# CONTENTS

ALLNET'S LEGAL PROBLEMS ........ 2
A SOLUTION TO VIRUSES ........ 4
HOW TO WRITE A VIRUS ........ 8
BUILDING A RED BOX ........ 13
REPLY TO CAPTAIN ZAP ........ 16
LETTERS ........ 24
2600 MARKETPLACE ........ 41
FUN PHONE NUMBERS ........ 44

SECOND CLASS POSTAGE
Permit Pending at
East Setauket, N.Y.
11733
ISSN 0749-3851

**2600 Magazine**
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

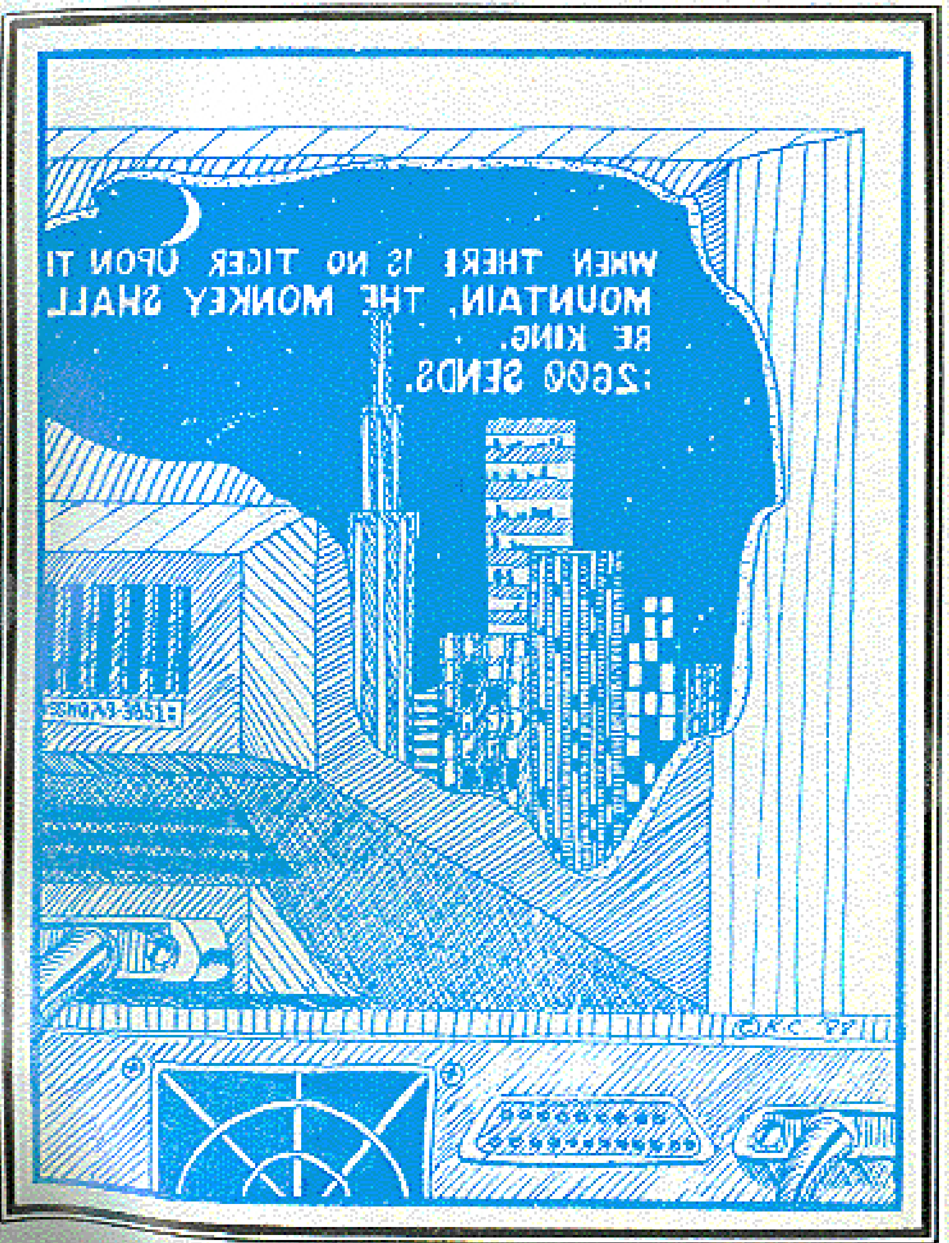
DANGER:
MISSING LABEL

---

# 2600

The Hacker Quarterly

Volume 5, Number 2
Summer, 1988



WHEN THERE IS NO TIGER UPON IT
MOUNTAIN, THE MONKEY SHALL
BE KING.
:2600 SENDS.

## IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MICHIGAN
## SOUTHERN DIVISION

IN RE LONG DISTANCE TELECOMMUNICATIONS LITIGATION

MDL Docket No. 558
All Cases
Hon. Anna Diggs Taylor

### NOTICE OF CLASS ACTION AND PROPOSED SETTLEMENT TO CERTAIN CURRENT AND FORMER CUSTOMERS OF ALLNET COMMUNICATION SERVICES, INC.

By Order of the United States District Court for the Eastern District of Michigan, PLEASE TAKE NOTICE THAT:

A class action lawsuit has been filed on behalf of certain former and current customers against Allnet Communication Services, Inc. (formerly known as Combined Network, Inc.). The Court has preliminarily approved a settlement of this lawsuit.

YOU ARE URGED TO READ THIS NOTICE CAREFULLY BECAUSE IT AFFECTS YOUR RIGHTS AND WILL BE BINDING ON YOU IN THE FUTURE.

**I. NOTICE OF A PENDING CLASS ACTION**

**A. Description of the Lawsuit**

Plaintiffs have sued Allnet, alleging that Allnet charged customers for certain unanswered telephone calls, including time, busy signals, and central office recordings (collectively "unanswered calls") without adequately disclosing such charges to their customers or the public. Plaintiffs seek to present their own claims for charges for unanswered calls, as well as the claims of other current and former Allnet customers for similar charges.

Allnet denies the violations alleged by plaintiffs and contends that at all times Allnet has charged its subscribers fairly and properly and has disclosed fully and fairly the basis for its long distance charges. Allnet has agreed to settle Plaintiffs' suit solely to avoid the expense, inconvenience and disruption of further litigation.

This Notice is not an expression of any opinion by the Court of the merits of this litigation or of the Settlement Agreement.

The Complaint, the Settlement Agreement and other pleadings in this case may be inspected during normal business hours at the office of the Clerk of the United States District Court for the Eastern District of Michigan, 231 West Lafayette Boulevard, Detroit, Michigan 48226.

**B. The Settlement Class.**

Plaintiffs and Allnet have entered into a Settlement Agreement, which has been preliminarily approved by the Court. Under the terms of the Settlement Agreement, the parties have agreed, for purposes of settlement only, that this suit has been brought on behalf of the following class of persons similarly situated to Plaintiffs (the "Class"):

All persons and entities that subscribed to and utilized the long distance telephone service of Allnet or its predecessor, Combined Network, Inc. (referred to collectively as "Allnet"), at any time during the period March 2, 1981 through December 31, 1985.

**C. How to Remain a Class Member.**

If you were a subscriber to and utilized Allnet's long distance telephone service at any time during the period March 2, 1981 through December 31, 1985, you are a member of the Class. If you choose to remain a member of the Class, you may participate in this settlement and you will be bound by the results of the settlement and/or the lawsuit.

**D. How to Exclude Yourself From the Class.**

You are not required to be a member of the Class. Should you decide that you do not want to be a member of the Class, you must send an exclusion notice that states your name, current address, and your desire to be excluded from the Class to the Clerk of the United States District Court for the Eastern District of Michigan at the address given at the end of this Notice, postmarked no later than June 18, 1988. If you choose to be excluded from the Class, you may not participate in the settlement. You will not, however, be bound by any judgment dismissing this action and you will remain free to pursue on your own behalf any legal rights you may have.

**II. TERMS OF THE SETTLEMENT**

The Settlement Agreement requires Allnet to provide to class members long distance telephone credits up to a maximum of $525,000 (the "Settlement Credits") and cash refunds up to a maximum of $75,000 (the "Cash Refunds"). These benefits are available to Class members who properly complete and file a Proof of Claim in the manner described in Section III below. Class members may choose one benefit from the following options:

- A. A standardized credit toward Allnet long distance telephone service of 50 cents for each year from 1981 through 1985 in which the Class member: (i) was an Allnet customer; and (ii) claims that she/he was charged by Allnet for unanswered calls; or
- B. A standardized cash refund of 50 cents for each year from 1981 through 1985 in which the Class member: (i) was an Allnet customer; and (ii) claims that she/he was charged by Allnet for unanswered calls; or
- C. An itemized credit toward Allnet long distance telephone service of 30 cents for each minute of unanswered calls for which the Class member was charged during the Class Period (March 2, 1981 through December 31, 1985) and for which the Class member has not been previously reimbursed or credited; or
- D. An itemized cash refund of 30 cents for each minute of unanswered calls for which the Class member was charged during the Class period (March 2, 1981 through December 31, 1985) and for which the Class member has not been previously reimbursed or credited.

To obtain an itemized credit or cash refund, the Class member must itemize and attest to each unanswered call for which a refund or credit is claimed. If the total credits claimed by Class members exceed $525,000, each Class member claiming Settlement Credits will receive his/her/its pro rata share of the total Settlement Credits available. If the total cash refunds claimed by Class members exceed $75,000, each Class member claiming a Cash Refund will receive his/her/its pro rata share of the total Cash Refunds available.

Class members need not be current Allnet customers to claim the standardized and itemized credits. Allnet will automatically open an account for any Class member who requests credits and executes an authorization to open such an account. If a Class member incurs a local telephone company service charge in connection with the opening of an Allnet account, Allnet will issue a credit to the Class member's account for the full amount of such service charge upon receipt of the local telephone company's bill for the service charge. Allnet is not responsible for any other service charge that a local telephone company may impose for ordering, using or terminating Allnet service.

The Settlement Agreement requires Allnet to pay the costs of giving this Notice (up to a maximum of $240,000) and of administering the settlement described above.

The Settlement Agreement further provides that upon final approval of the settlement, the Court will enter a judgment dismissing with prejudice all claims of plaintiffs and members of the Class that have been or might have been asserted in this action or relate to Allnet's billing and disclosure practices for unanswered calls.

Counsel for the Class have investigated the facts and circumstances regarding the claims against Allnet and their defenses. In view of these circumstances, counsel for the Class have concluded that this Settlement Agreement is fair and reasonable and in the best interests of the Class.

**III. HOW TO FILE A PROOF OF CLAIM**

To receive Settlement Credits or a Cash Refund, you must provide all of the information requested in the Proof of Claim at the end of this Notice and return it to the Clerk of the Court at the address indicated below, postmarked no later than July 28, 1988. The Proof of Claim must be signed by the Class member or, if the Class member is not an individual, an authorized representative. All claims are subject to confirmation and approval. PLEASE FILL OUT THE CLAIM FORM CAREFULLY.

**IV. NOTICE OF SETTLEMENT HEARING**

A settlement hearing will be held on June 28, 1988 before the Honorable Judge Anna Diggs Taylor, United States Courthouse, in Courtroom 737 at 231 West Lafayette Boulevard, Detroit, Michigan. The purpose of the Hearing is to determine whether the Settlement Agreement should be approved and confirmed by the Court as fair, reasonable, and adequate.

At the settlement hearing, counsel for the Class shall petition the Court for an award of attorneys' fees and expenses not to exceed $100,000. Allnet has agreed not to oppose this petition. In addition, Allnet has agreed to reimburse plaintiffs' counsel for up to an additional $15,000 for fees and expenses incurred in monitoring the settlement. These fees and expenses shall not reduce any of the Settlement Credits or Cash Refunds available to Class members.

Any Class member wishing to appear and be heard at the Settlement Hearing must file a notice of intention to appear with the Clerk of the Court, which notice must be postmarked no later than June 18, 1988. If such Class member objects to any one or more terms of the Settlement Agreement, the notice of intention to appear must be accompanied by a statement of the basis for this objection. A Class member may also object to the Settlement Agreement without personally appearing at the Hearing by filing written objections to the Settlement with the Clerk of the Court no later than June 18, 1988. A copy of the objections in any case must also be served upon lead counsel for the plaintiff class, Sachnoff Weaver & Rubenstein, Ltd., Attention: Allnet Settlement, 30 South Wacker Drive, Suite 2900, Chicago, Illinois 60606. You will not be heard at the Hearing or entitled to contest the Proposed Settlement unless you file and serve your objections in accordance with the foregoing instructions.

**V. IF YOU HAVE ANY QUESTIONS ABOUT THIS NOTICE OR THIS LAWSUIT**

If you have any questions about this Notice, the attached Proof of Claim, the lawsuit or the Settlement, you may write to Allnet Settlement, P. O. Box 277, Franklin, Michigan [illegible].

**NO TELEPHONE CALLS CONCERNING THIS NOTICE SHOULD BE MADE TO ALLNET, COUNSEL FOR PLAINTIFFS, OR THE COURT.**

(continued on page 42)

*We think you'll find this issue to be most informative and educational. At last we've devoted some space to the subject of computer viruses.*

*But we've done it in a way no other magazine has yet done. For the first time, you can read what goes through the mind of someone who deliberately plants viruses in computer systems. And you can also see what measures are being taken to thwart this person's efforts.*

*We're happy to announce yet another 2600 computer bulletin board, this one in the Washington DC area. This one is PC-Pursuitable and you can reach it at (703) 823-6591. Hopefully, we'll expand to the west coast by next issue.*

*Remember that 2600 meetings now take place on the first Friday of the month only. See page 41 for details. Turnout has been quite good in recent months.*

---

## STAFFBOX

**Editor-In-Chief**
Emmanuel Goldstein

| **Office Manager** | **Production** | **Cover Art** |
|---|---|---|
| Bobby Arwatt | Mike DeVoursney | Ken Copel |

**Writers:** Eric Corley, John Drake, Mr. French, Chester Holmes, Lex Luthor, Phantom Phreaker, Bill from RNOC, David Ruderman, Bernie S., Silent Switchman, Mike Yuhas, and the usual anonymous bunch.

---

**2600** *(ISSN 0749-3851) is published monthly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit pending at Setauket, New York.*

**POSTMASTER:** Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright © 1988, 2600 Enterprises Inc.

Yearly subscription: U.S. and Canada —$15 individual, $40 corporate.
Overseas—$25 individual, $55 corporate.
Back issues available for 1984, 1985, 1986, 1987 at $25 per year, $30 per year overseas.
**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:** *2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:** *2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
*2600* Office Line: 516-751-2600
BBS #1 (OSUNY): 914-725-4060
BBS #2 (CENTRAL OFFICE): 914-234-3260
BBS #3 (YOYODYNE): 402-564-4518
BBS #4 (BEEHIVE): 703-823-6591
USENET ADDRESS: 2600@dasys1.UUCP
ARPANET ADDRESS: phri!dasys1!2600@nyu

# A Form of Protection For You and Your Computer

by Ross M. Greenberg

### What is a Trojan?

Back in the good old days (before there were computers), there was this bunch of soldiers who had no chance of beating a superior force or of even making it into their fortress. They had this nifty idea: present the other side with a gift. Once the gift had been accepted, soldiers hiding within the gift would sneak out and overtake the enemy from within.

We can only think of the intellectual giants of the day who would accept a gift large enough to house enemy soldiers without checking its contents. Obviously, they had little opportunity to watch old World War II movies to see the same device used over and over again.

Consider the types of people who would be thrilled at the concept of owning their own rough hewn, large wooden horse! Perhaps they wanted to be the first one on their block, or something silly like that.

