly as possible. Ms. Harriet Serenkin offered invaluable advice in revising drafts.

We first heard the phrase "safe hex" from Michael Cervansky, Vice President of Sophco in Boulder Colorado. We found that the phrase is highly recognizable to lay as well as professional computer users and chose to use it to give people a memorable description of the group of protective measures that minimize your chances of problems with virus programs.

Except for one poster reproduction, the book was created entirely using computer tools. Drafts were printed on a laser printer at Galbraith Law Offices, and the typesetting was done from the same PostScript files by the University of Alberta Printing Services.

After reading this book, we hope you will see that viruses are not all that magical or mythical. They unfortunately can be produced and spread by all too many individuals. We hope this book will make you more aware of the problem. Once you are aware, your chance of being exposed or, if exposed, infected, is less. We want you to practice safe hex.

As a final point, we want you to know that we consider introducing viruses into other people's computer systems unethical, unprofessional, and unlawful. *Don't do it!*

CONTENTS

Chapter 1

INTRODUCTION

Is today the day? I know there's something important I must do if the time is right. No, it's not Friday the 13th yet. Let's see now: If today isn't the day, I have to reproduce myself. Let's look at the system files; I know there will be one, every computer has one. There's one: Is there one of me there already? If there isn't, I can copy myself. No, I'm already in that program; let's check out this computer's program files. Surely there's at least one where I haven't been yet. Yes, there's one, and I found it after only 48 tries. Oh, it's marked read-only; that's OK, I'll just change that marking so I can change the file. This feels good; I'm copying myself into that program; now I change the program just a bit, a little jump here and a return there, after my copy. I remember changing something--oh, yes, change the file back to read-only. Now, did I cover my tracks? Let's see, all the attributes are the same as when I got here; the length hasn't changed since I found some empty space to copy myself into. I must remember to change the creation date back to what it was when I got here, too. No point in making it easy to see where I've been. Am I finished yet? No; I need to go through the same process on the diskette drives, if there are any, and see if I can reach through a network too. Am I finished now? Yes--oh, that's what I'm supposed to do on Friday 13th! I wonder what FORMAT C: means? Hey, I'm supposed to do that if I've made fifty copies of myself. And I was already at forty-nine. Next time . . . .

You've just been introduced to what a computer virus might be thinking (if it could think) as it goes about its business. There have been viruses that worked exactly that way. You wouldn't even know the virus was in your system, until something went wrong. Then you not only have to fix the visible damage, but you also have to find any place the virus might have made copies of itself.

You can be very safe, of course. You could purchase a machine from a trusted manufacturer, write all of your own programs, never use anyone else's programs, and never communicate with another computer. As long as your trusted

manufacturer is really careful, you would not be risking exposure to viruses. You also would not have a very useful computer, and you wouldn't be taking part in one of the things that is changing our world in ways never before possible in human history.

There are other ways you can protect yourself; some even offer good protection. The purpose of this book is to tell you the real story about computer virus programs, and help you protect yourself against them without missing out on the information revolution.

USING THIS BOOK

This book contains four kinds of information: moderately technical information; references for other reading on security in general and viruses in particular; reviews of antiviral products in the Appendix and definitions in the Glossary; and general information about the whole computer virus phenomenon.

If you think you've got a computer virus, turn to the Appendix *immediately*, and contact one of the vaccine developers to begin solving your problem. While you're waiting for your new vaccine, look at Chapters 8 and 9; they contain several hints about what to do. After you've cleaned up everything, look at Chapters 4 and 7, for suggestions on how to avoid future problems.

If you just want to learn about viruses, continue reading. If you already know a fair bit, look at Chapter 5, which has the most technical material.

If you're thinking that it might be good fun to create and spread a virus, read Chapters 10 and 11, where you'll see that it's against the law. Then read Chapter 6, which describes some of the bad effects that unethical people who spread computer diseases cause for everyone else. *Don't do it!* You make things worse for yourself as well as for the rest of us.

