COMPUTER VIRUS HANDBOOK

COMPUTER VIRUS HANDBOOK

Dr Harold Joseph Highland FICS

Elsevier Advanced Technology
Mayfield House, 256 Banbury Road, Oxford OX2 7DH, UK

British Library Cataloguing in Publication Data
Highland, Harold Joseph
Computer virus handbook.
1. Computer systems: Security measures
I. Title
005.8
ISBN 0-946395-46-2

PREFACE

This book is about a low-probability but high-consequences computer security risk -- the computer virus. The chances of any system becoming infected by a computer virus is small when compared with the probability of computer fraud, accidental data errors, fire and a multitude of other risk factors. The amount of chaos and disaster a computer virus can cause however can often be greater than that caused by fraud and/or data errors.

Companies and individuals spend money on fire insurance although in many cases the probability of a fire is exceedingly small. What is wrong with providing some form of anti-virus protection? Unless one has lived through a computer virus attack he or she really has little understanding of such an event.

If your microcomputers do not have sensitive data and that data is stored only on mainframes, one can justly ask why did you need the microcomputers? Even normal company correspondence cannot be interrupted "comfortably" because of a computer virus attack. Furthermore, the probability of a computer virus attack, albeit very small, is increasing rapidly. Although most reports are from universities, this does not mean that corporations are immune. In the 60 days prior to writing this copy, I have been called upon to assist a very large corporation with hundreds of retail outlets, a major advertising agency, the research division of a government agency, a hospital, a petroleum company and several other "non-small" organizations that had infected systems.

Some computer security specialists consider the computer virus as a disease found at universities. True the highest incidence of infection has been found at these sites. Yet consider a company whose employees take courses at these universities, use the university's microcomputer facilities, and then bring their floppy disks to the office to do homework. Consider too the dedicated employee who takes work home and uses the floppy disk in a microcomputer that his/her son or daughter uses to play computer games. Consider as well the case of a university that has been plagued for months by virus infections. Their graduates have been hired by many companies in New York City. These former students bring their infected disks in to "enhance" their office microcomputers by adding some handy utilities.

A Management/Technical Approach

This book was written for management, the computer security specialist, and the microcomputer technician. It is not "the sky is falling book," forecasting doom and gloom. It was designed to provide some understanding of the computer virus problem, an evaluation of some 20 anti-virus products, some procedures to reduce the virus threat and recommendations to assist in the evaluation and selection of an anti-virus product.

* A bifurcated approach was used in writing the chapter on the history of computer viruses. There are non-technical descriptions of a number of the more common computer viruses for those who want general information. There are also detailed, technical descriptions of how these viruses work, written for the technician. The information contained is based on those viruses in my own collection supplemented by information from responsible researchers.

* **The reports from virus hunters, three individuals involved with the earliest computer viruses, is the first time each has been able to explain what happened without their words being modified or distorted by writers eager to make headlines. The articles are vicarious reading for those who never encountered a virus attack. Some publications have started such features recently, probably reflecting the great interest in mystery and spy story books.**

* **Procedures to reduce the virus threat contains some no-cost and/or low-cost methods to help any organization fend off computer virus attacks.**

* **There is also a collection of seven previously published papers selected from among the refereed papers published earlier in *Computers & Security*.**

A Guide to Product Selection

Also included in this book are a series of product reports. These reports are from two sources. First there are those from the two test centers at which the products were tested and subjected to live computer virus attacks. More important are the reports from some 50 test sites — potential users of anti-virus products or individuals involved in corporate consultation.

Several microcomputer publications have published evaluations of some of the anti-virus products These tests were done by microcomputer technicians who do not need manuals and who are thoroughly familiar with the architecture and operating systems. They are not the typical corporate user; instead they are "grosssprecherei," self-appointed experts who do not consider human factors found in the corporate world or the need for cost effectiveness.

Product testing and evaluation must follow a scientific protocol if the results and comparisons are to be meaningful. No rating scale was used in the final report in this book because each organization's needs are somewhat different. One must recognize that no program can claim to protect your microcomputer system perfectly! As Paul Mace wrote late in 1988, "that kind of nonsense is a red flag to the kooks that write these little gems. The most elaborate protection scheme can, at best, stay one step behind the latest wrinkle."