Anyway, you're all aware of the story of The Trojan Horse.

Bringing ourselves a bit closer to the reality we've all grown to know and love, there's a modern day equivalent: getting a gift from your BBS or user group which contains a little gem which will attack your hard disk, destroying whatever data it contains.

In order to understand how a potentially useful program can cause such damage when corrupted by some misguided soul, it's useful to understand how your disk works, and how absurdly easy it is to cause damage to the data contained thereon. So, a brief technical discussion of the operation of your disk is in order. For those who aren't concerned, turn the page or something.

Data is preserved on a disk in a variety of different physical ways having to do with how the data is encoding in the actual recording of that data. The actual *structure* of that data, however, is the same between MS-DOS machines. Other operating systems have a different structure, but that doesn't concern us now.

Each disk has a number of "tracks". These are sometimes called cylinders from the old type IBMers. These are the same people who call hard disks DASDs (Direct Access Storage Devices), so we can safely ignore their techno-speak, and just call them tracks. Tracks can be thought of as the individual little grooves on an audio record, sort of.

Anyway, each track is subdivided into a number of sectors. Each track has the same number of sectors. Tracks are numbered, as are sectors. Any given area on the disk can be accessed if a request is made to read or write data into or out of Track-X, Sector Y. The read or write command is given to the disk controller, which is an interface between the computer itself and the hard disk. The controller figures out what commands to send to the hard disk, the hard disk responds and the data is read or written as directed.

> *"Typical Trojan programs cause damage to your data, and were designed to do so by the worms who writhe in delight at causing this damage."*

The first track on the hard disk typically will contain a small program which is read from the hard disk and executed when you first power up your machine. The power up sequence is called "booting" your machine, and therefore the first track is known as the "boot track".

In order to read information from your disk in a logical sequence, there has to be some sort of index. An unusual index method was selected for MS-DOS. Imagine going to the card index in a library, looking up the title you desire, and getting a place in another index which tells you where on the racks the book is stored. Now, when you read the book, you discover that only the first chapter of the book is there. In order to find the next chapter of the book, you have to go back to that middle index, which tells you where the next chapter is stored. This process continues until you get to the end of the book.

Sounds pretty convoluted, right? You bet! However, this is pretty much how MS-DOS does its "cataloguing" of files.

The directory structure of MS-DOS allows for you to look up an item called the "first cluster". A cluster represents a set of contiguous ("touching or in contact" according to Random House) tracks and sectors. It is the smallest amount of information which the file structure of MS-DOS knows how to read or write.

Based on the first cluster number as stored in the directory, the first portion of a file can be read. When the information contained therein is exhausted, MS-DOS goes to that secondary index for a pointer to the next cluster. That index is called the File Allocation Table, commonly abbreviated to "FAT". The FAT contains an entry for each cluster on the disk. An FAT entry can have a few values: ones which indicate that the cluster is unused, another which indicates that the associated cluster has been damaged somehow and that it should be marked as a "bad cluster", and a pointer to the next cluster for a given file. This allows for what is called a linked list: once you start looking up clusters associated with a given file, each FAT entry tells you what the next cluster is. At the end of the linked list is a special indicator which indicates that there are no more clusters associated with the file.

There are actually two copies of the FAT stored on your disk, but no one really knows what the second copy was intended for. Often, if the first copy of the FAT is corrupted for some reason, a clever programmer could recover information from the second copy to restore to the primary FAT. These clever programmers can be called "hackers", and should not be confused with the thieves who break into computer systems and steal things, or the "worms" [Joanne Dow gets credit for *that* phrase!] who would get joy out of causing you heartache!

But that heartache is exactly what can happen if the directory (which contains the pointer to the first cluster a file uses), the FAT (which contains that linked list to other areas on the disk which the file uses), or other areas of the disk get corrupted.

And that's what the little worms who create Trojan programs do: they cause what at first appears to be a useful pro-

*(continued on next page)*

# Protecting Yourself From Infection

gram to eventually corrupt the important parts of your disk. This can be as simple as changing a few bytes of data, or can include wiping entire tracks clean.

Not all programs which write to your hard disk are bad ones, obviously. Your word processor, spreadsheet, database, and utility programs have to write to the hard disk. Some of the DOS programs (such as FORMAT), if used improperly, can also erase portions of your hard disk causing you massive amounts of grief. You'd be surprised what damage the simple "DEL" command can do with just a simple typo.

But what defines a Trojan program is its delivery mechanism: the fact that you're running something you didn't expect. Typical Trojan programs cause damage to your data, and were designed to do so by the worms who writhe in delight at causing this damage. May they rot in hell -- a mind is a terrible thing to waste!

Considering the personality required to cause such damage, you can rest assured that they have few friends, and even their mother doesn't like to be in the same room with them. They sit back and chortle about the damage they do with a few other lowly worms. This is their entire social universe. You should pity them. I know that I do.

### What is a Virus?

Trojan programs are but a delivery mechanism, as stated above. They can be implemented in a clever manner, so that they only trigger the malicious part on a certain date, when your disk contains certain information or whatever. However they're coded, though, they typically affect the disk only in a destructive manner once triggered.

A new breed of programs has the capability of not only reserving malicious damage for a given event's occurrence, but of also replicating itself as well.

This is what people refer to when they mention the term "Virus Program".

Typically, a virus will spread itself by replicating a portion of itself onto another program. Later, when that normally safe program is run it will, in part, execute a set of instructions which will infect other programs and then potentially, trigger the Trojan portion of the program contained within the virus.

The danger of the virus program is twofold. First, it contains a Trojan which will cause damage to your hard disk. The second danger is the reason why everyone is busy building bomb shelters. This danger is that the virus program will infect other programs and they in turn will infect other programs and so forth. Since it can also infect programs on your floppy disks, you could unknowingly infect other machines! Pretty dangerous stuff, all right!

Kenneth van Wyck, one of the computer folks over at Lehigh University, first brought a particular virus to the attention of the computer community. This virus infects a program, which every MS-DOS computer must have, called COMMAND.COM. This is the Command Line Interpreter and is the interface between your keyboard and the MS-DOS operating system itself. Whatever you type at the C> prompt will be interpreted by it.

Well, the virus subverts this intended function, causing the infection of neighboring COMMAND.COMs before continuing with normal functionality of the command you typed. After a certain number of "infections", the Trojan aspect of the program goes off, causing you to lose data.

The programmer was clever. But still a worm. And still deserving of contempt instead of respect. Think of what good purposes the programmer could have put his or her talents to instead of creating this damage. And consider what this programmer must do, in covering up what they've done. They certainly can't tell anyone what they've accomplished. Justifiable homicide comes to mind, but since the worms they must hang around are probably as disreputable as they are, they must hold their little creation a secret.

A pity. Hopefully, the worm is losing sleep. Or getting a sore neck looking behind them wondering which of their "friends" are gonna turn them in.

### The Challenge to the Worm

When I first released a program to try to thwart their demented little efforts, I published this letter. What I say in it still holds:

"As for the designer of the virus program: most likely an impotent adolescent, incapable of normal social relationships, and attempting to prove their own worth to themselves through these types of terrorist attacks.

"Never succeeding in that task (or in any other), since they have no worth, they will one day take a look at themselves and what they've done in their past, and kill themselves in disgust. This is a Good Thing, since it saves the taxpayers' money which normally would be wasted on therapy and treatment of this miscreant.

"If they *really* want a challenge, they'll try to destroy *my* hard disk on my BBS, instead of the disk of some innocent person. I challenge them to upload a virus or other Trojan horse to my BBS that I can't disarm. It is doubtful the challenge will be taken: the profile of such a person prohibits them from attacking those who can fight back. Alas, having a go with this lowlife would be amusing for the five minutes it takes to disarm whatever they invent.

"Go ahead, you good-for-nothing little slimebucket: make *my* day!"

Alas, somebody out there opted to do the cowardly thing and use the FLUSHOT programs as a vehicle for wrecking still more destruction on people like you. The FLUSHOT3 program was redistributed along with a companion program to aid you in reading the documentation. It was renamed FLUSHOT4. And the reader program was turned into a Trojan itself.

*(continued on page 28)*

---

***From the Guiness Book of World Records:***

*The largest collection of valid credit cards, as of May 3, 1980, is one of 1,003, all different, by Walter Cavanagh of Santa Clara, CA (known as "Mr. Plastic Fantastic"). The cost of the acquisition was nil, and he keeps them in the world's largest wallet, 250 feet long, weighing 31 pounds, and worth more than $1,250,000 in credit.*

***

***Largest Incorrect Telephone Bill***

*On August 18, 1975, the landlord of the Blue Bell Inn, Lichfield, Staffordshire, England received a telephone bill for $4,386,800,000. It was later admitted that this bill contained "an arithmetical error".*

# the dark side of viruses

by The Plague

I'm sure you've heard about computer viruses. But what you were probably fed was misinformation. This article will attempt to de-mystify your perception of the computer virus, give you the facts, as well as teach you how to create your very own virus. This is not a second-hand or bystander explanation of viruses; I have had first-hand experience in the writing, distribution, and tracking of my very own virus, so I'm quite knowledgeable on the subject. Most viruses do destroy data. They also spread somewhat exponentially when unnoticed and not controlled. The beauty of the computer virus is that it perfectly mimics a real virus or small organism, thus having the potential of being a great tool in artificial intelligence. I will not write about how to protect yourself from a virus, because that would defeat the purpose of this article, and anyone with common sense already knows how to prevent being infected.

Recently, viruses have been a very hot issue in the media, but I assure you that I'm not jumping on the bandwagon because my virus has been around long before the term "computer virus" was ever mentioned in the media. The media has a very shallow understanding of what a virus is. Examples of the media's reporting of computer viruses include the article in the February 1, 1988 issue of *Newsweek* written by William D. Marbach and Richard Sandza called "Is your computer infected? Systems fall to silent and contagious killers." Another report appeared on ABC World News Tonight in late February, and I must say that the computer animation was quite good. It showed the virus (a pink spiny blinking sphere) as it entered the resistors on the motherboard (come on, are these guys for real?). This was followed by a guy who claimed to be the inventor of the virus, which is absolutely bogus, because the computer virus was not invented by any one person. I don't even know why he decided to claim the credit -- it's nothing to be proud of.

My experience with viruses comes from writing CyberAIDS, a virus for the Apple II family of computers. This is the first and only virus for the Apple which operates under ProDOS that I know of. Due to ease of use of the ProDOS MLI (Machine Language Interface), it was incredibly easy to write the virus. This is because I didn't need to deal with the hardware directly, only make a few simple system calls (i.e., read block, write block, open file, close file, etc.). The fact that ProDOS runs on the entire spectrum of the Apple II family also allows my virus to reach the broadest audience available. The ProDOS MLI is very similar to the operating systems of most personal computers, mini-computers, and mainframes. Thus the virus can be adapted to run on any computer, so don't make the same mistake that the Apple community made, that is in thinking that a virus will never appear for their computer. Operating systems with similar calls and characteristics as ProDOS MLI are MS-DOS, Unix, AmigaDOS, Atari's TOS, and Macintosh's OS.

I was asked whether I had any moral feelings about viruses, or whether I thought that they were wrong, or evil, or whatever. My feelings are the following: I don't care one way or the other. If people's data is destroyed, then so be it. If people are stupid enough to accept pirated software, then they deserve to be punished. The fact is that most business PC users will never be infected with a virus unless they download public domain or pirated software. Also, businesses may be affected if someone in the organization decides to infect the system, in which case the destruction is not preventable, because the person doing the infecting would have enjoyed destroying data even if viruses didn't exist. As for people who use their computers for home/entertainment/hobby, they are the ones most susceptible to the virus revolution. They should be wary of software that was not previously tested by others. Nowadays, it's becoming quite dangerous to accept software 'off the street'. I hate to use this expression, but "viruses don't kill data, people kill data". A virus is perfectly harmless unless it is being spread by people willingly/unwillingly. Therefore, people must take the responsibility to protect themselves and others by taking precautions. This will not be discussed in this article.

Creating a virus is by no means a simple project. Anyone who has ever attempted to write a virus, or any cybernetic organism for that matter, will tell you about the difficulties and tribulations involved. If anything, I'm quite upset that most people don't realize what an accomplishment this is. One person even told me, "Hey, anybody could write a virus. The reason I never wrote one is because it's wrong to do so." Well, he was wrong at the time because it is quite difficult to write a virus completely from scratch. But perhaps this article will allow anyone to write a virus by giving them at least a good start.

My main concern about my project was how to track the spread of the virus, in order to gather data. This data could be used in the future to make better, stronger, and more deceptive viruses. The technology behind the virus has come a long way since the 1970's. It's a field yet to be fully explored and appreciated by the computer community. I, for one, hope that people become more aware of the computer virus and that they take measures to protect their data. The ideal scenario would be computer companies rewriting their operating systems to be virus-resistant. In the long run, the computer virus may strengthen our defenses against data loss, whether it be due to viruses, trojan horses, power outages, or unauthorized users. My main hope is that the threat of the virus will help curb software piracy and allow software companies to prosper. If a person knows that he stands a chance of being infected by accepting pirated or modem distributed software, he will realize that he's much better off buying the software and receiving the documentation as well.

> *"The beauty of the computer virus is that it perfectly mimics a real virus or small organism."*

### How The Virus Works

Before I go any further, let me just say that

(continued on next page)

# straight from the source

a virus should be written in assembly language, "C", or any other language that allows low-level functions (byte manipulation, system calls, memory moves). I doubt you can write a virus in BASIC or PASCAL (a trojan horse maybe, but certainly not a virus). Viruses in the future may be written in Prolog or LISP and incorporate artificial intelligence.

As an example, I'll discuss the CyberAIDS virus, which was written purely in 6502 Assembly. CyberAIDS is an "application resident" virus (see **Virus Types**). Most viruses must make themselves permanent in the storage device in order to continue reproduction. See the **Virus Types** section for a detailed description of the various methods that viruses use for reproduction and where they may hide themselves.

After attaching itself to a file or disk that was previously uninfected, the actions of any particular virus may vary, but the virus will check the disk counter before proceeding to any intended action other than reproduction. The disk counter, an individual byte somewhere on the infected disk, keeps track of how many times the virus has accessed that particular disk, and thus assures that the virus will not detonate prematurely. Some viruses are totally harmless and print a simple text message (such as the Macintosh virus), while others are created to cause harm and/or to destroy data (like CyberAIDS). There are still other viruses which were not originally meant to be destructive, but due to the fact that they come between an operating system and it's applications, cause harm nonetheless. This harm is usually in the form of system crashes or the destruction of protected software (i.e., the Amiga virus, which would not affect standard disks but would destroy protected disks due to their non-standard file/disk format).

### How The Virus Spreads

All viruses spread. This is what makes them distinct from trojan horses. Whereas a trojan horse program simply wipes out your hard drive when you run it once or twice, a virus will attach itself to normal applications or disks and make them carriers. Care must be taken that the virus will only infect one file each time the infected application runs, thus making sure that the time before the original application executes is kept to a minimum. This will allow the virus to go unnoticed during the user's daily activities. You can run a virus-infected program a hundred times and it will behave normally with the exception that it will make copies of the virus portion and attach itself to other disks/applications, but when you run it the final time, it will perform its intended activity. Since only that copy of the virus has detonated, you are still left with perhaps dozens of infected files which will not detonate until they are run several hundred times (and thus will spread the virus even more).

The benefits of an application resident virus such as CyberAIDS are several. Since no new files are ever created on the disk by the virus, the user will probably not notice anything is wrong. Instead, normal applications are modified by the virus to execute viral code. When individual files (non-text executable code files) are infected, the virus can be spread in three ways:

(1) The manual copying of the file from disk to disk by the user. User-group disk distribution can achieve the best results when this method of reproduction is used.