How Viruses Affect You

In the past few months, the press has published many reports about computer viruses. There's been a real outbreak, with the impetus probably provided by the triggering of the *MacMag* "Peace" virus in March 1988.[1] Unfortunately, some of the material has been sensational or garbled, such as a report that every computer in Seattle has a virus. In reality, computer viruses don't spread like the

[1] See [Peace Virus 1988], [O'Connor 1988]. This virus was first reported around February 1988. It's referred to either as the *MacMag* virus or as the peace virus. We believe in assigning responsibility where due, and use the perpetrators' name.

common cold. They aren't intelligent; they don't hate you; and it's not even very difficult to avoid most exposures.

But there have been, and there are now, some pretty nasty viruses floating around in computers. Some developments in the past few years have increased people's exposure. If you communicate with other computers, especially if you download programs from public bulletin boards, your risk could be high. If you accept pirate copies of software from people you don't know (or even if you do know the source of your copy, but not the source of the other person's copy), your risk could be *very* high.

On the other hand, if you have programs that you purchased in shrink wrap and perhaps an electronic mail setup, your risk isn't too great.

You need to ask yourself, "Does anyone dislike *me* that much?" If you're a specific target, you need to take precautions. If you're just John User (or Jane User) you'll probably never have a problem if you simply apply some common sense.

WHAT'S THE PROBLEM?

About 10 years ago, one of us needed to run a job as cheaply as possible on a time-sharing system. The job would take a while to run and had to wait for other higher priority, and higher-paying, jobs. It was late Friday afternoon. A small file was created that would check to see if the job had run; if it had run, commands in the file would direct output appropriately and clean things up; if it had not run, it would submit itself into the job queue again. In this way, the job would be sure to get the lowest rate, and the author could go home rather than wait around Friday evening.

Unfortunately, the command file wasn't tested carefully enough. It wound up submitting itself repeatedly. In fact, as soon as the job actually did run, the command file went wild. Ten minutes after the system was started up on Sunday, the author got a polite and rather pointed call from the system administrator, who wanted the 4096 copies of the same job deleted from the job queue so someone else could get in (Figure 1.1). The situation wasn't intentional, but its effect was to create a quasi-virus and put it into a system. (It was fixed, with much embarrassment, taking about 15 minutes and several utilities to get rid of all those jobs.)

