The Complete Computer Virus Handbook

Price Waterhouse

ISSUE 2 SEPTEMBER 1989

The Complete Computer Virus Handbook

Price Waterhouse

Pitman

PITMAN PUBLISHING
128 Long Acre, London WC2E 9AN

A Division of Longman Group UK Limited

First published in Great Britain 1989
Reprinted with corrections 1990
Reprinted 1990 (twice)

ISBN 0 273 03255 0

Printed and bound in Great Britain by
Biddles Ltd, Guildford and King's Lynn

THE COMPLETE
COMPUTER VIRUS
HANDBOOK

THE COMPLETE COMPUTER VIRUS HANDBOOK

PREFACE

Welcome to the second edition of this handbook. This edition contains details of the initial research and investigations that we carried out during the summer of 1988 together with our more recent research and investigations. This edition of the handbook has been updated with :

- expansion of MS-DOS technical details and new sections on OS/2 and MACINTOSH systems
- information of new viruses
- update on anti-virus software products
- evaluation of the role of insurance
- explanation of the legal issues

I am confident that you will find the explanation of different aspects of the virus threat interesting and useful. We have addressed how you can be attacked and possible defensive methods including prevention, detection and removal.

As computer viruses become increasingly sophisticated and new viruses are being discovered, the problem of prevention, detection and recovery from a virus attack is of more importance. Therefore we believe that if you are contemplating purchasing an anti-virus product you should seek specific advice upon your objectives and the current products available. Our evaluation of the anti-virus products can only be considered against the background of the viruses known to us at the time when the evaluation was undertaken.

David Frost

9350 116

September 1989

Price Waterhouse

THE COMPLETE
COMPUTER VIRUS
HANDBOOK

ABOUT THE AUTHORS

DAVID FROST

David is responsible for computer audit work on a number of international clients. He has a comprehensive knowledge of computer systems and his experience includes many detailed data security reviews. He leads our corporate disaster recovery services team.

David is 43 years old and was admitted to the partnership in 1983. For many years he has been a partner in our UK specialist computer audit practice. His experience has included a period in industry and he is actively involved in the Computer Service Association Data Privacy Working Party.

IAN BEALE

Ian is a managing consultant within the Price Waterhouse computer audit and data security group, where he has played a leading role in the development of the worldwide Price Waterhouse Data Security Methodology. He has given training courses to clients in the UK and Europe on the methodology and practice of data security, and has lectured at INSEAD in France and at Loughborough University in the UK.

His experience covers all aspects of computer audit and data security in a range of system and business environments. He has gained experience working for major computer suppliers (IBM, ICL, Data General, NCR).

Ian is 33 years old, and a member of the EDPAA. He joined the Price Waterhouse computer audit group in January 1984.

September 1989 *Price Waterhouse*

CHRIS FROST

Chris is a senior consultant in the Price Waterhouse computer audit and data security group, who has over nine years experience in the installation, operation and management of database systems and associated operating system environments, combined with a strong system programming background. During this time, Chris has specialised in the security aspects involved, ranging from physical site security to access control systems. He lectures frequently to senior management and end users on a range of security issues.

Chris is 33 years old, and joined Price Waterhouse in May 1986. Prior to that he worked for NATO in Luxembourg, Clayton Devandre Holdings Ltd and CGS Ltd.

oOOoo

We also acknowledge the assistance which Richard Dedman, a partner in Barlow, Lyde and Gilbert, has provided. Richard, a solicitor and practitioner in information technology law, kindly wrote the section describing how the law can help a victim of a virus attack.

oOOoo

The following people have kindly supplied details of viruses to us and their help is greatly appreciated:

David Ferbrache - Heriot-Watt University Computer Department, Joe Hirst - Brighton based technical programmer, Klaus Brunnstein - Hamburg, Jim Goodwin - Homebase bulletin board, Dr Alan Solomon - Chairman of the IBM PC User Group.