(2) The automatic copying of viral code by the virus itself to non-infected files in other drives or the hard disk. Usually serves to give the virus a better foothold within a particular user's software library.

(3) The transfer of infected files over the modem. The infection has a good chance (whether by accident or on purpose) of reaching public domain or pirate bulletin boards. The distribution of that file will be incredible. Infected files may also be spread through LAN's (Local Area Networks).

**Application Resident Virus Outline**

A. INITIALIZE.

1. Find current location of virus in memory.

2. Relocate itself to predefined memory location.

3. Make sure DOS is active and ready to accept system calls.

4. Move original application header (6 bytes) back to original memory.

"*The virus may even call its creator and allow the transfer of data from the infected system.*"

B. SEARCH.

1. Choose random volume (disk device).

a. Make sure volume is not write protected

b. Make sure volume is on line (no I/O error)

2. Increment disk counter (See NOTE1) and go to destroy (See NOTE2) if necessary.

3. Check for enough space on volume.

4. Choose candidate file.

a. File must be a system or application file.

b. File must not be already infected (choose appropriate method for identifying infected files).

c. File must be small enough to allow viral attachment (so that the application and virus code both fit in memory).

d. If the file is locked then unlock it.

C. INFECT.

1. Open candidate file.

2. Load first block of candidate file into a main.buffer.

3. Take first (6 bytes) and save to alt.buffer (also known as SH).

4. Calculate viral location in new file.

a.Viral.Addr= Application.Start Addr + Length.of.Application + 6

5. Store a JUMP Viral.Addr at beginning of file.

6. Rewrite main.buffer.

7. Set file pointer to end of file (for append).

8. Write the alt.buff (6 bytes).

9. Write the viral code afterwards.

10. Close candidate file.

D. DESTROY (Optional).

1. Lock out Keyboard and Reset Key if possible.

(continued on next page)

# how to do it

2. Destroy data.
    a. Recognize all disk devices (hard disks, floppies, 3.5", ram).
    b. Wipe out the directory (FAT) blocks of each device.
    c. Wipe out key block for each file in each directory block.
3. Do graphics and music (optional).
    a. Totally up to virus writer.
4. Present text message (optional).
    a. Totally up to virus writer.

E. LEAVE.
1. Jump back to Application.Start.Addr
    a. Thus continue as if nothing had happened.

NOTE1: The disk counter is a particular byte on the disk that the virus uses to hold the value of how many times that virus has run with that particular disk inserted (active).

NOTE2: DESTROY or LEAVE is executed depending on the status of the disk counter.

### Virus Types

**Application Resident:**

Hides in applications (see **Virus Outline**). Patches an application (or system file, .EXE, .COM, .SYS file) so that the virus is appended at the end of the file and a call to the virus is provided at the beginning of the file. The original beginning of the file is saved to the end of the file as well, as it will be moved back (SH is moved back to where JC is, see Figure B) into place at the beginning of the file when the virus executes, thus allowing the application to execute normally after the viral chores are completed. Due to the different position of the viral code in each infected file (because of different file lengths) and unless the viral code can run anywhere in memory, it must be able to relocate itself into a pre-set memory location where it will run.

```
(a) Normal (not infected file)
+----+--------------------+----+
| SH | rest of application | EOF|
+----+--------------------+----+
(b) Infected file
+----+--------------------+----+----+----+
| JC | rest of application | SH | VC |
EOF |
+----+--------------------+----+----+----+
```

SH = Standard Header (first few bytes of the original file's executable code).

JC = Jump Code (jumps to the address of the virus).

VC = Viral Code (see **Virus Outline**).

EOF = End of File.

**Boot Block Resident:**

Activated upon boot. Usually loads additional program code from other blocks on disk. This is quite invisible as files are never altered, and blocks used by the virus on disk are designated as busy for protection. The Amiga virus is a perfect example.

**Memory Resident:**

Resides in memory. Usually a terminate and stay utility that can be activated by any event (clock, keyboard, DOS call). On multi-tasking systems (such as Unix, Xenix, OS/2) it can be a background task. It will usually allocate memory for itself from the memory manager.

(continued on page 14)

# BUILDING A RED BOX

by J.R. "Bob" Dobbs

Essentially, the red box is a device used to fool the phone company into thinking you are depositing coins into a payphone. Every time you drop a coin into a payphone, the phone signals the type of coin inserted with one or more bursts of a combinatinn of 1700 hz and 2200 hz. The tune bursts are coded as follows:

**Nickel:** One 60 millisecond pulse

**Dime:** Two 60 millisecond pulses separated by 60 milliseconds

**Quarter:** Five 35 millisecond pulses separated by 35 milliseconds

### How to Use It

Operation is simple. Simply dial a long distance number (some areas require you to stick in a genuine nickel first), wait for the ACTS computer to demand your cash, and press the "deposit" button on the red box for each coin you want to simulate. The coin signals are coupled from the red box into the phone with a small speaker held to the mouthpiece. For local calls, either you must first deposit a genuine nickel before "simulating" more coins or place your call through the operator with 0 + 7d. Use some care when the operator is on the line -- sometimes they catch on to your beeper ploy.

### Circuit Operation

Each time the pushbutton is pressed, it triggers half of IC1, configured as a monostable multivibrator to energize the rest of the circuit for a length of time determined by the setting of the coin selector switch. This in turn starts the other half of IC1, configured as an astable multivibrator, pulsing on and off at regular intervals at a rate determined by the 50k pot between pins 12 and 13. The output of the astable thus alternately powers of IC2, configured as a square wave oscillator, providing the required 1700 hz and 2200 hz to the op amp which acts as a buffer to drive the speaker.

### Construction

Assemble the circuit as you wish. Component placement is not critical. I found the easiest method was to use point-to-point wiring on a "universal" PC grid board with solder ringed holes. Use sockets if you aren't a whiz with a soldering iron. Be sure to leave easy access to the potentiometers for alignment.

### Alignment and Testing

For alignment, a frequency counter and triggered sweep oscilloscope are extremely handy (but not *absolutely* necessary).

Install a temporary jumper from +9v supply to pin 14 of IC2 and temporarily disconnect the 0.01uF

(continued on page 22)

# how it's done and why

(continued from page 12)

**DOS Resident:**

A virus that's patched into DOS and infects any disk, file, or DOS on disk that's accessed during the time that the infected DOS is active. Since DOS is the program which runs on the computer 98% of the time, it would be advantageous to add viral code to a frequently executed portion of DOS (such as Read Block code). The infected DOS will usually attempt to patch any DOS on disk and to make it infected. Care must be taken to prevent crashes, thus making sure the virus will only patch DOS versions that can be successfully altered by the virus. Any unrecognized DOS on a disk should be left alone.

**Application Oriented:**

A virus that's integrated into an application and works closely with it. Application oriented trojan horses are quite common, but viruses that are integrated into an application are hardly ever seen. For example, a packing (file compression) program such as ARC or a terminal program that infects files before packing or transmitting them.

## Types of Viral Action

**Complete Disk Data Destruction:**

Affects floppy, 3.5", hard disks, ram disks. Usually the most common action taken by a virus. It is quick and is not noticed until it is too late. Care must be taken to prevent the user from prematurely stopping the destruction by locking out the keyboard or by giving a text message that will make them feel comfortable (i.e., "Loading Data Segment", "Checking for files").

**Slow Disk Data Degradation:**

Similar to above, except data is slowly destroyed on a disk with each activation of the virus. Usually a disk block at a time, but may be done a byte or even a bit at a time. This is perhaps the most sinister viral action as it will take quite a long time before anyone notices anything is wrong. Also known as the "disk bit spray".

**Slow Memory Data Degradation:**

Data in memory is modified a byte or a bit at a time. Usually done by a memory resident or background task virus. This will slowly destroy program code and data as the person is working at the computer. Weird things may happen and usually data integrity is compromised or program crashes will occur at random times. This is also known as the "memory bit spray".

**Hardware Destruction:**

A virus will attempt to destroy hardware if possible. It usually attempts things like overloading the address or data bus by attempting to activate all peripheral cards at the same time. "Head Slamming" may also be done, a process which allows older hard disks to have their read/write heads slammed at high velocities into the parking position or into the side of the disk enclosure. If any mechanical parts are present in the computers (relays), the virus will attempt to wear out or jam these devices by turning them on and off at very high speeds. This may also destroy various video and uart chips. Also, the virus will attempt to alter the time and date in any clock card or chip, or even destroy the pre-set configuration in battery-backed ram.

**Modem manipulation:**

A virus that usually attacks BBS systems and is a memory resident virus. It will activate itself during the time the BBS is not in use and play with the modem and the phone line. It does things like call Europe directly or call the police over and over. This virus may actually cause the infected person to go to jail or increase their phone bill or both. The virus may even call its creator and allow the transfer of data from the infected system.

That concludes this article. I hope you enjoyed it. I would like to see some more viruses out there. To write and distribute a virus you must lose every shred of moral fiber, and if I know the readers of this magazine, there will be a computer virus plague in the very near future. So have fun, kids. If you write a successful virus, don't hesitate to release it, and by all means send the source code to *2600*. We'd like to hear from you.

CALL ONE OF OUR COMPUTER BULLETIN BOARDS TODAY!
2600 BBS#1
(OSUNY)
914-725-4060
*
2600 BBS#2
(CENTRAL OFFICE)
914-234-3260
*
2600 BBS#3
(YOYODYNE)
402-564-4518
*
2600 BBS#4
(BEEHIVE)
703-823-6591
ALL OPEN 24 HOURS

New Jersey Bell central offices, Church Street, New Brunswick, 1912.

# A READER'S REPLY TO CAPTAIN ZAP

**by The Rancid Grapefruit**

**Query:** "What happens to inept computer criminals who get caught?"

**Answer:** "They open up 'security' companies and start preaching to an extremely gullible public -- usually casting themselves as some kind of 'hacker expert' whereas the only thing they are 'experts' at is getting caught."

The opening comments have absolutely nothing to do with Captain Zap, whose reputation is impeccable, and we most certainly would not want people to misconstrue the comments as a vicious attack on his person. Lord, no....

Obviously, we disagree with Captain Zap's brilliant observations on the state of "Hacking and Phreaking". If we did agree with him, we'd hardly be writing this swell response, eh?

"The ongoing wave of computer crime that is being reported in the media around the world shows" the shallowness of the media's never ending quest for anything that will titillate a technology-ignorant public, and push up the ratings of whatever publication or feed happens to be catering to the public's fear of technology on that particular occasion.

"An Interpretation of Computer Hacking" is just that: Captain Zap's personal *opinion* on the subject. In the first several paragraphs, Zap essentially summarizes the opening chapter of almost any given "Beginner's Introduction to Computers" and somehow manages to pass off observations that have already been made a few hundred times as his own "ideas". The only real mystery to us is why he decides on "16 Megabytes of RAM" as an arbitrary amount of memory that "today's personal computers" are supposedly equipped with.

This leads into the "information is power" spiel, and the inevitable arrival of ISDN wherein phones and computers will become one glorious entity and live happily ever after.

All of this ends up with Zap giving you his opinion on "The Dawn of Phreaking", the usual mention of Draper and blue boxing, followed by a summary of the boxes that matches slang to function, and terminating with a simplified account of toll fraud where Zap babbles about the various OCC's for a while.

Although we were very impressed by the programming ingenuity of the supplied "Wargames dialer" listing, and find ourselves constantly looking to the first section of Zap's article when we feel lost or at a need for guidance, we will regrettably have to let it stand. Since aside from the ill-chosen "highlights of yesteryear" there is nothing there that hasn't been discussed or otherwise summarized too many times in the past. As such it would be a waste of our time to do so yet again.

> *"Rarely is the purpose of a conference to 'pass information over to other hackers that can work on a problem and plan for more tactical attacks to the target system.'"*

Hacker Communications! Shhhhh! Secrets being exchanged!

While we don't dispute the fact that people do call each other, sometimes in large groups hooked together on a conference (without paying for it, gasp!), *rarely* is the purpose of a conference to "pass information over to other hackers that can work on a problem and compare results and plan for more tactical attacks to the target system." The usual reason a conference starts is because one kid is bored and wants to talk to a bunch of his peers at the same time. What takes places on almost any given conference is a bunch of screaming kids harassing TSPS operators, calling pizza parlors in Europe, and in general pranking or annoying anyone they can think of at the moment.

"Attacks" placed on Bell System computers are usually the result of one kid -- who is *not* some genius, rather he's quite often the friend or relative of somebody who understands the *concepts* involved, not only the commands -- who thinks it would be a blast to turn off CAMA on a few switches, or disrupt COSMOS operations. All of this potential damage is made possible by the RBOC's themselves, which provide extremely minimal security that is more of a study in faulty security techniques and shoddy organization than any kind of obstacle to the potential hacker.

While "computing power" is now within reach of a vast number of people, almost all of that "vast number" are ignorant as to their system's potential. In fact, most never get beyond running their spreadsheet or doing taxes on that wonderful PC with "16 MB RAM". And if they ever do sink into the sordid depths of depravity and actually try something awful like making a bit copy of someone else's program and xeroxing its manual, it's our personal belief that the world will in all probability not come to an end. Of course, we could be wrong.

Almost all potential hackers are little kids with a lot of time on their hands, and most of those kids will never get anywhere because they are not brilliant, or in any way gifted -- regardless of what the public might think of them. The vast majority of people that the public views as computer geniuses are quite average teenagers whose only "skill" is calling up boards -- with "better security than most large computer systems" -- and blindly applying things they see posted on them, *without* understanding what they are doing. Granted this is a "threat", but it's the *only* threat that boards pose. And the only reason it's a problem to begin with is because the "threatened" organizations or companies have ridiculously bad security.

While it is true that more people now own personal computers than at any other time in history, the overall effect of this influx of new hackers is negligible. Instead of one kid annoying his local CO from information he found on some board, there are 10 kids using the same information from the same board to harass the same CO. In short, there is a deluge of "idiot savants" who are capable of doing no more damage than trained chimps.

### The Bulletin Board Systems

Bulletin board systems (BBS's) pose a possible threat for the simple reason that the more highly skilled users will post potentially dangerous information in a

*(continued on next page)*

# A READER'S VIEW OF THE ZAP ARTICLE

place where the "idiot savants" can read it. The better versed user's reason for posting it is ego gratification. Regardless of what he claims, the only incentive he has to post this information is an ego boost. He already knows that the "idiot savants" are going to do something stupid with the information, at worst simply making it valueless, at best flexing their muscles and showing their target how vulnerable they are to an outside attack.

Granted, if BBS's didn't exist, much of the trouble various people and companies now experience would vanish along with the "idiot savants". But the only thing the boards really do is provide a forum for the more intelligent users to bask in the adoration of fools. They are not some great organized crime wave of the future; they are simply used by several thousand bored kids, the great majority of them trying to live out some kind of power trip while the remaining minority congregate together because they like being surrounded by those they view as their peers.

In summary, boards are a social medium -- not the forefront of some well orchestrated, nationwide attack on loopholes in "the system". Just about any issue of *Soldier of Fortune* contains all the information you could possibly want about where to obtain books on plastic explosives, nerve gas, special weapons, electronic devices, and anything else that has been dreamed up. You hardly need a BBS in order to have access to that kind of knowledge. In fact most of the information posted on the "death and destruction" subs of boards is a word-for-word copy of some article that originally appeared in one of these books. The only crime taking place is copyright infringement.

**Specific Responses to**
**Some of Zap's Statements**

Let's cover Zap's statements one by one:

➥ "Such information like dial-up port numbers, logons, and passwords are common information available to the main hacker population." No shit. It's also common information available to anyone who calls up any of the carriers and requests it. The logons and passwords are usually the end result of credit card fraud, and have nothing to do with the ingenuity of hacking into a system.

