A SOFTWARE BESTIARY

Computer Parasites & Remedies

A Catalogue of First Sightings of Real & Imaginary Beings ~

by

Corinne Cullen Hawkins
illustrated by H.S. Robins

VIRUSES

Viruses, in their simplest form, just replicate themselves. A slightly more advanced virus not only duplicates a program but renames each one slightly differently. More sophisticated viruses erase files, scramble memory, turn off the power, or do any/all of these things with a time delay, called a time bomb. Some viruses "burn a hole" somewhere so that a certain command will do something else, i.e., given an addition command the program subtracts instead.

Creeper — Possibly the first known virus, first sighted in 1970. Built by Bob Thomas of BBN, it was a demonstration program that crawled through ARPAnet, a nationwide Pentagon-funded network linking university, military and corporate computers, springing up on computer terminals with the message, "I'm the creeper, catch me if you can!"

A version of Creeper done by Ray Tomlinson not only moved through the net, but also replicated itself at times.

Reaper — In response to Creeper, this virus also jumped through the network, but it proceeded to detect and "kill" creepers. (*The Cincinnati Post*, Feb. 1, 1988)

Rabbit — One of the first known viruses, first sighted in 1974 by Bill Kennedy. When Rabbit was introduced into a system, it copied itself and continued to toss the copies back into the input jobstream (the place where programs start). This slowed the communication between the input jobstream and its console (teletype where system operator sees what's going on), which made Rabbit harder to kill the longer it ran. (comp.risks *[an electronic journal on the Usenet network]*, Mar. 29, 1988).

Pervading Animal — An early proto-virus attached to a Univac 1108 game program called Animal. While the user was playing the game, Pervading Animal copied itself into every write-enabled program file available. (Mike Van Pelt, comp.risks Mar. 29, 1988.)

Smart Virus — In the book *The Adolescence of P-1* (Thomas J. Ryan, Collier Books, 1977), there is an example of an intelligent, information-hunting virus.

ARPAnet Data Virus — On October 27, 1980, multiple "status" messages began appearing on the ARPAnet. Status messages are normally broadcast from each node of the network to relay their readiness to handle new data. Each node then propagates copies of incoming status messages to other nodes in an ongoing determination of the optimal path for the electronic traffic. Status messages are supposed to be trashed immediately afterward, but in this case the message from a particular node somewhere near Los Angeles became mutated. Its contaminated form caused a "garbage collector" malfunction in the receiving nodes. No messages could be thrown out, thus saturating the nodes. Yet the nodes continued to propagate waves of this debilitating message, infecting others which couldn't dump the infected message, until it spread throughout the whole network like cancer and ground it to a halt. It was 72 hours before technicians could revive it. (*Software Engineering Notes*, Jan. 1981.)

2600 VAX Virus — This one replicates itself, sends jobs continuously to the batch queue (where programs line up, waiting to be run). All that happens is the

Queue might overflow. (*2600*, Aug. 1986, vol. 3, no. 8.)

Elk Cloner Virus — First sighted in 1981 or 1982, this one runs on the Apple II family. It inserts itself into the DOS operating system. Elk Cloner hooks into the RUN, LOAD, BLOAD, and CATALOG commands to make them check the accessed program disk and infect it. It prints a poem:

The Program with a personality
It will get on all your disks
It will infiltrate your chips
Yes, it's cloner!
It will stick to you like glue
It will modify Ram too
Send in the cloner!

(comp.risks, Apr. 26, 1988 by Phil Goetz)

Finger Virus — A speculative virus that would go out replicating until it found a specific person. Then it would send that person's e-mail address back to its creator. (Fred Hapgood, First Artificial Life Conference, Sept. 1987).

Lehigh Virus — First sighted Nov. 25, 1987 by Jeffrey Carpenter, posted on Usenet. It attached itself to a few lines of the operating system used on the IBM PCs that Lehigh University provides for student use. It is a corruption of a legitimate program, Command.Com, the basic boot-up file of MS-DOS and PC-DOS. The virus destroys data on floppies and hard disks by writing zeros to the first thirty-two sectors of a disk (which erases the directory kept in the first couple of tracks), making the data unrecoverable.