THE COMPLETE
COMPUTER VIRUS
HANDBOOK

THE COMPLETE COMPUTER VIRUS HANDBOOK

CONTENTS

Page

Introduction 1
Definition Of Terms 3
Risks Posed By Viruses 5
Sources Of Viruses 7
How Can Viruses Get Into Systems? 12
Analysis Of Virus Sources 14
Virus Symptoms 16
Tools Used By MS-DOS Virus Programmers 17
    The Future: 0S/2-286 25
    The Future: OS/2-386 27
    The Macintosh Operating System 28
How Can Viruses Be Prevented? 34
How Can Viruses Be Removed? 36
How Can The Law Help? 38
Insurance Coverage Against Viruses Attacks 49
How Can Price Waterhouse Help? 50

Appendix

Computer Viruses I
Anti - Virus Product Evaluation II
    MS - DOS
    MACINTOSH
Glossary of Terms III
DOS Interrupts IV
References V

September 1989

Price Waterhouse

THE COMPLETE COMPUTER VIRUS HANDBOOK

INTRODUCTION

During 1988 there were a large number of articles in the press describing a new type of security problem to computer users. As a result of the increasing interest in the issue, Price Waterhouse investigated the threat to computer systems which has become known as the "computer virus". During October 1988 we published the first edition of "The Complete Computer Virus Handbook". The handbook provided an objective view of the virus problem and included detailed appendices describing viruses and anti-virus software. The first edition was extremely popular and we are pleased that interest in the handbook has continued.

Since our initial research, carried out in 1988, the virus threat has constantly developed and changed. New viruses have been reported, and new/enhanced anti-virus products have been developed. This edition contains details of all viruses known to us and an evaluation of the latest available version of all vaccine products known to us.

Our definition of a computer virus states that a virus is computer code usually designed to carry out two tasks: Firstly the virus is designed to replicate itself from one computer system to another. Secondly, the computer virus is designed to locate itself within a computer system in such a way as to make it possible for it to amend/destroy programs and data files, by interfering with the normal processes of the operating system.

The Price Waterhouse team based in the London office have examined reported computer viruses from around the world and evaluated a large number of anti-virus products. In addition, we have proposed a methodology which will help to reduce the risk of exposure to computer viruses.

Our detailed commentary on each anti-virus product is contained in Appendix II. Our evaluation method included reviewing available technical documentation and supplementing this by discussions with the supplier. Where possible we also carried out hands on evaluation of the product. The method(s) used are summarised in Appendix II.

While we have made every effort to ensure the accuracy of our evaluation, we have in a number of cases relied on information supplied to us. In addition, as anti-virus products are constantly being updated to deal with new virus threats, there is a risk that by the time this book is published at least some of our reviews will be out-of-date. We recommend that anyone attempting to select an anti-virus product should contact the suppliers before a final decision is made. We have recorded the date of our evaluation and, where applicable, the version number of the software.

For this research to continue to be effective, Price Waterhouse need both details of virus attacks and copies of computer virus software, so that anti-virus software can be properly evaluated and techniques used by virus writers can be monitored. Details of anti-virus products and copies of the software are also needed.

If you would like to help, please send either details of an attack or copies of virus software and vaccines, (clearly marked "virus" if necessary) to

David Frost
Price Waterhouse
No 1 London Bridge
London
SE1 9QL Telephone 01-378 7200

Confidentiality will be respected

Details of new viruses and vaccines examined will be published in future editions of this handbook.

DEFINITION OF TERMS

Software threats to computer systems may originate from a wide variety of sources and can be classified into a number of categories. The following describes the most common type of threat :

Virus

A virus is a computer program that spreads from one system to another, eventually performing the illicit function for which it was designed. Each reproduced virus code works independently of the initial virus.

Worm

This term is often used interchangeably with virus. A worm is a software program that generally "burrows" into the computer's memory. The worm is designed to search for idle computer memory, it then rewrites itself successively through the computer's memory until the system crashes. The worm differs from the computer virus in that the recurring segments of the program maintain communication with the segment from which they were created.