Some of the anti-virus product producers have modified their products since our evaluators tested them in 1988-1989. Nonetheless the reactions of the evaluators provide the reader with insight into the problem of considering any product for office use. These product reviews should make the reader aware of what features to look for in a product. To assist the reader further, there is also a special chapter on "Testing an Anti-Virus Product."

On the Lighter Side

Conducting the product evaluation study reported in this book had its problems considering that it involved two test centers and working with evaluators at 50 sites in the States and over the world, ranging from Australia to Sweden. I should like to share a few of the humorous (?) incidents.

Where is the Disk? — One producer provided me with about 10 copies of his product in shrink-wrapped packages which were sent to the evaluators. In less than one week we heard from

all of them. When they opened the package they found the manual and the quick-start procedure on a card. There was even a floppy disk sleeve, but there was no floppy disk.

It Must Run on an IBM! — Another producer sent a copy of his program which I tested on my Compaq 286. Dr. Jon David found that the program failed to install itself on the true-blue IBM AT he used for testing. When he called the producer he was told that either he was doing something wrong or the disk was defective. After he tested the replacement disk, which also failed, Dr. David was told by the producer that the program had been tested on IBM-clones. Because there were no problems he assumed it would work on an IBM AT!

You Do Not Have an AT? — Several evaluators received copies of one product in its shrink-wrapped package. When opened it contained only 3 1/2-inch disks but they did not have an AT.

Everyone Has a High-Density Disk Drive. — Another producer sent floppy disks but failed to indicate that the disks were high-density 1.2 megabyte disks. Many of the evaluators assumed that the disk was defective and called to receive new ones. When I called the producer he said that he used the 1.2 megabyte disks because he ran out of 5 1/4-inch floppies.

How Do I Get Rid of It? — Some of the programs tested do not have a de-install program. Since the programs created a number of files for its use [not indicated in the manual], evaluators found themselves editing the numerous files on their hard disks to determine which could be deleted after the testing was completed.

Where Were You When the Lights Went Out? — A few of the programs radically altered the AUTOEXEC.BAT and/or the CONFIG.SYS files during their installation. Three evaluators had power interruptions during the install procedure; it was not possible to reboot the system from the hard disk.

Our Next Version Eliminates That Problem! — After I installed one program on my system I rebooted the system as noted in the manual. During the start-up of the system there was a plethora of error messages on the screen. In searching for the cause I found that the program had renamed all my system drivers [and I have 11 on my system] to the identical name as the anti-virus product's driver. When I called the producer he informed me that he too had that problem but the new version, being sent, would correct this difficulty.

Acknowledgments

In some respects I served as the coordinator, filter and synthesizer of this book which is an amalgam of the efforts of many individuals and organizations whom I should like to acknowledge and to whom I wish to express my thanks. Foremost I wish to thank the 76 evaluators from 50 organizations for taking their time to test the many anti-virus products that were sent for evaluation. Unfortunately because of the company policy, a number of the evaluators cannot be publicly acknowledged. [A brief biographical sketch of some of them is contained in an Appendix in this volume.] We should also like to thank the 20 product producers for contributing their products for evaluation in this study.

Specifically I want to thank seven individuals who wrote special chapters or copy for this volume. Dr. **William J. Caelli**, FACS, head of the Information Security Research Centre of Queensland University of Technology, **Dr. Jon David** of Systems Research and Development Corporation, **Harry B. DeMaio** of Deloitte, Haskins & Sells, **William H. Murray** of Ernst and Whinney, **Yisrael Radai** of Hebrew University of Jerusalem, **Kenneth R. van Wyk** of Lehigh University, and **Ms Anne E. Webster** of the University of Delaware.

A very special thanks to **Bill Kenny** of Digital Dispatch, Inc. for his assistance in isolating the computer viruses, disassembling their code and writing the technical description of how each worked. His extensive work served as a verification of one phase of the project undertaken at the two test centers involved in this study.