此为试读,需要完整PDF请访问: www.ertongbook.com

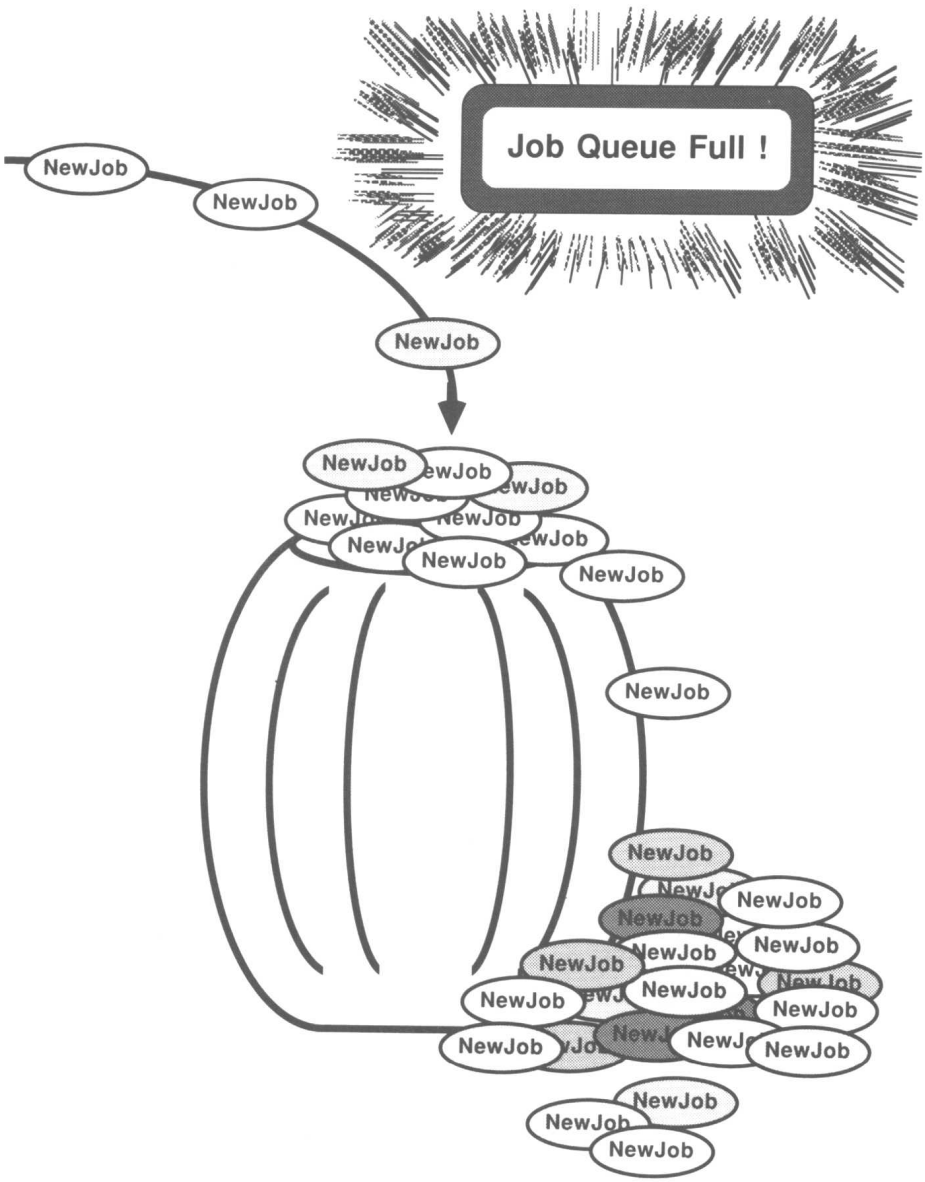


Figure 1.1 Too Many Jobs

Fred Cohen hadn't coined the term "virus" yet,[2] but that command file fit his later description. The point of the story is that a virus isn't anything new, magical, or otherwise unknown, in spite of what you can read today.

But if the concept of a virus isn't really new, and it's not very difficult to create one, even accidentally, why is there suddenly a problem? Partly, it's because the increasing compatibility of computers and communications have made it possible for a virus to spread much farther, faster, and easier than was possible in the past. And partly, it's because a lot more people, in fact millions, now use computers. (See Chapter 2 for the "connectivity" issue.)

Take a look at the kind of people who could create a virus. They have to have some skill with computers, especially writing programs. They have to have some kind of access to a computer, specifically to yours. They have to have a reason to spread a virus. Most likely, millions of people have the skills to create a virus, on purpose or accidentally. Any computer science student and a whole lot of bright youngsters with computers have the skills.

Professionals can, of course, create virus programs. But they think of the return from their effort. Before they do something, they ask, "Is there an easier and safer way to achieve my objective?" There have not been many computer viruses spread by professionals for the simple reason that those who want to destroy or damage programs or computers have easier ways to do it.

There *are* people with professional skills and training who desire to mess up computer systems. Terrorists and spies, as well as legitimate professionals, possess the needed skills. To date, they've had better results by doing things like attacking power supplies and bribing bank tellers. It's probable that the current rash of viruses wasn't created and spread by professionals to achieve an objective.

There's another category of people. We call them vandals. Their motivation is to throw a monkey wrench into the works and watch the sparks fly or to demonstrate how superior their minds are (as judged by themselves) by cracking computer systems. They're not usually looking for gain, and they don't care that the return may be less than the risk and cost. They are the kind of people who slash paintings in museums, throw rocks through windows, and generally are rather nasty and pitiful examples of human being. If people like this have technical skills, they might create a computer virus.

---

[2] [Cohen 1984].

WHAT IS A COMPUTER VIRUS?

A computer virus can be defined as malicious software which replicates itself.[3] This definition is a little biased for our purposes: A virus need not be malicious. The key things about a computer virus are that it reproduces itself, and can reproduce itself in systems other than the one in which it was created; and that it can somehow attach itself to other programs (see the Glossary and Chapter 2). The command file example mentioned earlier is almost a virus: It reproduced and denied access to that system (malicious, although not intended that way), and it would have done the same on any of the other computer systems maintained by that company if it had been copied; it didn't infect any other programs, however.