➥ Zap's entire spiel on board security, the "select few", and the security of hacker boards takes place for the most part in his head and nowhere else. The only reason most people never move into these hallowed ranks is because they have somehow convinced themselves that this isn't possible. The only thing separating you from anything you want to access is ignorance of how the sysops' minds function and the *reality* of how security works, as opposed to the ridiculous fantasies presented by Zap.

Assuming a sysop had no life outside of his board, and he got paid by the hour to sift through all of those records of his potential users, all he'd accomplish would be to weed out people who didn't know how the system worked. Anyone who wanted access and understood the basics of how to falsify information would still gain entry, and the end result is a security breach. *There is no such thing as perfect security*. When *anyone* "builds a better mousetrap", a few days later an inventive person will "build a better mouse".

In any case, the security examples presented by Zap *do not* exist on any private or "elite" phreak or hacker BBS now in existence. If the sysop *claims* that is what they do, it's simply meant to scare potential users into submitting valid information which the sysop doesn't bother to verify beyond the telephone number.

➥ Disclaimers and Clauses: Whether Zap's comments originate from actual ignorance or simply a desire to knowingly misinform, is unknown to us.

A disclaimer, *any* disclaimer, will have very little value in any kind of legal situation. While the sysop might feel better if "it's not my fault" and "for information purposes only!" are splattered over every part of his board, it isn't going to make any difference to *any* judge in *any* court! Disclaimers are *not* legally binding. All they do is take up space and lull sysops into a false sense of security.

Thinking you're safe because you have a good disclaimer translates out to "ignorance is bliss". If you haven't had any trouble with law enforcement agencies to date, it only means that they don't know about your existence (buried as you are amongst 1,000 other quasi-legal BBS's), or that they know and don't care because you aren't doing anything that they're worried about.

➥ Tele-Trial: I can't believe this! Zap, where ya been for the last three years? Tele-Trial was a ridiculous "electronic tribunal" started by King Blotto as a joke. For whatever reason, he started taking himself seriously and for a few months in 1985 "Tele-Trials" were being held, in which "electronic execution" took place and stupid kids cried about being thrown off Blottoland and being declared "uncool!" (The horror!)

It is *impossible* for anyone to enforce any "ruling" over anyone else in the modem community. The boards are not all interconnected and what one person, or group of people, declares as "law" on one system, or set of systems, is utterly meaningless to the hackers the next area code over. And even to the people involved with those specific systems, it only pertains to them if they want to play the game. There is nothing preventing an "exiled" person from picking up a new handle and starting over.

Aside from the complete impossibility of enforcing such "rulings" over anyone but the most brain-damaged kids, all of this is nothing more than a history lesson.

(continued on next page)

**WILL PAY**
**$1,000**
**FOR EARLIEST INFORMATION**
**LEADING TO ARREST**
**AND PROSECUTION**
**WITHIN NEW YORK AREA OF**
- CALLING ROOM OPERATORS
- BLUE BOX OPERATORS
- COMPUTER HACKING INVADING LONG DISTANCE TELECOMMUNICATIONS

**Call (212) 227-4519**
(Between 7:00 A.M. and 11:00 P.M.)
CONFIDENTIALITY STRICTLY MAINTAINED

THIS AD APPEARED IN A NEW YORK NEWSPAPER THIS SPRING. THE HUNT IS ON!

# RESPONDING TO THE CAPTAIN ZAP ARTICLE

Tele-Trials have been over since the summer of 1985.

As for Richard Sandza, Tele-Trial still existed at the time of the publishing of his articles for *Newsweek*. The "Tele-Trial" he was put on was simply a conference of abusive kids who felt that he had given hackers unfair treatment. In retaliation they threatened him: a Captain Quieg posted his credit report and numerous kids ran up bills on his credit cards, sending assorted junk to his house.

Hackers cannot "perform the destruction" of *anyone*. All they can do is scare the shit out of "normal" people who are shocked that a bunch of kids can get their unlisted number, credit cards, and various other records, and abuse them.

In any case, Sandza is something of an exception since he managed to piss off a large percentage of people who were in a position to make life hard for him in return. Most people who disagree with him can write a complaint to *Newsweek*, but if you have the ability to bring your displeasure to his personal attention, in a way that will ensure he gives notice to it, wouldn't you do the same thing? After all, it isn't *Newsweek* you're mad at, it's Richard Sandza. Some of you probably wouldn't, but that's one of the fringe benefits of being a hacker. Instead of being bound by "the system's" rules and regulations, you can get around it and let your conscience be your guide (if you happen to have a conscience).

➥ "And remember, the hacker can be the best prevention for computer security sickness and that a reformed hacker can make for the best data processing security person." Another token stab at self-promotion by Zap.

➥ "The boards in general have been a major problem in the control of information due to the use of the boards by what some may call 'information junkies'." What's wrong with people who want to collect information? Are you suggesting that arbitrary censorship would be an improvement?

➥ "One of the major contributing factors involving computer abuse is the non-education of the users in ethics." While it makes for a nice sweeping generalization, this statement has little to do with reality.

Most "normal users" think no more of copying a piece of software than they think of taping a copy of an album, or xeroxing a page out of a copyrighted publication. While all of these acts are illegal, there aren't many people that actually care. "Educating" people is not going to eradicate these problems.

As far as the phreaks and hackers are concerned, the statement is even more ludicrous. While a minority undoubtedly justify their actions to themselves as "curiosity" and thus set their consciences to rest, the greater percentage know that in the course of doing whatever it is that they happen to be doing at the moment, they are committing crimes. And they don't care.

Morality and ethics are subjects that cannot be "taught" to anyone. Each individual has to make his or her personal choices based upon whatever tenets or beliefs they happen to espouse. Very often people who function from a predominantly logical perspective come to the conclusion that "right and wrong" are relative to a given time and situation. As applied in our society they typically denote values that most of our present population subscribes to. Why should anyone do something just because everyone else is doing it?

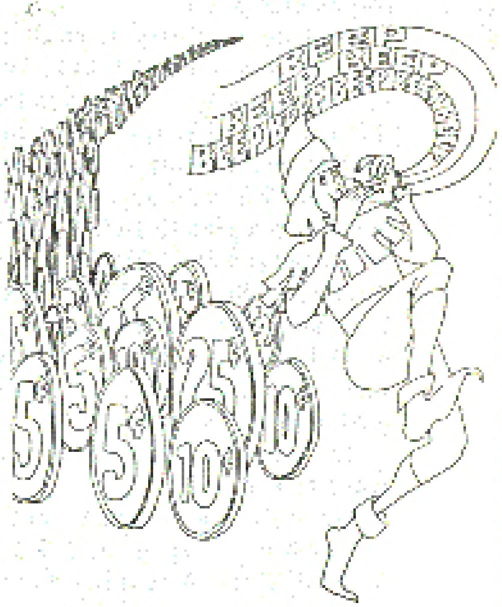
Ethics will always be up to the individual, who will in many cases come to the logical conclusion that he doesn't care what the rest of society condones or accepts, and instead of blindly following their dictums he will choose to think for himself and perhaps arrive at conclusions that don't coincide with what society happens to find acceptable at that particular time.

➥ Accessing government and military computers: Why it is that people come to the conclusion that government computers should be bastions of security we couldn't begin to guess. When you speak of the government and military, we presume you mean *our* government and military; you know, the one run by incompetents, bureaucrats, and other paper pushers that excel at nothing except wasting time and money.

For someone who cautions others against making "rash statements", Captain Zap has apparently written an entire article filled with statements that neatly ignore his own dictum.

Lastly, we'd like to bring up one relevant fact that most "security analysts" manage to ignore: hackers and phreaks (for the most part) are not criminals. At least that isn't the way they view themselves. While nobody lays awake nights worrying about the fact that today he's cost a few phone companies some money, and perhaps wasted system resources on un-authorized applications, a hacker or phreak's primary motivation is either a real hunger for knowledge, or ego gratification. In neither case does monetary gain enter the picture. The people you really have to worry about are career criminals. They aren't kids and they don't call boards. If a hacker is present in your system, then a criminal could easily gain entry to your system as well. If anything, you should view it as a blessing that the hacker has brought your lack of security to your attention.

The previous paragraph shouldn't be misconstrued as a moral judgment on criminals. Personally we couldn't care less how you make your living as long as you're good at what you do.



**Artwork by J.R. "Bob" Dobbs**
**Red Box article on page 13**

(continued from page 13)

# HOW TO BUILD A RED BOX

capacitors from pins 5 and 9 of IC2. Power up the circuit. Measuring the output from pin 5 of IC2 with the frequency counter, adjust the 20k pot between pins 1 and 6 for an output of 1700 hz. Now adjust the 20k pot between pins 8 and 13 for an output of 2200 hz from pin 9 of IC2. Remove the temporary jumper and re-attach the capacitors to pins 5 and 9. (Note: if no frequency counter is available, the outputs can be adjusted by ear one at a time by zero-beating the output tone with a computer generated tone of known precision.)

Next, temporarily disconnect the wire between pins 5 and 10 of IC1. Set coin selector switch in the "N" (nickel) position. With the oscilloscope measuring the output from pin 9 of IC1, adjust the 50k pot between pins 12 and 13 of IC1 for output pulses of 60 millisecond duration. Reconnect the wire between pins 5 and 10. (Note: If no scope is available, adjust the pulse rate by ear using computer generated tones for comparison.)

The remaining adjustments are made by ear.

Leave the selector switch in the "N" position. Adjust the 50k pot labelled "Dime" for a quick double beep each time the pushbutton is pressed.

Finally, set the selector to "Quarter". Adjust the 50k pot labelled "Quarter" until exactly 5 very quick beeps are heard for each button press. Don't worry if the quarter beeps sound shorter and faster than the nickel and dime ones. They should be.

### Conclusion

If all went well to this point, your red box should be completely aligned and functional. A final test should now be conducted from a payphone using the DATL (dial access test line) coin test. Dial 09591230 and follow the computer instructions using the red box at the proper prompts. The computer should correctly identify all coins "simulated" and flag any anomalies. With a little discretion, your red box should bring you many years of use. Remember, there's no such thing as space change!

**Parts List for Red Box**

*Semiconductors*

(2) 556 Dual Timer

(1) 741 Op Amp

(1) 1N914 Switching Diode

*Resistors*

(6) 10k (1) 4.7k

(2) 100k

(4) 50k PC Mount Potentiometer

(2) 50k Multi-Turn Potentiometer

*Capacitors*

(10) 0.01 uF (1) 1.0 uF

(2) 10.0 uF Electrolytic

*Miscellaneous*

(2) 14 Pin Dip Socket

(1) 8 Pin Dip Socket

(1) 3-position Rotary Switch

(1) Momentary Push-Button Switch (normally open)

(1) SPST Toggle Switch

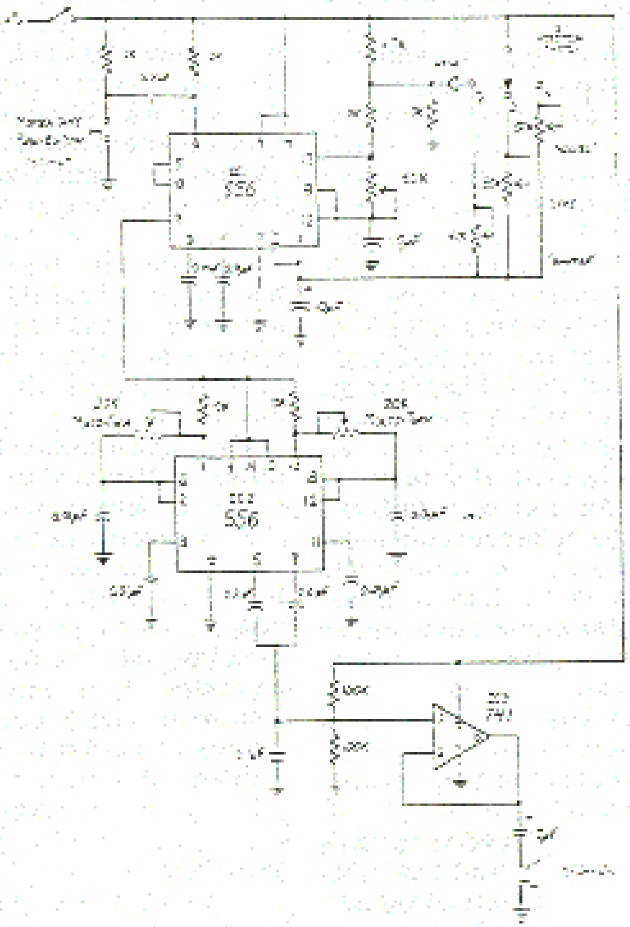
(1) Speaker or Telephone Earpiece

Circuit Board

Box

Mounting Hardware

9V Battery Clip



# THESE ARE THE LETTERS

## Reactions to Zap

**Dear 2600:**

After reading Captain Zap's article in your last issue I'm left with the feeling that it was not meant to inform. Rather it seems to me that Zap wants to scare legitimate users and people in charge of security at various companies into believing in the existence of an incredibly organized and complex organization that decides upon who attacks what and makes up laws and regulations. In short, it looks to me like Zap desperately wants people to believe that the big bad hackers are out there waiting to get them (especially if they happen to be Fortune 500 companies, in which case the hackers *really* have it in for them), and only Captain Zap and his security company can protect you from us, so by God ya better hand him some cash and a long term contract, or we'll eat you alive!

Either that or Zap is just hopelessly out of it. In either case I wouldn't put my security into his hands.

**Murdering Thug**
**and The BOY!**
**Circle of Deneb/**
**Digital Gang**

**Dear 2600:**

Is Captain Zap for real? Is this the same Captain Zap who used to go by the name of Ian Murphy and is consulting on computer security? It's a pretty far-fetched picture of an evil underground conspiracy. All of the "elite" underground BBS's I was on (and I was on several of the *exact* same ones Captain Zap was on) had no real checkups on identity. Most even skipped the callback to verify and a famous name could get you on.

The FBI has some of the best hacking info available and I'm sure they would trade a few trapped MCI codes and traced computer passwords to get on any system.

The biggest bull of the whole article is: "Granted they did not move the bird [satellite], but they did gain access to the rotation control for the satellite." *Pure* bull. Please see the article I wrote for you on page 2-52 (August '85) about moving satellites. Tells exactly what was misunderstood. I know, because I posted the "satellite routing codes".

**The Shadow**

**Dear 2600:**

In the Spring 1988 issue, *2600* presented an article called "The Hacker Threat" written by Captain Zap. While I don't agree with the article, I'm glad you published it because I like to see different opinions which provoke discussion. After reading the article I decided to do a little research on him.

Captain Zap, whose true name is Ian Murphy, is now a computer security consultant. This was not always true. Until the time of his arrest, he was a hack (Taxi Driver) by trade and a hacker by hobby. In 1984 he was convicted of credit card fraud. Now, as a reformed hacker, he *attempts* to help companies free their systems from hackers. Recently, he has been active on many BBS's, including those sponsored by *2600*. On Central Office BBS he claimed that a rival computer security consultant from Detroit had been charged with criminal sexual conduct and harassment. He then threatened to sue that same consultant for alleged slander. He also vigorously attacked The Telecom Security Group (TTSG), a respected Newburgh (NY) based consulting firm, for having advertised in *2600* and for being closely involved with computer hackers. TTSG is considering legal action against Murphy.

Murphy has been profiled by such periodicals as *The Wall Street Journal* and *USA Today*. In these interviews he has admitted to such acts as: monitoring his ex-wife's telephone with an illegal wiretap, breaking and entering a client corporation's facilities, and refusing to turn in information about alleged criminals.