Several of the evaluators provided considerably more input than others. This input at times required a review and reevaluation of some of the work done at the test centers and/or additional instructions being sent to evaluators. Some of the input provided greater insight into the design of anti-virus products and aided in developing the material for product selection. Among these evaluators are: **John Abolins** of the New Jersey Department of Environmental Protection, **Jack Anderson** of AFUTEC/SEC Office Automation and Support, **Peter P.C.H. Kingston** of Kingston, Goulbourn & Associates, **Dean Dennis Longley** at Queensland University of Technology, **Dr. Ben Shneiderman**, head of the Human-Computer Interaction Laboratory at the University of Maryland, and **Captain Gregory White** of AFCSC / SREN U.S. Air Force Cryptographic Support.

In addition I should like to thank my secretary **Ms Virginia Tantillo**, and both **Mrs Alison Saunders** and **Paul Evans** of Elsevier Science Publishers, Ltd for their assistance in the production of this book.

Finally, I must thank my wife, **Esther H. Highland**, Professor Emerita of the City University of New York and Managing Editor of *Computers & Security*, for her patience and her advice. For over a year she had to listen to my problems in connection with this book and as usual provided insight and guidance in the solution of simple and complex issues.

Dr. Harold Joseph Highland, FICS
Elmont, NY, USA August 1989

Foreword

Professor William J. Caelli
Director of the Information
Security Research Centre
Queensland University of Tech.
Brisbane, Queensland, Australia

As the world of information technology and its applications moves towards Open Systems, through the ISO's [International Standards Organisation] model and other efforts in common operating systems, such as proposed by the Open Systems Foundation [OSF], the benefits of potentially lower costs and ease of implementation will be offset against the heightened threat of attack. Not only are systems "standardized" but these very standards become widely available at low cost, worldwide.

The mass availability of the IBM Personal Computer Systems [PCs] and their "clones" has been accompanied by the mass-market, low-cost publication of the design details of the machine and its operating systems, including MS-DOS, PC-DOS, OS/2 and UNIX/XENIX. The same applies to other mass market computer systems. Such publication obviously enables normal and *illicit* usage. The problem in the 1990s then, is that this publishing will be extended to include the details of **open standards** for Electronic Data Interchange [EDI] and allied computer-to-computer messaging schemes, along with the UNIX/OSF operating system details.

This book demonstrates the simple fact that enthusiastic people will donate their time willingly to the pursuit of new ways to defend computer systems. The "enthusiasts" know no national boundary as a quick scan of the book will verify. The PC has become a worldwide commodity.

In addition, the PC's computational power, along with its incorporation into large scale information systems and data networks, has grown by orders of magnitude. The computer virus, along with its cousins — worms, Trojan horses and the like — have thus become an international and pressing challenge to information systems in the 1990s.

The problem is also that the virus developer may no longer be content with attacking small and personal systems but may increasingly move to medium and large scale, shared computer systems and interlinked workstations. The 1988 Internet "worm" attack demonstrates that the problem is shared by multi-user, distributed computer networks based around medium performance computer systems.

In The 1990s

The market for car theft alarms and household security technology exploded in the late 1980s. In the computer industry the days of implicit protection because of a lack of knowledge by the general public, have gone. Computer programming has become a primary school topic in many countries. Computer operating systems and structures are taught in high school.

In the 1990s, the designer and developer of an information system is faced with the simple fact that the system will be used, or abused, by a computer-literate population. In particular, the employees of the organisation that depends upon the information system, often for its very existence, will own a computer similar or identical to the one used at work as a network-linked workstation.

Thus, so-called "insider" attacks become a major threat, e.g. through the insertion of a virus or worm into the workstation and then the network. Protection must now be extended from the main host computers, through the network, to the workstation.

The main tool for protection is cryptography. This art and science of "scrambling" presents a set of tools to enable "locks" and "alarms" to be set up in the workstation and network. The incorporation of encryption schemes in the workstation and network could prevent the insertion of **unauthorized** programs [viruses] into workstation or networks.