It spreads when a clean PC is booted from an infected disk and the user accesses a second, uninfected program disk with the resident commands: TYPE, COPY, DIR, CHDIR, ERASE, MKDIR, RMDIR, VERIFY. The virus waits until it has been copied four times before it wipes out the data on the disk on which it resides.

© Brain Virus — First sighted Fall, 1987 at the University of Delaware. It changes the volume label (the given name) of a floppy or hard disk to © Brain. The boot record contains a message: "Welcome to the dungeon . . . Beware of this VIRUS. Contact us for vaccination." The message includes the address and phone number of Brain Computer Services, a computer company in Lahore, Pakistan, and the names of two brothers, Basit and Amjad.

The virus marks some disk sectors as bad. It modifies several command files, maybe all of them eventually, without changing file sizes or dates. Even if the boot sector is rewritten, the virus remains active through the command files it modified. No known cure. (comp.risks, Apr. 5, 1988.)

This is the first virus to infect an American newspaper's computer system (*The Providence Journal-Bulletin*). When the phone number in Pakistan was called, the person who answered expressed surprise that the virus had travelled so far — and refused to give his last name. (*New York Times*, May 25, 1988.)

Amiga Virus — This one is a simple modification of the Amiga boot block. On an Amiga floppy the boot block consists of the first two sectors on the disk. Normally it contains a small bit of code that loads and initializes the DOS when it is "booted" or turned on. Some commercial software packages and games store special information in the boot block. Since the virus overwrites this, the information is lost forever. After a certain number of disks have been infected the virus will print a message:

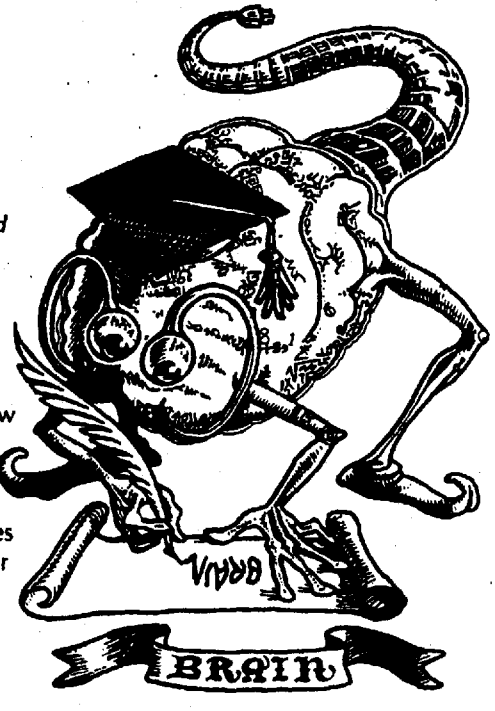
"Something wonderful
has happened.
Your Amiga is alive!!!
and even better
Some of your disks are infected
by a VIRUS
Another masterpiece of the
Mega-Mighty SCA"

(comp.risks, Dec. 7, 1987.)

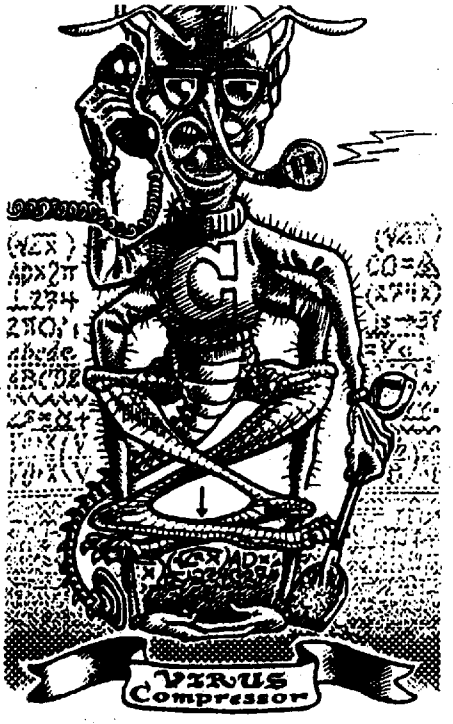
Israeli Virus — First sighted by Yuval Rakavy, a student at Hebrew University; first mentioned publically in *Maariv*, one of Israel's daily newspapers, Jan. 8, 1988. Designed to begin destroying files on May 13, and to slow computer response on the 13th of any month, it would also put garbage on the screen from time to time. What called attention to the virus was an error in the virus code itself, which caused it to mistake previously infected programs as uninfected. In error, it would add another copy of itself to the program. Some programs were infected as many as 400 times and the growth in size of the program was noticeable. This one was discovered before D-day, but it had infected home, university, and military computers before it was detected.