A virus is just a name for a class of programs. They reproduce and infect other programs. Beyond that they could do anything any other program can (see Chapter 3 for more).

You may run into another sort of computer vermin, the *worm*. It is a program that "worms" its way through a system, altering small bits of data or code whenever it can get access (Figure 1.2).

A virus might also be a worm; if a worm *reproduces* itself in other systems and *infects* other programs, it would also be a virus.

Note that a computer virus is a program and it has to be *run* in order to reproduce or to do any damage. This fact is the key to several of the protection strategies discussed later.

HOW DOES A VIRUS SPREAD?

A computer virus does *not* spread through the air. You can't get it by shaking hands, or touching a doorknob, or by having someone next to you sneeze. A computer virus must be *put* into your computer by you or by someone else. One way a computer virus can be put into your system is as a *Trojan Horse*. A Trojan Horse (see Chapter 2 and Figure 1.4) is, for our purposes, a program that seems to do one thing but also does something else.

[3] See [Podell 1987] for a similar definition.

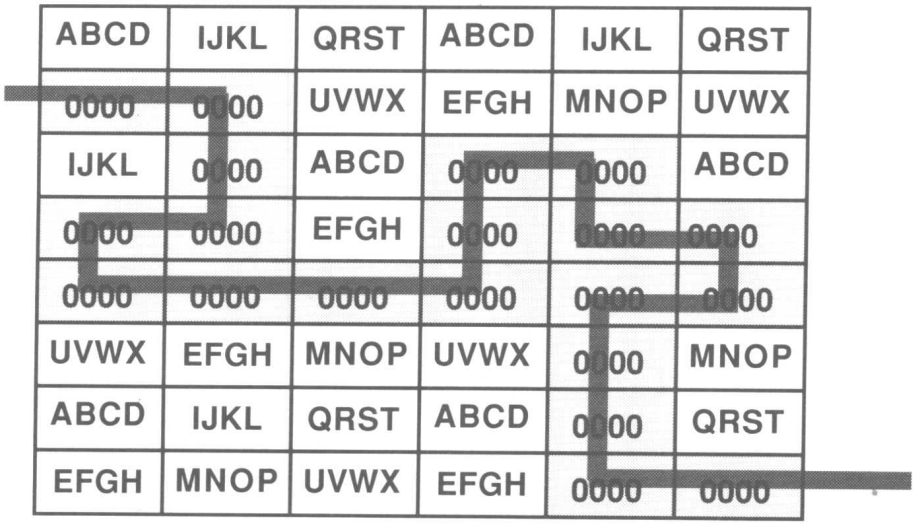


Figure 1.2 Worm Tracks

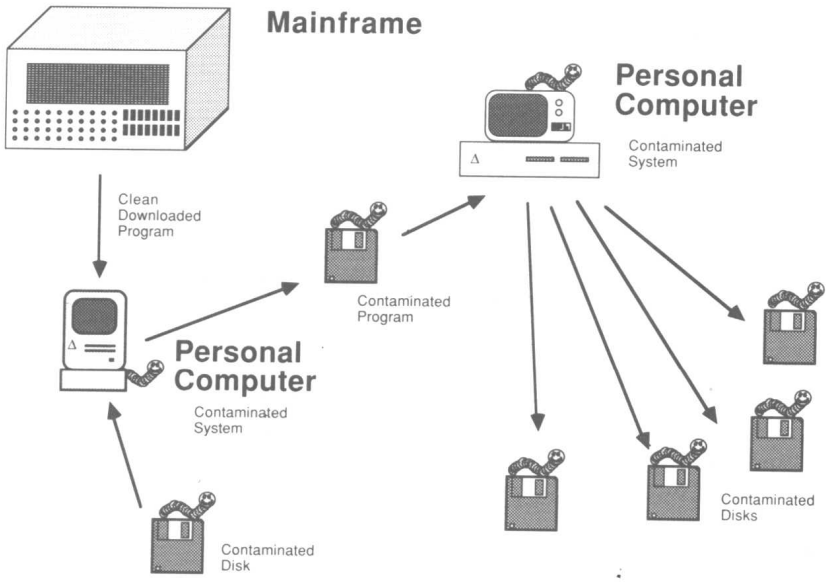


Figure 1.3 How a Virus Spreads

Figure 1.4 Trojan Horse

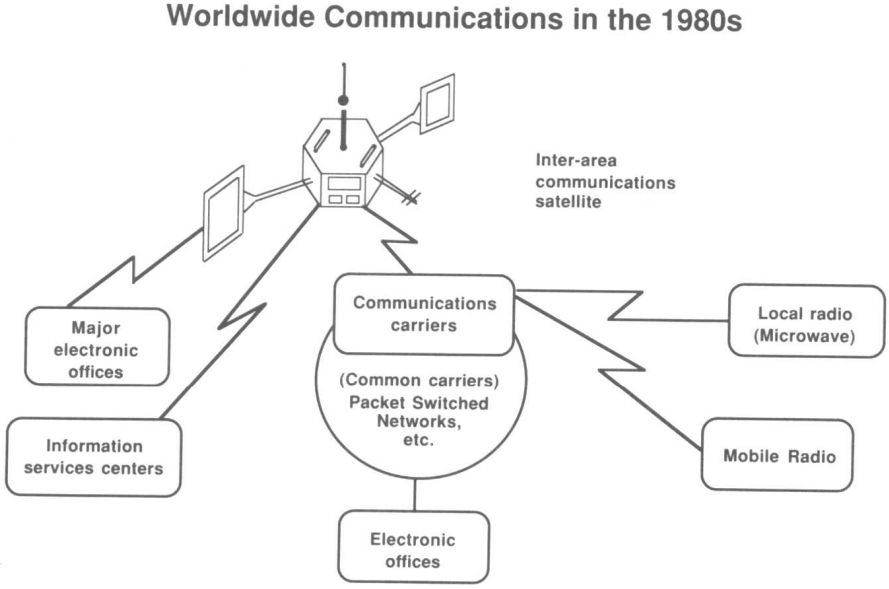


Figure 1.5 Worldwide Communications

We've said that computer viruses don't spread through the air and must be put into your system. This leaves an enormous number of possible infection pathways. For example, any time you download a program from another computer, or run a program from a diskette you've obtained, whether purchased, swapped, or borrowed, there is some exposure. Moreover, someone can tap telephone lines and insert a virus into your system--but this is not an easy task: Is there someone who dislikes *you personally* that much?