I hope this is of interest.

**Yevgeny Zamyatin**

*For a reply to last issue's Captain Zap article, turn to page 16.*

## Gripes and Feedback

**Dear 2600:**

Hi. I am one of your numerous subscribers and interested readers who has a few gripes with the Spring 1988 issue of *2600*.

Although I don't mind the new format and appreciate its larger size I think it could stand somewhat better editing.

"The Threat of Computer Hackers." One or two nice anecdotes but the rest should have gone into *Byte* or *Compute!* I mean you can assume that you have more enlightened readers on that subject that don't need a "HCK-100 BBS & Systems Intro".

*(continued on next page)*

# YOUR LETTERS

"ROLM Phone System." You could have cut this to one or two pages. About 50 percent of the article is fluff, like the complaints that people can't use the new phone with those weird buttons. Times change faster than humans and some of the complaints are hardly worthy of the reader's time. So what if the info number changes from 246-3636 to 632-6830?

Given a larger magazine this wouldn't be so bad, but *2600* is relatively small and so I'd prefer more and shorter articles (if they exist).

OK. What I LIKED: "Monitoring TVRO." Although I am no phreak I love to read stuff like that just to keep informed.

"VM/CMS." Although I hope I will never be on a system like that it might come in handy sometime.

"Weathertrak." Not my real interest, but interesting nevertheless.

"From the *2600* Files." Fun and informative.

"Happenings" and "Letters". These are my favorites.

I hope you don't mind a little feedback from a reader.

Best of luck to you and your mag.

**Natuerlich!**

*We never mind getting comments and criticism. It shows that our subscribers are reading the magazine. What more could we ask for?*

*We presented Captain Zap's article ("Threat of Computer Hackers") not as a revelation but as an example of what is being said by some. We did this with the intention of opening up a dialogue which, judging from the response in this issue and on the boards, is precisely what happened.*

*The ROLM article was meant to illustrate more than the simple inconvenience of having to adjust to something new. We were attempting to point out how it's becoming increasingly common for the installers of such systems to blatantly disregard the needs of the users and just assume everyone will figure it out in the end. Being denied the freedom to select an easy-to-remember phone number seemed particularly ironic, considering user flexibility was one of the "advantages" of this new phone system.*

*By the way, another page that we got lots of comment on was the reprint of our six-cent RCI phone bill that's been showing up faithfully here every month for nearly two years. Well, guess what? RCI must be reading these pages because we suddenly stopped getting them. (Maybe we should reprint our $200 MCI bill and hope that goes away!)*

## A Useful Trick

**Dear 2600:**

Just a note from a subscriber. I love *2600*. It gives a lot of food for thought.

A contribution: On the AT&T Horizon PBX (lately discontinued) there is a "toll-restriction" feature. Ports can be connected to a special card that enforces toll-restriction: i.e., you can't dial 1+ for long distance. The software knows about this too. If you try to dial 1+, you'll get a fast busy tone to let you know it's forbidden. However, the hardware is expensive to modify and it's the software that gives the busy tone, so many companies just let the software do the toll-restriction and don't bother buying the special hardware.

Mistake. If you are on such a system and get the fast busy, just hang on the line for about 30-45 seconds. Presto! Unrestricted dial tone. Most people give up when they hear the fast busy.

Also, here in Atlanta the digital exchanges (Northern Telecom DMS-100's) are programmed so that 940-xxxxxxx (where x is any digit) will tell you the number you're calling from.

Have fun and keep up the good work.

*Your little trick for getting an unrestricted dial tone is probably the single most common technique that exists. And what's so remarkable about it is that so many companies seem completely unable or even unwilling to put a stop to it! We urge our readers to try this on any system that offers any kind of dialing restrictions. Please let us know what you find.*

*We appreciate the ANI (Automatic Number Identification) information. If readers from other parts of the country know what their ANI numbers are, please let us know. (In the New York metro area, it's 958.)*

## "Deluxe" Call Waiting

**Dear 2600:**

Enclosed is another example of how Ma Bell loves screwing the telecommunicating public. This was clipped from "On Line Today", the Compuserve magazine. On one page is a letter in which the writer thanks another correspondent for advice on temporarily suspending call

(continued on page 39)

# Protection From Computer Viruses

(continued from page 7)

I guess the programmer involved was too cowardly to take me up on my offer and prefers to hurt people not capable of fighting back. I should have known that, I suppose, but I don't normally think of people who attack innocents. Normally, I think of people to respect, not people to pity, certainly not people who must cause such damage in order to "get off".

They are below contempt, obviously, and can do little to help themselves out of the mire they live in.

Still, a worm is a worm.

### About FLUSHOT
### A Brief History

The original incarnation of FLUSHOT was a quick hack done in my spare time. It had a couple of bugs in it which caused it to trigger when it shouldn't, and a few conditions which I had to fix. A strangeness in how COMMAND.COM processed certain conditions when I "failed" an operation caused people to lose more data than they had intended -- certainly not my intent!

> *"No matter what software protection you use, somebody will find a way around it one day."*

FLUSHOT was modified and became FLUSHOT2. It included some additional protections, protecting some other important system files, and protecting against direct disk writes which can be used to circumvent FLUSHOT's protection mechanisms.

Additionally, FLUSHOT2 forced an exit of the program currently running instead of a fail condition when you indicated that an operation should not be carried out.

FLUSHOT2 was also now distributed in the popular archive format (have you remembered to send your shareware check in to Phil Katz for his efforts? You really should. It ain't that much money!).

Next came FLUSHOT3. A bug was fixed which could have caused certain weird things when you denied direct disk I/O to certain portions of DOS 3.x.

The enhancements to FLUSHOT3 included the ability to enter a 'G' when FLUSHOT was triggered. This allowed FLUSHOT to become inactive until an exit was called by the foreground task. So, when you used some trustworthy program which did direct disk I/O, you wouldn't be pestered with constant triggering after you enter the 'G'. Primarily this was a quick hack to allow programs such as the FORMAT program to run without FLUSHOT being triggered each time it tried to do any work it was supposed to.

Additionally, a CMOS RAM check was installed. If a foreground program attempted to change CMOS memory, you'd be advised.

What the heck is CMOS memory, you might be asking. Good question. In AT class and better machines, certain important parameters (such as the type of hard disk you're using, or how much memory there is in your machine) are stored up in special non-volatile memory, called CMOS.

If this gets changed, you might have a problem when you reboot. FLUSHOT3 sends at least one little slimebucket back to the drawing board, because it will restore the CMOS and prevent this hassle from occuring.

### FLUSHOT+ Features
### and Enhancements

This release of FLUSHOT has a new name: FLUSHOT+. Because FLUSHOT4 was a Trojan, I opted to change the name. Besides, FLUSHOT+ is the result of some real effort on my part, instead of being a part-time quick hack. I hope the effort shows.

FLUSHOT is now table driven. That table is in a file which I call FLUSHOT.DAT. It exists in the root directory on your C: drive. However, I'll advise you later on how to change its location so that a worm can't create a Trojan to modify that file.

This file now allows you to write and/or read protect entire classes of programs. This means that you can write protect from damage all of your *.COM, *.EXE, *.BAT, and *.SYS files. You can read protect all of your *.BAT files so that a nasty program cannot even determine what name you used for FLUSHOT+ when you invoked it!

Additionally, you can now automatically check programs when you first invoke FLUSHOT+ to determine if they've changed since you last looked at them. Called checksumming, it allows you to know immediately if one of the protected programs has been changed when you're not looking. Additionally, this checksumming can even take place each time you load the program for execution.

Also, FLUSHOT+ will advise you when any program "goes TSR". TSR stands for "Terminate and Stay Resident", allowing pop-ups and other useful programs to be created. A worm could create a program which leaves a bit of slime behind. Programs like Borland's SideKick program, a wonderful program and certainly not a Trojan or virus, is probably the best known TSR. FLUSHOT+ will advise you if any program attempts to go TSR which you haven't already registered in your FLUSHOT.DAT file.

Finally, FLUSHOT+ will also now pop-up a little window in the middle of your screen when it gets triggered. It also will more fully explain why it was triggered. The pop-up window means that your screen won't get screwed up beyond recognition -- unless you're in graphics mode when it pops up. Sorry, 'dems the breaks!

### Registering FLUSHOT+

FLUSHOT+ is not a free program. You're encouraged to use it, to distribute it to your friends and co-workers. If you end up not using it for some reason, let me know why and I'll see if I can do something about it in the next release.

But, the right to use FLUSHOT+ is contingent upon you paying for the right to use it. I ask for ten dollars as a registration fee. This entitles you to get the next update shipped when available. And allows you to pay me, in part, for my labor in creating the entire FLUSHOT series. I don't expect to get my normal consulting rate or to get a return equal to that of other programs which I've developed and sell through more traditional channels. That's not my intent, or I would have made FLUSHOT+ a commercial program and you'd be paying lots more money for it.

Some people are uncomfortable with

(continued on next page)

# A Flu Shot For Personal Computers

the shareware concept, or believe that there ain't no such thing as Trojan or virus programs, and that a person who profits from the distribution of a program such as FLUSHOT must be in it for the money.

I've created an alternative for these folks. I'll call it "charityware" [first called that, to my knowledge, by Roedy Green]. You can also register FLUSHOT+ by sending me a check for $10 made out to your favorite charity. Be sure to include a stamped and addressed envelope. I'll forward the monies onto them and register you fully.

Of course, if you wish, you can send me a check for more than $10. I'll cash it gladly (I'm no fool!).

**Site Licensing of FLUSHOT+**

So, you run the computer department of a big corporation, you got a copy of FLUSHOT+, decided it was wonderful and that it did everything you wanted and sent in your ten bucks. Then you distributed it to your 1000 users.

Not what is intended by the shareware scheme. *Each* site using FLUSHOT+ should be registered. That's ten bucks a site, me bucko! Again, make the check out to charity if you're uncomfortable with the idea of a programmer actually deriving an income from their work.

However, if you've really got 1000 computers, you should give me a call. As much as I'd like to get $10 for each site, that wouldn't be fair to you. So, quantity discounts are available.

**The FLUSHOT.DAT file**

FLUSHOT+ is table-driven by the contents of the FLUSHOT.DAT file. This file normally exists in the root directory of your C: drive (C:\FLUSHOT.DAT).

A little later in this article you'll see how to disguise the data file name, making life tougher for the worms out there. But for the purpose of this article, we'll assume that the file is called C:\FLUSHOT.DAT.

The FLUSHOT+ program will read this data file exactly once. It reads the data from the data file into memory and overwrites the name of the data file in so doing. A little extra protection in hiding the name of the file.

This data file contains a number of lines of text. Each line of text is of the form:

```
(Command)=(filename)(options)
```

Command can be any one of the following characters:

P - Write Protect the file named.

R - Read Protect the file named.

E - Exclude the file named from matching P or R lines.

T - The named file is a legitimate TSR.

C - Perform checksum operations on the file named.

The filename can be an ambiguous file if you wish for all commands except the 'T' and 'C' commands. This means that:

```
C:\level1\*.COM
```

will specify all COM files on your C: drive in the level1 directory (or its subdirectories). Specifying:

```
C:\level1\*\*.EXE
```

would specify all EXE files in subdirectories under the C:\level1 directory, but would not include that directory itself.

You can also use the '?' operator to specify ambiguous characters as in:

```
?:\usr\bin\?.COM
```

which would be used to specify files on any drive in the \usr\bin directory on that drive. The files would have to be single letter filenames with the extension of 'COM'.

Ambiguous file names are not allowed for the 'T' and 'C' options.

**Protecting files from Write Access**

Use the 'P=' option to protect files from write access. To disallow writes to any of your COM, EXE, SYS, and BAT files, specify lines of the form:

```
P=*.COM
P=*.EXE
P=*.SYS
P=*.BAT
```

which protects these files on any disk, in any directory.

**Protecting files from Read Access**

Similarly, you can use the 'R' command to protect files from being read by a program (including the ability to 'TYPE' a file!). To prevent read access to all of your BAT files, use a line such as:

```
R=*.BAT
```

Combinations of R and P lines are allowed, so the combination of the above lines would prevent read or write access to all batch files.

> *"I challenge them to upload a virus or other Trojan horse to my BBS that I can't disarm."*

**Excluding files**

Programmers in particular should find usage for the 'E' command. This allows you to exclude matching filenames from other match operations. Assume you're doing development work in the C:\develop directory.

You could exclude FLUSHOT+ from being triggered by including a line such as:

```
E=C:\develop\*.*
```

Of course, you might have development work on many disks under a directory of that name. If you do, you might include a line which looks like:

```
E=?:\develop\*.*
or
E=*\develop*
```

**Checksumming files**

This line is a little more complicated than others and involves some setup work. It's worth it, though!

A checksum is a method used to reduce a file's validity into a single number. Adding up the values of the bytes which make up the file would be a simple checksum method. Doing more complex mathematics allows for more and more checking information to be included in a test.

If you use a lie on the form:

```
C=C:\COMMAND.COM[12345]
```

then when FLUSHOT+ first loads it will check the validity of the file against the number in the square brackets. If the checksum calculated does not match the number presented, you'll be advised with a triggering of FLUSHOT, which presents the correct checksum.

When you first set up your FLUSHOT.DAT file, use a dummy number such as '12345' for each of the files you wish to checksum. Then, when you run FLUSHOT, you should copy down the "erroneous" checksum presented. Then, edit the FLUSHOT.DAT file and replace the dummy number with the actual checksum value you had copied down. Voila! If even one byte in the file is changed, you'll

(continued on next page)

# Controlling the Epidemic

be advised the next time you run FLUSHOT+.

But wait! There's more!

When a "checksummed" file is loaded by MS-DOS, it will, by default, be checksummed again. So, if you had a line such as:

```
C=C:\usr\bin\WS.COM[12345]
```

the venerable old WordStar program (still *my* editor of choice!) would be checksummed each time you went to edit a file.

Of course, you might not want the overhead of that checksumming to take place each time you load a program. Therefore, a few switches have been added. The switches are placed immediately after the ']' in the checksum line:

```
C=C:\usr\bin\WS.COM[12345](switch)
```

These switches are:

,n: will only checksum the file only 'n' times. Only one digit allowed.

-: only checksum this file when FLUSHOT+ first loads. ',1' and '-' are equivalent.

+: only checksum this file when it is loaded and executed, not when FLUSHOT+ first loads.

Therefore, if you wished to only check your WS.COM file when you first loaded the FLUSHOT+ program, you'd specify a line as:

```
C=C:\usr\bin\ws.com[12345],1
or
C=C:\usr\bin\ws.com[12345]-
```

If you wished to checksum your program called "MYPROG.EXE" only when it was used, try:

```
C=C:\path\MYPROG.EXE+
```

**Registering a TSR program**

Any unregistered TSR program which is run after FLUSHOT+ will cause a trigger when they "go TSR". You can register a program so no trigger goes off by specifying it in a line such as:

```
T=C:\usr\bin\tsr sisk.com
```

which will keep FLUSHOT+ from complaining about sk.com. Make sure to take a look at the '-T' option, specified in the next section.

**Protecting the FLUSHOT.DAT file**

Obviously, the weak link in the chain of the protection which FLUSHOT+ offers you is the FLUSHOT.DAT file.

You would think that you'd want to protect the FLUSHOT.DAT file from reads and writes as specified above. However this, too, leaves a gapping security hole: memory could be searched for it, and it could be located that way. A better alternative exists. In the distribution package for FLUSHOT+ exists a program called FLUPOKE.COM. This program allows you to specify the new name you wish to call the FLUSHOT.DAT file. Simply type:

```
FLUPOKE (flushot name)
```

where (flushot name) represents the full path filename of your copy of FLUSHOT+.