MacInVirus — First known encounter by David Spector. This virus was written by a West German and posted to CompuServe in a HyperCard stack. The virus is disguised as a resource that inserts itself in a system trap handler (the place where the computer catches errors so they won't cause system crashes). The virus destroys hard disks and the applications that run on them. (comp.risks, Jan. 10, 1988.)

"Good" Virus — Written by a West German programmer, this virus won't let "unknown" programs run on one's machine. If the programs to be run aren't already infected with THIS virus, they won't be allowed to run at all. (comp.risks, Jan. 10, 1988.)



244



Virus Compressor — First imagined by Fred Cohen, this virus would compress the coding of data, permitting it to be stored in a smaller space. It would ask permission of the user each time it acted. (*New York Times,* Jan. 31, 1988.)

Target Virus — This one would target a specific program or individual, for example, by systematically altering spreadsheet data or performing other subtle changes. (*The Cincinnati Post,* Feb. 1, 1988.)

The Anti-Virus Software Virus — First imagined by Chuck Weinstock, posted to Usenet Feb. 9, 1988. The virus is, of course, imbedded in the software you use to detect viruses, and therefore goes undetected.

Meta-Virus — First imagined by Jeffrey Mogul, Feb. 9, 1988 on Usenet. This is a paranoia virus, created only with words:

WARNING! A serious virus is on the loose. It was hidden in the program called 1987 TAXFORM that was on this bulletin board last year. . . . By now, it is possible that your system is infected even if you didn't download this program, since you could easily have been infected indirectly. The only safe way to protect yourself against this virus is to print all your files onto paper, erase all the disks on your system, buy fresh software disks from the manufacturer, and type in all your data again. But FIRST! send this message to everyone you know, so that they will also protect themselves.

This virus took Jeff Mogul two minutes to produce and he didn't even have to write any code.

Scores Virus — First sighting mentioned in *MacWeek,* Apr. 12, 1988. In existence since at least February, and possibly since as early as September 1987. It infiltrated several government agencies, Apple sales offices, and the Mac of an unidentified senator, as well as *MacWorld* and *Macintosh Today.*

First dissected by John Norstad and Bob Hablutzel, this virus has several time-delay features. It's designed to attack two custom applications called ERIC and VULT, but it will infect anything. Several days after infecting a Mac system, the virus attempts to locate and modify any files with the creator code of ERIC or VULT. The code of the virus is written to make the targeted program dysfunctional. The virus lies dormant for two days after infection. After two, four, and seven days various parts wake up and begin their mischief. Two days after the initial infection the virus begins to spread to other applications. After four days the second part of the virus wakes up. It begins to watch for the VULT and ERIC applications. Whenever VULT or ERIC is run, the system bombs after twenty-five minutes' use. After seven days the third part of the virus kicks in. Whenever VULT is run the virus waits fifteen minutes, then causes any attempt to write a disk file to bomb. If you don't do any writes for another ten minutes the application will bomb anyway.

Deleting the infected resources isn't enough to remove the virus since the virus recognizes the attempt and modifies its resource identification and memory location when probed by resource utilities. ResEdit "thinks" that the virus resources have been deleted, but they have been renamed and will return when the Mac is restarted.

Apparently, the virus doesn't attempt to spread itself over networks.

The Scores virus causes printing problems, system crashes, application crashes on launch, and damaged Excel files.

MacMag Virus — First sighted by Chris Borton Mar. 8, 1988 and posted to comp.risks on Usenet. First mentioned in print in the *Toronto Star* March 16, 1988. The virus was launched in December 1987 by Richard Brandow, publisher of *MacMag* magazine in Montreal, Canada. It was supposed to be a simple message of peace, designed to pop up on Macintosh screens on March 2, the anniversary of the introduction of the Apple Macintosh SE and Macintosh II. The virus infects the System file, but doesn't directly affect applications. After March 2 the virus erased itself. Although this virus was designed to be benign, it had some nasty side effects: it played havoc with users' System folders, resulting in thousands of hours of lost work. ►

The virus spread to Europe and the West Coast, and it is the first virus to infect a commercially available personal computer product. It was inadvertently passed to Aldus by Marc Canter, president of MacroMind Inc. of Chicago, which makes training disks for Aldus. Mr. Canter's personal machine caught the virus from an infected copy of Mr. Potato Head, a computer game. Mr. Canter ran the program only once; it was enough to infect his computer, which was later used to work on a training software disk for Aldus. Aldus admits that a disk-duplicating machine copied the infected disk for three days. Half of the infected disks were distributed to retailers; the other half were warehoused.