Trojan Horse

A Trojan horse is a section of code hidden within a legitimate program. The Trojan horse does not possess the ability to replicate itself. The unauthorised code may or may not direct the legitimate program to cause damage to the system. The Trojan horse may be activated immediately or may continue to operate as legitimate software for an extended period of time before activating itself.

Time Bomb

A logic bomb or a time bomb is a set of instructions that is executed in conjunction with a predetermined event. The "trigger" is often a specific date or time (e.g. April Fool's Day, Friday the 13th), but may be any event (e.g. a counter reaching a predetermined number). A virus or Trojan horse may contain a logic bomb.

Anti-Virus Programs

Within this handbook Price Waterhouse have used the system of classification of anti-virus programs proposed by the Computer Virus Industry Association (CVIA). The CVIA is a group formed by nine software suppliers specialising in anti-virus programs in the United States.

- **Class I**: Infection prevention designed to stop the virus replication process and prevent initial "infection" (does not apply to hardware infection prevention products).
- **Class II**: Infection detection, designed to pick up virus attacks soon after they happen, mark the specific component(s) infected and allow action to be taken. This class is more difficult to circumvent initially.
- **Class III**: Infection identification product des ed to report the specific types of strain of virus which is present. It will identify viruses in systems and remove them - but only works on known viruses.

RISKS POSED BY VIRUSES

The range of threats posed by viruses and the primary impact of a virus attack can be broadly classified into the following types:

Destructive Viruses

Massive destruction Attacks the format of disks whereby any program or data damage will not be recoverable.

Partial destruction Erasure and modification of a specific portion of a disk affecting any files stored in that portion.

Selective destruction Erasure and modification of specific files or file groups.

Random havoc Randomly changing data on disk or in memory during normal program execution, or changing key stroke values, or data from other input/output devices.

Network saturation Systematically using up computer memory or space to impede performance or cause the system to crash.

Non-destructive Viruses

Annoyance Displaying messages, changing display colours, changing key stroke values (e.g. changing the effect of the SHIFT/UNSHIFT keys), deleting characters displayed on a visual display.

Secondary Impact Of A Virus Attack

The most significant secondary effects of a virus are those that involve lost productivity. In any organisation or computer site affected by computer viruses, computer support personnel will be involved with the task of dealing with the problem, while management time may be required to formulate procedures which will prevent future virus problems and reassure affected customers/suppliers.

The tasks carried out by support personnel after discovery of a virus would typically include :

- Identification of virus
- Assessment of impact on programs and data
- Assessment of impact on customers, suppliers, and staff
- Development of software to remove virus code from the system
- Recovery of lost or damaged programs and/or data files
- Discovering how the virus code entered the system
- Evaluation and implementation of anti-virus products and procedures to prevent future attacks.

Recent reports have shown that software houses are also vulnerable to virus threats. The impact of such attacks will be magnified if the attack is only detected after copies of their product are shipped to suppliers and subsequently sold. The risk then arises that copies of their product could be affected by virus code and that the virus could be passed on to their customers, with the very real possibility that affected customers could sue for damages which have arisen from using the software. The consequences of such an attack could therefore have a serious impact upon the future viability of a software house and its reputation in the market place.

SOURCES OF VIRUSES

To date, the major threat posed by computer viruses is to microcomputer systems. Experimental work has shown that it is possible to create viruses capable of infecting minicomputer systems. However, it is generally believed that compared with the threat posed to microcomputer systems, the threat to either minicomputer systems or mainframe systems is not as significant at the moment although such systems when connected to a telecommunications network,or if microcomputers are linked to them are still vulnerable to attack. We have included details of a number of viruses which have affected minicomputer and mainframe systems.

This may be the case but two incidents in 1988 give further cause for alarm. The first relates to the programmer in Texas USA who managed to destroy a large number of data records on his previous employer's computer after he had been dismissed. Although he received a jail sentence, it cost the company considerable time, effort and money to rebuild their files. Although this is not an example of a computer virus it does show the sort of damage that could be inflicted on a mainframe computer if it were to be infected. Also this sort of publicity is certain to provide the authors of virus programs with the incentive and the challenge of infecting mainframe computers.