If you run a widely known bulletin board system (BBS), however, you might want to think about this. If you're an oil company transmitting exploration data, you're known to be at risk of corporate spying although probably not to viruses. If you're a government, you'd better plan on the enemy trying to put viruses into the computers that run your telephone system and your military communications in the event of war. If you are an individual microcomputer user, your exposure probably is not nearly as great.[4]

Different activities expose you to different risks. You can minimize your risk by practicing safe hex; simple common-sense measures that will cut your exposure to a very low level (see Chapter 7). These include things like avoiding pirate software, checking programs you download from a BBS before you run them, and using one or more of the antivirus tools described in the Appendix. Make sure you have good backups of your files and programs so you can recover from damage done by a virus (or by a power failure or static discharge, which is much more common).

Spreading Viruses Through Connectivity

The real reason computer viruses are becoming a serious problem, and could be catastrophic in the future, is linked to one of the long-term trends in the development of computers: connectivity. This issue is looked at in more detail in Chapter 2. For now, think of connectivity as something that makes it possible for you to use your microcomputer to contact other computers, anywhere in the world, even if the other machines don't have the same operating system (see Figure 1.5).

One of the things connectivity means is that other people can run programs you wrote, and you can run programs they wrote. If they decide to spread a virus, connectivity means it may infect you, or vice versa.

Connectivity also opens up some extra points of attack for people trying to put a virus into your system. Since communications is necessary for connectivity,

[4]It's much greater than being hit by lightning, though. There were 400 injuries or deaths from lightning in the US in 1987, or about 1 in 500,000. 350,000 Mac users were hit by the *MacMag* virus in 1988, about 1 in 5.

此为试读,需要完整PDF请访问: www.ertongbook.com