Immortal Virus — First imagined by Paul Hoffman, Mar. 13, 1988 in the Macintosh Conference on The WELL. This virus would live in some cache-like memory on a serial port or parallel port (what connects a printer to a computer) so it would survive a warm boot, even after a devirusing.

King Virus — A virus that kills other viruses and replaces them with itself. First imagined by Andrew Beals, Mar. 16, 1988 on The Well. No known sightings.

King II Virus — A virus that not only kills other viruses, but feeds on them, getting stronger each time. Imagined by Michael Zentner, Mar. 16, 1988, Macintosh Conference on The Well.

Bell Labs Virus — A compiler program (which translates a human programmer's instructions into a set of 1s and 0s that a computer can read) had been altered so that it secretly embedded a hidden "trapdoor" each time it created a new version of the operating system. The secret trapdoor altered the system so that, in addition to normal users' passwords, it would recognize a magic password known only to one person. The instructions never showed up in the program listing — it was undetectable through normal means. The virus never escaped Bell Labs.

Atari ST Virus — First dissected Mar. 22, 1988, posted on Usenet Mar. 26, 1988 by Martin Minow. Once installed, this virus will copy itself onto every non-write-protected disk used. It tests an uninfected disk to see if it contains the virus, replicates, then it keeps count of how many times the disk is used after that. When a certain limit is reached, the virus writes random data across the root (central) directory and file allocation tables (the computer's index of where data are stored) for the disk, making it unusable. The virus then removes itself from the damaged disk. The current virus doesn't affect hard disks. This virus may survive a reset (a warm boot — resetting the machine without turning it off).

No-Name Virus — First rumored to exist Mar. 26, 1988 on Usenet, posted by Martin Minow. This virus is almost impossible to detect because for each disk, it scans for any program file and appends itself to the text segment in some way. This makes it very difficult to tell whether or not the virus is actually on the disk.

TROJAN HORSES

These parasites are bits of code slipped into an otherwise innocent program. Viruses replicate; Trojan Horses do not. Some are written from scratch, some are adulterated copies of legitimate programs. Some Trojans erase or scramble data, some just scramble or erase the file allocation table. Some begin destruction within minutes of infection, others perform as legitimate software for weeks or months, then touch off a time bomb. Some Trojans put up a screen message such as: "I'm deleting all your files," then proceed to do so. Some put up a similar screen message, but don't follow through. The more sophisticated Trojan Horses delete themselves with their last line of programming. In other cases the Trojan isn't actually inserted directly into the program. Only a pointer is placed in the program, telling the system which program to run, and the horse is hidden elsewhere.

Notroj — This Trojan Horse pretends to be a program that guards against Trojans. It's actually a time bomb that wipes out the hard disk after it's more than 70 percent full. (*New York Times*, May 19, 1987.)

XmasCard Trojan — First known sighting Dec. 9, 1987. It was written as a prank by a West German student. This Trojan began in a European academic computer network (Bitnet) and jumped through electronic gateways to five continents and to the internal e-mail system of IBM. In the IBM internal e-mail system, a holiday message promised to draw a Christmas tree on the screen if someone would type the word "Christmas" on the computer. When they did, it drew a tree but it also sent a copy of itself to all of the other network mail addresses kept in each user's electronic rolodex. Along with a very primitive tree (made of capital "Xs"), a message was displayed: "A very happy Christmas and my best wishes for the next year. Let this run and enjoy yourself. Browsing this file is no fun at all. Just type 'Christmas.'"

Once opened, the program rarely accepted commands to stop. Operators who turned off their

246

XMAS CARD TROJAN HORSE

terminals to try to stop the Christmas message lost electronic mail or unfinished reports not saved in the computer. The Trojan infected so many machines that it brought IBM's global electronic mail network to a halt, disrupting the system for 72 hours. Plant officials were forced to turn off internal links between computer terminals and mainframe systems to purge the message.