For example, the incorporation of encryption hardware and user authentication technology into a workstation could be used to force a **single point** for the distribution of software. The security manager for a corporate information network may be responsible for the distribution of all software to user workstations or its provision in a program library at a central host computer. Any software must now be **encrypted** by the security manager, using so-called "keys" which are secret and known only to the security manager or his or her **security workstation**, before being usable in the network environment. For example, the security manager may now distribute encrypted diskettes for use in corporate workstations.

The hardware incorporated in the workstation decrypts [unscrambles] the programs and/or data prior to usage. Now if an employee, for example, brings in a diskette from home or from anywhere else, the workstation will not recognise it and will reject it. Incidentally, this also prevents data and programs from being taken from the workstation on diskettes or cartridges, etc. Even though a diskette itself may be removed the information it contains will be scrambled using the corporate "key" known only to the security manager. Thus, if the user tries to read the information on another system then the information will appear as undecipherable "gibberish."

While cryptography presents a technology that, if sensibly employed, can protect a network or alert users of illicit program entry to a reasonable level, the problem is one of management acceptance of the costs involved. Good car and burglar alarms cost money. The same applies to good information security products and services. However, if management applies a "risk assessment" program to corporate information resources, as it does to the company's physical resources, then the cost of incorporation of security technology can be assessed against a quantified risk.

In the future it is likely that manufacturers of computer and data communications equipment will

incorporate such security technology into their products from the design phase upwards. Personal computer-based workstations may contain **user authentication technology**, such as "smart card" readers and user "log-in" procedures, and high performance encryption hardware incorporated into magnetic media devices such as diskette and cartridge drives.

Professor Bill Caelli, Director of the Information Security Research Centre at Queensland University of Technology and winner of the 1986 Australian Information Technology Award for Achievement in the Information Technology Industry, has over 24 years' experience in the computer industry. He received his first degree in science from the University of Newcastle [New South Wales] in 1966 following some years of experience in computer programming and systems analysis for the Broken Hill Pty. Ltd., Australia's largest private company. In this role he worked with early IBM computer systems [1401, 1620, 650] and punched card based equipment in the development of commercial and technical applications for payroll, product and mill scheduling and related systems.

In 1966 he joined the Australian National University [A.N.U.] to work on computer systems related to high speed data acquisition and data storage for the Department of Nuclear Physics. During this time he designed and wrote a real-time operating system for the IBM 1800 computer system which included support for an early high speed, multi-host local computer network. In 1972 he received his Ph.D. degree from the A.N.U.

Professor Caelli joined Hewlett-Packard (Australia) Pty. Ltd. in 1972 as a Senior Computer Consultant with particular responsibility for the newly announced HP-3000 system. His major work involved the creation of database systems [IMAGE] and work with the Codasyl model for databases as well as in data communications.

In 1973 he joined Control Data [Australia] Pty. Ltd. to further work on large scale database systems and data networks and while with CDA became interested in problems of data security and cryptography. He served on a number of CDC corporate committees related to advanced database systems in Australia and in the U.S. as well as working with database standards development groups and with Control Data's Australian Federal Government marketing group.

In 1979 he left Control Data and with a U.S. partner formed Electronics Research Australia, now ERACOM Pty. Ltd., to develop a range of small to medium computer systems based around Stanford University Network [SUN] workstation concepts and data security products. He is currently Technical Director of ERACOM and in July 1988 he also became the Director of the Information Security Research Centre at the Queensland University of Technology.

Professor Caelli has been an active member of the Australian Computer Society [ACS] since its inception and was made a Fellow of the Society in 1981. He is a well known commentator on the computer industry and on data security and has published numerous papers on technical topics as well as on the social and economic implications of the technology. His first book, "The Microcomputer Revolution," was published by the ACS in 1979.

He is the Chairman of, and Australian representative on, IFIP [International Federation for Information Processing] Technical Committee 11 [Security and Protection in Information Processing Systems]. He also serves on the Standards Association of Australia's Committee on E.F.T.S. security standards and has lectured widely to national and international groups on information systems security.

Professor Caelli's research interests are in computer architecture for "broad-grain" parallel systems and their use in large scale message switches, in object-oriented languages and programming systems, and in computer and network security.

CONTENTS