You'll be prompted for the name of the FLUSHOT.DAT file. Enter the name you've selected (remember to specify the disk and directory as part of the name). Voila! Nothing could be easier.

**Protection Recommendations**

Here's a sample FLUSHOT.DAT file, basically the same one included in the archive. Your actual checksums will differ, and you may want to modify what files and directories are protected. Obviously, your exact needs are different than mine, so consider this a generic FLUSHOT.DAT:

```
P=*.bat
P=*.sys
P=*.exe
P=*.com
R=*AUTOEXEC.BAT
R=*CONFIG.SYS
E=?\dev\*
C=C:\COMMAND.COM[12345]-
C=C:\IBMBIO.COM[12345]-
C=C:\IBMDOS.COM[12345]-
```

**Running FLUSHOT+**

For extra protection, after you've run FLUPOKE, you should rename the FLUSHOT+ program to something unique and meaningful to you, but not a worm.

Assuming you didn't rename it, however, you could invoke the program simply by typing:

```
FSP
```

when at the prompt. That's all there is to it. When you're satisfied, you can add it to your AUTOEXEC.BAT file, after all of your trusted programs have run.

But there are some options you should know about:

**Checking CMOS - How often?**

The CMOS, as described earlier in this article, is a spot wherein a worm can just make things a bit miserable for you when you next boot your system. However, FLUSHOT+ allows you to protect the contents of your CMOS against such a worm.

CMOS only exists on AT class and better machines!!!

You must specify the '-C' option when you invoke the FLUSHOT+ program in order to have your CMOS safeguarded. There is a check done whenever DOS is accessed to determine if the CMOS has changed. This causes a slight performance penalty. However, this only happens once every 128 DOS accesses. You can modify this ratio, to more or less, by specifying a number after the '- C':

```
FSP -C10
```

will check CMOS every ten accesses.

**Intercepting Direct Disk Writes Through INT13**

The default operation of FLUSHOT+ is to intercept and examine every call to the direct disk routines. You can disable this by including the '-F' switch on your command line:

```
FSP -F
```

This is not recommended, but exists primarily for developers who can't use the constant triggering one of their programs may cause.

**What about INT26?**

Similarly, the same exists for the direct writes which normally are only made by DOS through interrupt 26. Again, I do not recommend you disable the checking, but

(continued on next page)

---

HOLLAND BBS'S
by John Drake

| | |
|---|---|
| Flevolands Brandon BBS | 80 54 73 63 (3/12) |
| Amsterdam | 20 15 41 54 |
| Rozenburg | 18 19 18 56 8 |
| Amersfoort | 33 75 54 44 |
| Eindhoven | 40 18 17 92 |
| Leiden | 71 12 51 25 |
| Staard | 47 55 20 41 |
| Arnhem | 85 25 55 77 |
| Kampen | 52 02 24 38 8 |
| Groningen | 50 14 51 45 |
| Hoorn | 22 90 34 84 6 |
| Almelo | 54 90 62 54 1 |
| Middelburg | 11 80 34 33 6 |
| Venlo | 77 82 25 22 |
| Zoetermeer | 79 51 04 25 (V/12) |
| Apeldoorn | 55 21 18 11 |
| Den Haag | 70 28 50 88 |
| Hengelo | 41 25 25 32 |
| Alkmaar | 72 12 67 83 |
| Rotterdam | 10 48 34 23 5 |
| Gouda | 18 20 22 31 4 |
| Emmen | 59 10 21 00 8 |
| CP/M BB | 74 42 16 60 (3) |
| IBM PC BB | 22 86 14 21 (3) |
| MSX BB | 20 96 25 02 (3) |
| Sharp/MZ BB | 52 40 38 86 5 |
| CP/M SW line 70 69 40 81 | |
| P2000 BB | 10 47 05 73 2 |
| Olivetti BB | 79 51 75 75 |
| Apple BB | 15 62 34 31 (3) |
| NOS Hobby Scoop | 35 45 39 5 (3) |
| Fido Gouda | 47 84 25 01 (3) |
| Fido John | 40 53 14 33 (3) |
| Fido Scotch | 34 88 83 9 |

# Virus and Trojan Prevention

if you desire to do so, use the '-D' switch.

**Turning off the header message**

If you've no desire to see the rather lengthy welcome message which is displayed when you first use FLUSHOT+, use the '-h' switch.

**Allowing Trusted TSR's to Work**

Normally, you'd load all of your trusted TSR's before FLUSHOT+ is loaded from within your AUTOEXEC.BAT file. However, you might want to use SideKick once in a while, removing it from memory as you desire. This could cause some problems, since SideKick, and programs like it, take over certain interrupts, and FLUSHOT+ could get confused about whether this is a valid call or a call that shouldn't be allowed. Normally, FLUSHOT+ will trigger on these calls, which is safer, but can be annoying. If you use the special '-T' switch upon program invocation, then calls which trusted TSR's (those specified with the 'T=' command in your FLUSHOT.DAT file) make will be allowed. Understand, please, that this basically means that calls made by a Trojan while a trusted TSR is loaded may not be caught. Please, use this switch with caution!

**Disabling FLUSHOT+**

There may be times when you're about to do some work which you know will trigger FLUSHOT+. And you might not want to be bothered with all of the triggering, the pop-up windows, and your need to respond to each trigger. If you look in the upper right hand corner of your screen, you'll see a '+' sign. This indicates that FLUSHOT+ is monitoring and attempting to protect your system. Depress the ALT key three times. Notice that the '+' sign turned into a '-'? Well, FLUSHOT+ is now disabled, and will not trigger on any event. If you depress the ALT key three more times, you'll see the '-' turn back into a '+' - - each time you depress the ALT key three times, FLUSHOT+ will toggle between being enabled and disabled.

**Disabling FLUSHOT+ Toggle Display**

Alas, there are graphics applications which will be screwed up by the '-' or '+' in the upper right hand corner of your display. Therefore, if you depress the CTRL key three times, you'll be able to toggle the display capability of FLUSHOT+. The default configuration of FLUSHOT+ is to "come up" with display turned on. You can reverse this capability if you include the '-G' (for graphics) switch on your command line when you run FLUSHOT+.

> *"All of the protection I had would have been for naught if I didn't use the first line of defense from these worms: full and adequate backup."*

**Interpreting a FLUSHOT+ Trigger**

So, you've run FLUSHOT+, and you're at your C> prompt. Great! Now stick a blank disk which you don't care about into your A: drive and try to format it.

Surprise! FLUSHOT+ caught the attempt! You have three choices now: typing 'Y' allows the operation to continue, but the next one will be caught as well. Typing a 'G' (for Go!) allows the operation to continue, disabling FLUSHOT+ until an exit from the program is made. When FLUSHOT+ is in the 'G' state, a 'G' will appear in the upper right hand corner of your screen.

Any other key will cause a failure of the operation to occur.

When you've got FLUSHOT+ running and you get signaled that there is a problem, you should think about what might have caused the problem. Some programs, like FORMAT, or the Norton Utilities, PC-Tools, or DREP have very good reasons for doing direct reads and writes to your hard disk. However, a public domain checkbook accounting program doesn't. You'll have to be the judge of what are legitimate operations and which are questionable.

There is no reason to write to IBMBIO or IBMDOS, right?

Wrong!

When you format a disk with the '/S' option, those files are created on the target diskette. The act of creating, opening up, and writing those files will trigger FLUSHOT+ as part of its expected operation. There are many other legitimate operations which may cause FLUSHOT+ to trigger.

So will copying a COM or EXE file if you have those protected with a 'P=' command. FLUSHOT+ is not particularly intelligent about what is allowed and what isn't. That's where you, the pilot, get to decide.

Here's a fuller listing of the messages which you might see when you're using FLUSHOT+:

**Checking ===)(filename)**

This message is displayed as FLUSHOT+ checks the checksum on all of the "C=" files when you first invoke FLUSHOT+. The files must be read in from disk, their checksum calculated and then compared against the value you claim the checksum should equal.

If the checksum does *not* equal what you claim it should (which means that the file may have been written to and might therefore be suspect), a window will pop up in the middle of your screen:

**Bad Checksum on (filename)**

**Actual Checksum Is: (checksum)**

**Press "Y" to allow, "G" to go till exit, any other key to exit.**

This message simultaneously advises you there is a problem with the checksums not matching, shows you what the checksum should be, and then awaits your response.

Except for the initial run of FLUSHOT+, if you type a 'Y' or a 'G', then the program will load and execute. Typing any other key will cause the program to abort and you will be returned to the C> prompt. When FLUSHOT+ is in the 'G' state, a 'G' will appear in the upper right hand corner of your screen.

If this is the initial run of FLUSHOT+, however, you'll be advised of the program's actual checksum, but FLUSHOT+ will continue to run, checking all remaining "C=" files in the FLUSHOT.DAT file.

If you're running a program and you see a screen like:

**? WARNING! TSR Request from an unregistered program!**

**Number of paragraphs of memory requested (in decimal) are: (cnt)**

**(Press any key to continue)**

you're being advised that a program is

*(continued on next page)*

# Controlling the Infection

about to go TSR. If this is a program you trust (such as SideKick, or KBHIT, or a host of other TSR programs you've grown to know and love), then you should considering installing a "T=" line in the FLUSHOT.DAT file so that future runs of this program will not trigger FLUSHOT+.

However, if you get this message when running a program you don't think has any need to go TSR (such as the proverbial checkbook balancing program), you should be a little suspicious. Having a TSR program is not, in and of itself, something to be suspicious of. But having one you don't expect --- well, that's a different story.

Most TSR's "hook into" an interrupt vector before they go TSR. These hooks might intercept and process key strokes ("hotkeys"), or they might hook and intercept direct disk writes themselves. In any event, FLUSHOT+ (in this version!) doesn't have the smarts to do more than advise you of the TSR'ing of the program. If you're truly suspicious, reboot your machine immediately!

If a program attempts to write directly to the interrupts which are reserved for disk writes, FLUSHOT+ will also be triggered and you'll see something like:

**Direct Disk Write attempt by program other than DOS!**

**(From Interrupt (xx))**

**Press "Y" to allow, "G" to go till exit, any other key to fail.**

where the (xx) represents either a 13 (indicating a direct BIOS write to the disk) or a 26 (indicating a direct DOS write). Again, pressing a 'Y' or a 'G' allows the operation to continue, pressing any other key will cause the operation to return a failed status to DOS, and the operation will not take place. When FLUSHOT+ is in the 'G' state, a 'G' will appear in the upper right hand corner of your screen.

If an attempt is made to format your disk, which may be a legitimate operation made by the DOS FORMAT program, you'll see a message such as:

**Disk being formatted! Are You Sure?**

**Press "Y" to allow, "G" to go till exit, any other key to fail.**

which follows similarly to the direct disk write operations. You should question whether the format operation is appropriate at the time and take whatever action you think is best.

If one of your protected files is about to be written to, you'll see a message like:

**Write access being attempted on:**

**(filename)**

**Press "Y" to allow, "G" to go till exit, any other key to fail.**

where (filename) represents the file you're trying to protect from these write operations. Your red flag should fly, and you should question why the program currently running should cause such an operation.

You may also see the same type of message when one of your "Read-Protected" files is being accessed:

**Read Access being attempted on:**

**(filename)**

**Press "Y" to allow, "G" to go till exit, any other key to fail.**

Again, the same red flag should fly, but it doesn't mean that you're infected with some nasty virus program! It could be something harmless or intended. You'll have to be the judge.

Finally, you may see a message like:

**CMOS has been changed!**

**Hit "Y" to continue, any other key to restore CMOS.**

which indicates that your CMOS has been changed while you weren't looking. Or maybe you were: if you're running a setup program which changes the date or the time, or the disk type attached to your AT class machine, this message should pop up. Losing your CMOS is not fatal, but can be an annoyance. If you hit a 'Y', then the new setting of the CMOS will be stored and you'll be able to continue, with alerts to any other change to the CMOS. Any other key will result in the original setting of the CMOS being restored.

**How Good is FLUSHOT+, Really?**

FLUSHOT+ is a pretty handy piece of code. But it can't absolutely protect you from a worm. No software can do that.

There are ways around FLUSHOT+. I'm of two minds about discussing them, since the worms out there are reading this, too. So I'll only discuss them in passing. And I'll tell you what I use here to protect myself from worms. First, though, a little story to tell you what it's like here, and how I protect myself from getting wormed.

The RamNet Bulletin Board System site I run is open access. No need to register, or to leave your phone number or address, although a note to that effect is always appreciated. As mentioned above, I dare the worm to try to affect the disk of somebody who can fight back. A couple of worms have tried and I have a nice collection of Trojans and viruses. Obviously, I run FLUSHOT+ on my board, along with checking incoming files with CHK4BOMB. My procedure for testing out newly uploaded code involves me doing a backup, installing all sorts of software to monitor what is going on, and doing a checksum on all files on the disk. I then try out all of the code I get, primarily to determine if the code is of high enough quality to be posted. After testing out all of the week's uploads, I run the checksum program again to determine if any of my files might have been modified by a worm's virus program.

Recently, what looked like a decent little directory lister was posted to the board. For some reason I've yet to fathom, directory aid programs seem to be the ones

(continued on next page)

*To obtain more information on FLU SHOT+, contact Ross Greenberg at Software Concepts Design, 594 Third Avenue, New York, NY 10016. Or call his BBS at (212) 889-6438 1200/2400 N/8/1*

# Controlling the Infection

about to go TSR. If this is a program you trust (such as SideKick, or KBHIT, or a host of other TSR programs you've grown to know and love), then you should considering installing a "T=" line in the FLUSHOT.DAT file so that future runs of this program will not trigger FLUSHOT+.

However, if you get this message when running a program you don't think has any need to go TSR (such as the proverbial checkbook balancing program), you should be a little suspicious. Having a TSR program is not, in and of itself, something to be suspicious of. But having one you don't expect -- well, that's a different story.

Most TSR's "hook into" an interrupt vector before they go TSR. These hooks might intercept and process key strokes ("hotkeys"), or they might hook and intercept direct disk writes themselves. In any event, FLUSHOT+ (in this version!) doesn't have the smarts to do more than advise you of the TSR'ing of the program. If you're truly suspicious, reboot your machine immediately!

If a program attempts to write directly to the interrupts which are reserved for disk writes, FLUSHOT+ will also be triggered and you'll see something like:

**Direct Disk Write attempt by program other than DOS!**

**(From Interrupt (xx))**

**Press "Y" to allow, "G" to go till exit, any other key to fail.**

where the (xx) represents either a 13 (indicating a direct BIOS write to the disk) or a 26 (indicating a direct DOS write). Again, pressing a 'Y' or a 'G' allows the operation to continue, pressing any other key will cause the operation to return a failed status to DOS, and the operation will not take place. When FLUSHOT+ is in the 'G' state, a 'G' will appear in the upper right hand corner of your screen.

If an attempt is made to format your disk, which may be a legitimate operation made by the DOS FORMAT program, you'll see a message such as:

**Disk being formatted! Are You Sure?**

**Press "Y" to allow, "G" to go till exit, any other key to fail.**

which follows similarly to the direct disk write operations. You should question whether the format operation is appropriate at the time and take whatever action you think is best.

If one of your protected files is about to be written to, you'll see a message like:

**Write access being attempted on:**

**(filename)**

**Press "Y" to allow, "G" to go till exit, any other key to fail.**

where (filename) represents the file you're trying to protect from these write operations. Your red flag should fly, and you should question why the program currently running should cause such an operation.