The second disturbing incident related to an attempted Eurobond fraud and to the comment in a number of press reports that it may have been the work of organised crime. If this is true, it may herald the start of the interest of "organised crime" in computer systems, then we would indeed have a very much bigger threat looming on the not too distant horizon.

Home Grown Versus Imported Viruses

Viruses have two principal methods of infecting a system. A virus may be introduced into a corporate computer system or network by a legitimate user who physically places an infected program into production either knowingly or unknowingly. A non-legitimate user could also deliberately introduce a virus in this way. Alternatively, a virus may be carried to a system via a telecommunications link with another system that has already been infected or by "uploading" software from a microcomputer connected to the system.

Microcomputers Versus Mainframes/Minicomputers

The greatest incidence of viruses has been in microcomputers. The proliferation of microcomputers has created an environment in which computer viruses can grow freely. Many of the tested and reliable controls that have been developed for information processing are not available or have been abandoned by microcomputer users. The development of a user-friendly environment, a leading contributor to the widespread acceptance of microcomputer technology, has created an environment that does not require a significant investment of management resources. Users are left to control the environment on their own. Recently, however, this situation has begun to change. Management is beginning to realise the dangers involved in the uncontrolled decentralisation of information processing.

An additional consideration contributing to the rapid growth of computer viruses in the microcomputer environment has been the free sharing of programs ("shareware") among microcomputer users. The practice of sharing computer software, either through legitimate bulletin board services or illegal software "pirating", is one of the principal methods of virus transmission. The use of electronic bulletin board services, while providing numerous benefits to consumers of microcomputer products and contributing to the free flow of information, carries with it the risk of receiving tainted software.

The microcomputer environment also has the added complication that, due to the limitations of the microcomputer operating systems, personal computers typically operate as single-state machines. Unlike mainframe and minicomputers, microcomputers typically do not have the internal hardware and software controls which protect application programs from one another nor the operating system from application programs. Mainframe and minicomputer systems have had these types of controls since the late 1960's. In the microcomputer environment it is possible, and fairly common, for application software to dynamically modify the operating system or application programs. In the case of a computer virus, the malicious software can use these weaknesses to affect other programs or modify the operating system.

The microcomputer market is dominated by IBM or IBM compatible computers. Therefore a virus which is written to operate on an IBM microcomputer can potentially affect a huge number of systems. Similarly there are large numbers of Macintosh microcomputers and again a single virus can therefore, without modification, potentially affect each of these systems. The absence of such a single dominant operating system running on thousands of mainframe computers may be another reason why mainframe based viruses have not appeared as frequently. A virus would need to be modified to operate on each type of mainframe.

Although the occurrences of viruses in minicomputer and mainframe systems have been low compared to the microcomputer environment, the potential for damage is far greater. In contrast to the user-friendly microcomputer environment, the minicomputer and mainframe environments require a greater degree of technical ability in order to operate the systems. As such, the knowledge of the systems resides with a group of technical staff (e.g. systems programmers) who typically have access to systems manager privileges or sensitive utilities and thus are capable of writing malicious programs, introducing trapdoors, or otherwise bypassing the security system - without management's knowledge. This is why hackers try to obtain systems manager privileges as the first point of attack.

Mainframe operating systems have for many years been designed to keep one users program separate from another. The operating system is usually protected from direct access by the user program. These functions have the by-product of making a virus more technically complicated to write and more difficult to use to cause damage.

Another area of great concern for users of minicomputer and mainframe systems are the communication links that connect their systems to the outside world. A virus may spread from the high-risk microcomputer environment to the minicomputer or mainframe via this type of connectivity. The availability of dial-in access to the computer system opens the system up to a host of dangers. A hacker, located anywhere in the world, has greater potential, with dial-up facilities, to plant a virus in a system if the virus program can somehow be entered into the system and executed. The virus program can be executed in one of two ways: firstly, the virus can be executed by the intruder if the privilege to run programs has been obtained or secondly the intruder can disguise the virus