You may also see the same type of message when one of your "Read-Protected" files is being accessed:

**Read Access being attempted on:**

**(filename)**

**Press "Y" to allow, "G" to go till exit, any other key to fail.**

Again, the same red flag should fly, but it doesn't mean that you're infected with some nasty virus program! It could be something harmless or intended. You'll have to be the judge.

Finally, you may see a message like:

**CMOS has been changed!**

**Hit "Y" to continue, any other key to restore CMOS.**

which indicates that your CMOS has been changed while you weren't looking. Or maybe you were: if you're running a setup program which changes the date or the time, or the disk type attached to your AT class machine, this message should pop up. Losing your CMOS is not fatal, but can be an annoyance. If you hit a 'Y', then the new setting of the CMOS will be stored and you'll be able to continue, with alerts to any other change to the CMOS. Any other key will result in the original setting of the CMOS being restored.

**How Good is FLUSHOT+, Really?**

FLUSHOT+ is a pretty handy piece of code. But it can't absolutely protect you from a worm. No software can do that.

There are ways around FLUSHOT+. I'm of two minds about discussing them, since the worms out there are reading this, too. So I'll only discuss them in passing. And I'll tell you what I use here to protect myself from worms. First, though, a little story to tell you what it's like here, and how I protect myself from getting wormed.

The RamNet Bulletin Board System site I run is open access. No need to register, or to leave your phone number or address, although a note to that effect is always appreciated. As mentioned above, I dare the worm to try to affect the disk of somebody who can fight back. A couple of worms have tried and I have a nice collection of Trojans and viruses. Obviously, I run FLUSHOT+ on my board, along with checking incoming files with CHK4BOMB. My procedure for testing out newly uploaded code involves me doing a backup, installing all sorts of software to monitor what is going on, and doing a checksum on all files on the disk. I then try out all of the code I get, primarily to determine if the code is of high enough quality to be posted. After testing out all of the week's uploads, I run the checksum program again to determine if any of my files might have been modified by a worm's virus program.

Recently, what looked like a decent little directory lister was posted to the board. For some reason I've yet to fathom, directory aid programs seem to be the ones

(continued on next page)

*To obtain more information on FLU SHOT+, contact Ross Greenberg at Software Concepts Design, 594 Third Avenue, New York, NY 10016.*
*Or call his BBS at (212) 889-6438*
*1200/2400 N/8/1*

which have the highest percentage of Trojans attached to them.

This directory aid program listed my directories in a wonderful tree structure, using different colors for different types of files. Nice program. When it exited, however, it went out and looked for a directory with the word "FLU" in it. Once it found a directory with a match in it, it proceeded to try to erase all of the files in that directory. An assault! No big deal. That's what backups are for.

But it brings up an interesting point: I was attacked by a clever worm, and it erased a bunch of files which were pretty valuable. All of the protection I had would have been for naught if I didn't use the first line of defense from these worms: full and adequate backup.

I've spent three years of my life developing one particular software package. Imagine what would have happened if that had been erased by a worm! Fortunately, I make backups at least once a day, and usually more frequently than that. You should, too.

Now, I quarantine that machine as well. I spent a couple of dollars and bought a bunch of bright red floppy disks. The basic rule around here is that Red Disks are the only disks that go into the BBS machine, and the Red Disks go into no other machine. You see, I *know* that there is some worm out there who is gonna find some way to infect my system. No matter what software protection I use, there *is* a way around it.

You needn't be concerned though -- you're making backups on a regular basis, right? And you aren't asking for trouble. I am, I expect to find it, and it is sort of amusing to see what the worms out there are wasting their efforts on.

At this point, Trojans and viruses are becoming a hobby with me: watching what the worms try to do, figuring out a way to defend against it, and then updating the FLUSHOT series.

However, there is a possibility that the FLUSHOT series (as well as other protection programs which are just as valuable) are causing an escalation of the terms of this war. The worms out there are sick individuals. They must enjoy causing the damage they do. But they haven't the guts to stand up and actually do something in person. They prefer to hide behind a mist of anonymity.

But you have the ultimate defense! No, not the FLUSHOT+ program.

*Full and adequate backups!*

There are a variety of very good backup programs which can save you more work than you can imagine. I use the FASTBACK+ program, which is a great little program. I backup 30 megs once in a while, and do an incremental backup on a very frequent basis. There are a variety of very good commercial, public domain, and shareware backup programs out there. Use them! Because, no matter what software protection you use, somebody will find a way around it one day. But they can't find a way around your backups. And, if you (and everyone else) do regular backups, you'll remove the only joy in life these worms have. They'll kill themselves, hopefully, and an entire subspecies will be wiped out -- and you'll be partially responsible!

My advance thanks for helping to exterminate these little slimebuckets.

(continued from page 27)

waiting (by dialing *70 or 1170). On the very next page is a news release from Bellcore about deluxe call waiting, which lies about the newest "multitiered" feature to suspend call waiting. As usual, the liars want to charge for a "new" feature which already exists. This is typical of the genius mind of Ma Bell. I hope that you will illustrate this abuse in your summer issue.

Also, I have mixed feelings regarding the quarterly format. But, as usual, it's worth the wait.

**GH**

*We actually did point that injustice out in a previous issue. While it isn't completely a lie (it seems somebody did invent something a little bit different that does basically the same thing as the old "*70"), it certainly qualifies as misleading the public.*

## New Falwell Numbers

**Dear 2600:**

I just got ahold of the new toll-free numbers for Jerry Falwell's All Time Gospel Hour! They are 800-345-8095 and 800-453-3800.

**A True Believer**

*It's amazing how popular these numbers are in the hacker world. We did a little checking (we called 800 info) and got 800-325-3388. Three toll-free numbers! Scary, isn't it?*

## What is Sprint Up To?

**Dear 2600:**

The very day that I received your Spring issue, I also got my Sprint bill. I read your issue first, of course, and I didn't touch my bill until I read your little blurb about Sprint's billing system in your "Happenings" column. And was I in for a surprise.

My bill was a total mess! Sprint had done two things to my bill as far as I could fathom from the mess printed on those pages. 1) They had charged me for busy signal calls. 2) They had chopped up large calls into 4 or 5 smaller calls.

I called Sprint right away and had it out with the billing person. He gave me credit for all of the one minute busy calls (about 40 altogether). As for why they did this in the first place I don't know. Is their billing computer really that messed up that they can't keep track of the status of a call? They must have a lot of this happening, because he gave

(continued on next page)

# 2600 LETTERS

me credit without too much of a problem.

As for the chopped up calls, that's a different matter altogether. He refused to change my billing to make the series of smaller calls into one big call. I'll have to write the company about that one.

Here is what I would like you guys to think about: We all know about those thieves who reprogram a bank's computer to shave off .00001 percent of all the accounts in the bank and drop it into another account for themselves. The small amount taken from the individual accounts will be insignificant for anyone to notice, but the total amount can be quite large. Well, here we have a long distance company that is cutting up callers' long calls into smaller calls and then charging the callers more for the first minute on all of the small calls. This amount is small and I don't really care about it. But if they're doing this to ALL callers--how much are they actually making per month?

**Cray-Z Phreaker**
**Skunk Works**

*What you're implying here is a very serious matter. If Sprint is in fact doing this, they could be facing an awful lot of trouble (something a lot of phone phreaks would no doubt relish). Let's find out for sure. Let's all put them to the test and keep logs. In fact, why not do it for all of the companies?*

---

***If you have a letter for us, send it to:***

***2600 Letters***
***P.O. Box 99***
***Middle Island, NY 11953***

***Or send it electronically using our bulletin boards or network addresses listed in our staffbox.***

NORWAY BBS'S BY JOHN DRAKE

| | |
|---|---|
| Bogus Byte | 5 32 62 86 |
| Big Blue | 2 42 96 98 |
| Casa de Vinduene | 5 15 36 10 |
| DAF BBS | 2 15 96 87 |
| DASAN | 3 45 85 30 |
| Datakjelleren | 3 65 92 53 |
| Firefly Data Club | 3 92 89 53 |
| Hackers Unlimited | 3 34 37 45 |
| Haugaland RBBS | 4 71 40 46 |
| HC Info 9.35 | 3 35 45 74 |
| Hot Stuff BBS | 2 30 45 06 |
| Modula-2 Klubb | 8 57 33 33 |

U.K. BBS'S BY JOHN DRAKE

| | |
|---|---|
| TBBS | 348 9400 |
| London Underground | 863 0198 |
| Apple 2000 | 0904 270396 |
| Apple | 0268 778565 |
| Black Tower | 474 3903 |
| The Outer Limits | 549 4640 |
| Adult PBBS | 04862 25174 |
| 666 | 0787 247604 |
| Aired | 208 7496 |
| MacTel | 0622 459441 |
| Mega Anchorage | 747 4662 |
| Twilight Zone (ST) | 739 0894 |
| BBS90 (ST) | 0705 780025 |
| Alternate Reality | 0539 75000 |
| | 264 8733 |
| Peoples Palace | 041 556 6597 |
| | 0423 855 502 |
| Dublin | 683654 |

800 BBS'S
THANKS TO DENNIS FROM L.I.
AND WBAI IN NEW YORK

| | |
|---|---|
| 800-323-7444 | 800-222-4922 |
| 800-345-6262 | 800-842-5151 |
| 800-632-7227 | |

# 2600 Marketplace

**WANTED** copied (dead) or alive! TAP'S "C" & "D" elec. courses. Cassette tape (TAP exclusive), & fact sheets #1-4. Have any or all? Contact me--willing to pay good money for orig's. B. Barton, 84 Daphne Cres., Barrie, Ontario L4M 2Y9. (705-726-6617)

**WANTED:** All newer hardware you find a must to quickly get rid of. Product evaluations are welcomed. Also looking for Technics SL1200 and any information related to pirate radio (including stories written by ex-pirates, groups, equipment information, FCC) for a write-up. David Jon Hyams, E 9116 Sprague Av., Apt. 111, Spokane, WA 99206.

**SELLING COPIES** of Abbie Hoffman's "Steal This Book". $7.95 + $2 shipping & handling. Marco, P.O. Box 1211, Westerly, RI 02891.

**FOR SALE:** Ultimate blue box, Berry Electronics Model 312A trunk test set, has rotary dial/MF keypad, monitor speaker. Uses L-C oscillators. VERY stable. Can be used as Std phone when head/handset added. $250. Write: Testset, 6715 Eberlein Ave., Klamath Falls, OR 97603.

**WANTED:** Any hacker and phreaker software for IBM compatible and Hayes compatible modem. If you are selling or know anyone who is, send replies to A.H. Moon, 25 Amaranth Crt., Toronto, ONT., Canada M6A 2P1.

**WOULD YOU LIKE TO MAKE SOME MONEY?** Big money? Send a business sized S.A.S.E. to: J. Duffy, 408 Michell St., Ridley Park, PA 19078. This plan is completely LEGAL.

**QUALITY TAP REPRINTS.** Complete set (#1-91) punched and bound. High quality copies with all special supplementals. $75/set, shipped UPS or USPS or $90/set shipped Federal Express. Money orders only, payable to Jeff. TZG, P.O. Box 1515, Columbus, NE 68601-1515.

**WANTED:** G-file "Better Homes and Blueboxing Part 2" by Mark Tabas. If anyone can provide a hardcopy, please send it to JRE, 1447 Graber Dr., Cleveland, OH 44107.

**TAP BACK ISSUES**, complete set Vol. 1-90 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid via UPS or First Class Mail. Cash/MO sent same day, checks to Pete G., P.O. Box 463, Mt. Laurel, NJ 08054. We are the original; all others are copies!

**FOR SALE:** Okidata Microline 92 personal printer. Includes manual for instructions. Hardly used. Make an offer and if it's reasonable, I will pay postage. Matt Kelly, 310 Ishell, Howell, MI 48843.

**2600 MEETINGS.** First Friday of the month at the Citicorp Center--from 6 to 8 pm in the Market (also known as the lobby with the tables where all of the weirdos hang out). Located at 153 East 53rd Street, New York City. Come by, drop off articles, ask questions. Call 516-751-2600 for still more info.

**Deadline for Autumn Issue: 8/31/88.**

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

(continued from page 2)

## VI. KEEP YOUR ADDRESS CURRENT

To assist the Court and the parties in maintaining an accurate list of the members of the Class, please notify the Clerk of the Court of any change of address.

All Proofs of Claims, Exclusion Notices, notices of intention to appear, objections, and address corrections should be addressed to:

Clerk of the United States District Court
Eastern District of Michigan
Allnet Class Action
P. O. Box 277
Franklin, Michigan 48025

ENTERED BY ORDER OF:
Honorable Anna Diggs Taylor, Judge
United States District Court
Eastern District of Michigan
Detroit, Michigan

Clerk
United States District Court
Eastern District of Michigan
Detroit, Michigan

Dated: March 30, 1988

## PROOF OF CLAIM

To participate in the settlement, you must complete this Proof of Claim and mail it (along with the address label below) to the Clerk of the United States District Court, Eastern District of Michigan, Allnet Class Action, P. O. Box 277, Franklin, Michigan 48025. **This Proof of Claim must be postmarked on or before July 28, 1988.** Please print or type.

1. Name of claimant ______________________
   Address ______________________
   Telephone number where you can be reached during business hours ( ____ ) ______________
   Name and position of person completing this form if claimant is not an individual ______________
   Allnet account number ______________________
2. Check here if claimant is currently an Allnet subscriber. ______
3. Please choose one of the four options listed below. Please provide the information requested.

A. ____ **Standardized Credit** or B. ____ **Standardized Cash Refund**

Subject to the pro rata provisions set forth above in Section II of the Notice of Settlement, a Standardized Credit or Cash Refund equals 50 cents for each year you were a customer.

(i) Please circle each year or part of a year in which you were an Allnet customer.

1981 1983 1985
1982 1984

(ii) Total number of years circled ________

C. ____ **Itemized Credit** or D. ____ **Itemized Cash Refund**

Subject to the pro rata provisions set forth above in Section II of the Notice of Settlement, an Itemized Credit or Cash Refund equals 30 cents for each minute of unanswered calls for which you were charged.

(i) Provide the following information for each unanswered call for which you were charged and have not received a prior credit or refund. This information may be provided by attaching copies of your bills with the calls circled.

| Date of Call | Area Code And Number Called | Number of Minutes |
|---|---|---|

(ii) Total number of minutes listed ________

(iii) Please attach copies of the bills for each call listed. If you no longer have the bills, provide the Allnet access code to which the calls were billed, or if an access code was not used, the telephone number to which the calls were billed. ________________

4. If you chose the **standardized credit or itemized credit** options, and you are not currently an Allnet customer, you must complete the following authorization form:

I authorize Allnet to notify my local telephone company that I am choosing Allnet as my Primary Long Distance Carrier on the telephone number listed below. I understand that:

(i) If I incur a telephone company service charge in connection with the opening of my Allnet account, I will receive a credit to be applied to my Allnet account for the full amount of such service charge upon submission to Allnet, at the address to which this authorization form was sent, of a copy of the invoice for such charge.
(ii) While Allnet will be my Primary Long Distance Carrier, I will also be able to place calls with AT&T or any other carrier at any time I wish.
(iii) I may choose only one Primary Long Distance Carrier for the listed telephone number. If I choose another carrier later on, this selection will be invalidated.
(iv) I may change to another carrier at any time, and, if I do, my local telephone company may apply a service charge.
(v) I may designate only one telephone number. The telephone number listed below is the one for which I am making this designation.

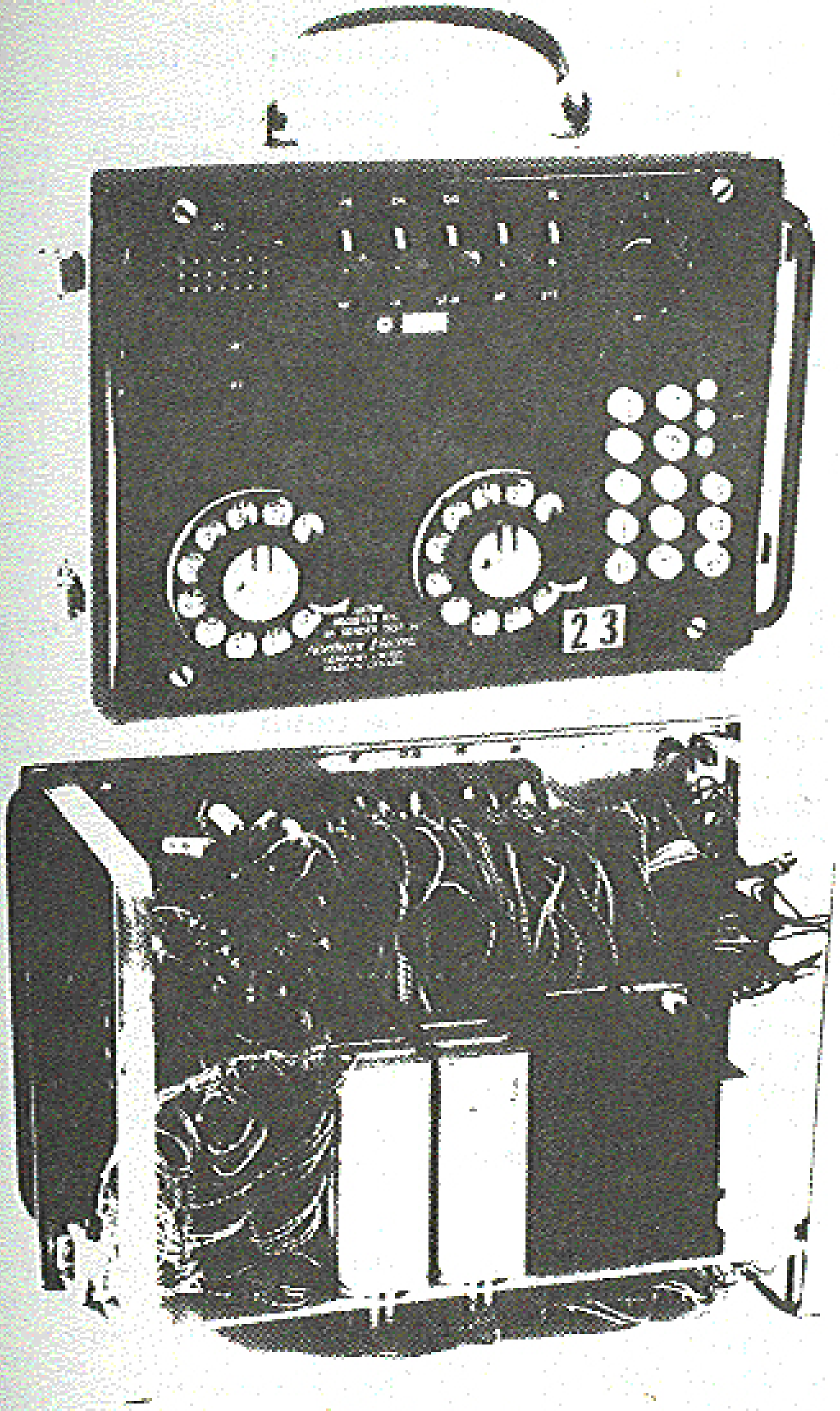
Customer name ______________________
Name of billing contact (if different) ______________________
Billing address ______________________
Suite or apartment no. ______________________
City ______________ State ______________ Zip ______________
Installation address (if different) ______________________
Telephone number to be converted ( ____ ) ______________
Date ______________ Signature ______________________

## CERTIFICATION AND RELEASE

I certify under penalty of perjury that I am authorized to make this claim, that the claimant was an Allnet customer at some time during the period March 2, 1981 through December 31, 1985, and that the claimant was charged for unanswered calls for which no credit or refund was previously received. I further certify that all information in this Proof of Claim is true and correct to the best of my knowledge, information and belief; that the claimant did not elect to be excluded from the Settlement Class; that the undersigned is the claimant or is authorized to execute and submit this Proof of Claim on claimant's behalf; and that this claim is the only claim being submitted in this settlement by or on behalf of the claimant.

In consideration of the right to receive benefits under the settlement, the claimant expressly covenants and agrees that he/she/it shall not now or hereafter institute, maintain or assert any claim relating to the billing of claimant for unanswered calls by Allnet during the period from March 2, 1981 through December 31, 1985. Claimant further releases all claims against Allnet, its predecessors, successors, affiliates, assigns and its officers, directors, agents and employees, past and present, that have been, might have been, are now or could be asserted in the lawsuits described in the Notice or that relate in any way to the matters alleged in the complaints in those lawsuits.

______________________
(Signature)



Photos by John Drake

```
#====================================#
#                                    #
#          THUNDER SEVEN'S           #
#                                    #
#          List Of Numbers           #
#             Rev. 1.0               #
#                                    #
#====================================#
```

Compiled as of 5/4/88

```
+-----------------+
: (800) COMPUTERS :
+-----------------+
```

| | |
|---|---|
| (800)222-0011 | ?? |
| (800)222-0555 | World Bank Mainframe |
| (800)223-3312 | CitiCorp |
| (800)227-0074 | RIS BBS |
| (800)227-3083 | IBM 3708 |
| (800)227-3404 | Bowman Network |
| (800)227-6544 | [Unix] |
| (800)228-0003 | ?? *300 baud only* |
| (800)228-0018 | ?? |
| (800)228-0329 | ?? |
| (800)228-0616 | Maryland C.C. |
| (800)228-0748 | ?? |
| (800)228-0993 | BCS |
| (800)228-0994 | BCS |
| (800)228-1111 | Visa (?) |
| (800)228-1170 | ?? |
| (800)228-1657 | PHILNET |
| (800)238-0631 | Telenet |
| (800)321-1646 | ?? *300 baud only* |
| (800)321-3910 | ?? |
| (800)325-4112 | Easylink |
| (800)327-9638 | Easynet |
| (800)328-0024 | ?? |
| (800)328-0137 | ?? |
| (800)328-0157 | ?? |
| (800)328-0187 | BWRR |
| (800)328-0198 | ?? |
| (800)328-4011 | ?? |
| (800)336-0149 | Tymnet |
| (800)345-3878 | Telex [1200] |
| (800)358-5860 | ?? |
| (800)368-3343 | The Source |
| (800)421-0082 | "please LOGIN" |
| (800)421-0092 | ?? |
| (800)424-9494 | Telenet |
| (800)426-2638 | Soft Search |
| (800)444-4472 | Novell |
| (800)521-2255 | Autonet |
| (800)526-3714 | RCA |
| (800)533-5294 | |
| (800)533-5295 | |
| (800)533-5296 | |
| (800)533-5297 | |
| (800)533-5298 | |
| (800)533-5299 | |
| (800)543-0010 | CINTI OH AD |
| (800)558-0001 | Agridata |
| (800)621-1411 | Freedom network *300 baud only* |
| (800)621-4243 | Pathology Clc. |
| (800)621-9080 | Datalynx |
| (800)624-5123 | AT&T Mail |
| (800)638-8369 | GEnie |
| (800)826-8855 | AM. Peoplelink |
| (800)828-6321 | XEROX |
| (800)847-0109 | ?? |
| (800)848-4480 | Compuserve |
| (800)852-0005 | [DIAL:] |

```
+-------------------------+
: VOICE MESSAGE SYSTEMS :
+-------------------------+
```

| | |
|---|---|
| (201)953-2222 | VMBS |
| (317)267-1901 | VMBS |
| (415)330-7831 | VMBS |
| (415)338-7000 | ASPEN |
| (415)463-6099 | VMBS |
| (415)882-7170 | VMBS |
| (703)934-3400 | VMBS |

800's are MUCH better...

| | |
|---|---|
| (800)222-0311 | ASPEN |
| (800)222-4653 | VMBS |
| (800)222-5273 | ASPEN |
| (800)222-9823 | VMBS |
| (800)228-0368 | Phone Mail System |
| (800)228-0464 | ESPN North America |
| (800)22-VOICE | Voicebank *another dialup for 88-VOICE* |
| (800)262-6477 | Unisys Answering Service |
| (800)284-MAIL | Meridian Mail |
| (800)323-3433 | VMBS |
| (800)323-3138 | VMBS |
| (800)323-4222 | VMBS |
| (800)323-4535 | Dexter Midland |
| (800)323-5840 | Safety Claims Corp. |
| (800)323-5917 | VMBS |
| (800)323-6274 | VMBS |
| (800)325-5534 | VMBS |
| (800)331-1763 | Innovative Software |
| (800)333-MAIL | Phone Mail System |
| (800)342-MAIL | Phone Mail System |
| (800)344-1884 | VMBS |
| (800)345-5104 | Security Link and Telelink |
| (800)423-7574 | VMBS |
| (800)424-3434 | VMBS |
| (800)424-6262 | ITT Voice Mail System |
| (800)437-6100 | Phone Mail System |
| (800)441-5612 | VMBS |
| (800)444-2003 | VMBS |
| (800)445-MAIL | Phone Mail System |
| (800)456-6899 | Olympic Transportation |
| (800)521-8477 | VMBS |
| (800)524-2133 | ASPEN |
| (800)541-0641 | VMBS |
| (800)543-MAIL | VMBS |
| (800)631-1146 | VMBS |
| (800)654-8692 | Security CN Life Insurance |
| (800)662-MAIL | Voice Message Exchange |
| (800)678-MAIL | VMBS |
| (800)733-1212 | The Message Center |
| (800)759-5000 | Ingram Switchboard |
| (800)777-MAIL | MCI Mail |
| (800)824-0010 | ?? |
| (800)847-6181 | Western Digital |
| (800)872-4634 | VMBS |
| (800)877-TALK | VMBS |
| (800)888-0030 | Receiver America |
| (800)888-1313 | VoiceLink |
| (800)888-MAIL | Phone Mail System |
| (800)88-VOICE | Voicebank *is the same as 22-VOICE* |
| (800)993-0025 | Access Service |
| (800)999-0080 | ASPEN |
| (800)999-TALK | ASPEN |

```
+---------------------+
: Other Phun Stuff :
+---------------------+
```

| | |
|---|---|
| (201)644-2330 | ("Enter first and last name...") |
| (201)644-2332 | ...Call this one collect!! |
| (201)644-2333 | News Service |
| (201)644-2336 | ("Enter first and last name...") |
| (201)644-2338 | Credit Transfer/ATM |
| (201)644-2339 | Automated Juror Select |
| (201)644-2340 | Credit Transfer/ATM |
| (201)644-5621 | Computerized Test |
| (201)644-5639 | " " |
| (201)840-5403 | Bridge |
| (202)456-1414 | The White House |
| (202)456-7639 | Executive Office of The President |
| (202)457-2980 | Bridge |
| (202)457-3200 | Bridge |
| (202)457-7970 | CBS News, Washington |

NOTES: * The (201)644-XXXX numbers are only Bell computerized test numbers and their functions are not actually put into effect (as far as I know).

* The status of bridges may change daily, so they may or may not be up at a given time. All the ones on here have worked recently.

* The XXXX in ringback numbers are the last 4 of your number, and you will probably have to pick up the phone and hang it up again before it rings.

* For a large list of other AT&T Newslines, see BIOC Agent 003's Basic TELECOM Part VI, many still work.

```
(212)976-4747,4848,7272,7979,8080,8686,8787,9090,9494,9898,9999  Sex Lines
(213)617-2287  976 Backdoor
(213)617-3284  976 Backdoor               (800)759-TALK  Skytalk
(213)935-1111  Sweep Tone Test            (800)777-MEET  Gay Conference Line (kill em!!) @
(214)357-8686  Sweep Tone Test            (800)826-6290  Automatic Disconnect Service
(215)340-0052  Packet Switch              (800)877-4700  Sprint Weather Line
(215)538-7032  Packet Switch              (801)782-9699  Sweep Tone Test
(215)610-X#XX  Ringback (215 N/A)         (818)761-1193  Bridge
(215)698-0049  Sweep Tone Test            (818)501-3400  Bridge
(215)867-1212  WIZO Weatherline           0-959-1230  Coin Test (works from some payphones)
(303)363-5929  Bridge                     0-700-456-100x  Alliance Teleconferencing
(312)592-6888  Bridge                     10041-1-700-777-7777  Allnet Conference
(313)424-0900  Mich. Bell Automated CN/A
(313)827-7151  Bridge
(412)633-3333  AT&T Newsline, PA          @ 2600 NOTE: WE THOROUGHLY DEPLORE IGNORANT
(415)284-1111  Sweep Tone Test              AND PREJUDICED STATEMENTS LIKE THIS ONE
(513)375-8500  Bridge                       AND HOPE MOST OF OUR READERS DO TOO. WE
(513)241-8580  Bridge                       DECIDED TO KEEP IT IN THIS LIST TO FACE
(603)226-3949  Bridge                       UP TO THE FACT THAT THE HACK/PHREAK
(617)494-9900  Sweep Tone Test              WORLD HAS ITS OWN REDNECK ELEMENT.
(619)375-1234  Time & Temperature
(717)255-5555  AT&T Newsline, PA
(718)528-9979  Sweep Tone Test
(800)222-TALK  Consolidated Connection Talking Yellow Pages
(800)223-3331  Bank-By-Phone
(800)225-0233  Conference Operator
(800)228-0014  CC Check (hit # after tone)
(800)228-0032  CC Check (hit #)
(800)228-9901  CC Check
(800)233-3996  Discover Check
(800)257-TALK  Money Talk
(800)325-5555  AT&T service report/check?
(800)327-1111  Visa/Mastercard Check
(800)433-4424  Discover Check             Originally uploaded to:
(800)424-5454  Fraud Hotline              ======================
(800)424-9090  White House Press Line     Atlantis
(800)445-3024  Sprint Operator            Digital Logic
(800)526-3366  Jam Demo Hotline           Demon Roach Underground
(800)527-6178  Midas Touch Credit Check   The Central Office
(800)528-2121  American Express Check
(800)554-2265  Visa Check
(800)692-8766  Watson Voice Message Demo
(800)732-2255  "High Seas" Operator
```

# NOTICE

Does your address label say "Time to Renew"? Don't miss an issue. Renew your subscription today and enjoy peace of mind. Simply indicate the amount enclosed and which, if any, back issues you want. Your address label should be on the back of this form.

| | |
|---|---|
| $15 | 1 year of 2600 |
| $28 | 2 years of 2600 |
| $41 | 3 years of 2600 |
| $40 | 1 year corporate subscription |
| $75 | 2 year corporate subscription |
| $110 | 3 year corporate subscription |
| $25 | overseas subscription (1 year only) |
| $55 | overseas corporate subscription (1 year only) |
| $260 | lifetime subscription (never again will we bother you) |

Back issues are available. Prices are:

| | |
|---|---|
| $25 | 1984, 1985, or 1986 issues (12 per year) |
| $50 | Any two years |
| $75 | All three years (36 issues) |

(Overseas orders add $5 for each year ordered)
Allow 4 to 6 weeks for delivery.

Send all orders to:
2600
PO Box 752
Middle Island, NY 11953 U.S.A.
(516) 751-2600

**1987 ISSUES ALSO AVAILABLE!**

**AMOUNT ENCLOSED FOR SUBSCRIPTION: ______**

**AMOUNT ENCLOSED FOR BACK ISSUES: ______**

**1984 1985 1986 (circle years ordered)**

**TOTAL AMOUNT ENCLOSED: ______**

*(clip and send to us—your address is on the back)*