A virus was written to follow and destroy the Christmas Card Trojan and then self-destruct in mid-January. The Trojan was generally stamped out by December 14, 1987. The culprit was tracked down and barred from access to his system.

Turkey Trojan — A program being passed around via ARPAnet and some other computer networks, called "Turkey." It's supposed to draw a picture of a turkey but it doesn't. Instead it erases all of the unprotected files in the directory. (comp.risks May 12, 1988.)

Run.me — This is a graphics program which plays the Star-Spangled Banner and displays the American flag while it worms its way into the hard disk and erases the data on it. (*New York Times*, May 19, 1987.)

WORMS

Essentially, worms are simple creatures: memory crunchers which rewrite themselves successively through the computer's memory. The programs on individual computers are the segments, which remain in communication with each other. Almost any program can be modified to incorporate the worm mechanism.

Xerox PARC Worm — In 1980 John Shoch at the Xerox Palo Alto Research Center devised a worm which wriggled through large computer systems looking for machines that were not being used and harnessing them to help solve a large problem. The worm could take over an entire system. (John F. Shoch and Jon A. Hupp, Sept. 1980, Xerox Palo Alto Research Center.)

Existential Worm — A worm whose sole purpose is to stay alive. It runs no substantive application program. The Cookie Monster Worm at MIT was one such. It might display a screen message such as: "I'm a worm, kill me if you can!" (John Shoch, 1980.)

Billboard Worm — A worm used to distribute a full-size graphic image to many different machines. Some have graphics of the worm nibbling up the screen and heading off into memory. (John Shoch, 1980.)

Alarm Clock Worm — A worm that reaches out through the network to an outgoing terminal (one equipped with a modem), and places wake-up calls to a list of users. (John Shoch, 1980.)

Gladiator Worms — Bill Buckley and James Hauser developed Core Wars, where the object is to write a worm program that can replicate itself faster than another worm program can eat it. The one alive at the end wins. Some of the winning programs have a chromosome consisting of only four lines of code. Longer genes can't execute as fast as short ones, so they tend to get weeded out. (*WER* #58.)

Shockwave Rider Worm — Still the most sophisticated worm is the fictional one created by writer John Brunner in his novel *The Shockwave Rider*. Brunner's tapeworm ran loose through a computer network, gobbling up computer memory in order to duplicate itself — there was no stopping it. The worms were used by rebels to undermine a dictatorial government wielding power through a computer network.

> "And — no, it can't be killed. It's definitely self-perpetuating so long as the net exists. Even if one segment of it is inactivated, a counterpart of the missing portion will remain in store at some other station and the worm will automatically subdivide and send a duplicate head to collect the spare groups and restore them to their place."

(John Brunner, *The Shockwave Rider*, Ballantine, 1975.)

Worm Watcher — A special program which automatically takes steps to limit the size of a worm, or shut it down if it grows beyond a certain limit. The worm watcher also maintains a running log recording changes in the state of individual segments. This information can be used to analyze what might have gone wrong with a worm. (John Shoch, 1980.) ►

WORMS

VIRUS REMEDIES

As viruses have proliferated, so have vaccines and other remedies.

Viralarm System (Lasertrieve Inc., of Metuchen, N.J., 201/906-1901) — Consists of a special program to protect another program, creating a software barrier. The protection is available for individual personal computers and works for most operating systems now available.

Protec ($195 from Sophco. Inc., P. O. Box 7430, Boulder, CO 80306-7430; 800/922-3001) — A system of programs that includes Vaccinate — a virus itself, which infects the host via the Syringe program. It warns the end user (the person using the program as opposed to the one who wrote it) if a virus infection has occurred. It also includes Canary, a quarantine program. When new files are imported from an unknown source, a user places the Canary program on a diskette with the suspect files. If the Canary dies, a virus program is present. Protec works on the IBM-PC family of computers.

Checksum — Commonly attached to the end of a program. Although not designed as a virus catcher, it can be used to see if the size of the program changes.

Ferret — Created by Larry Nedry and Scott Winders. Notifies an infected user of the date that the Scores virus installed itself. It's helpful in determining where/how the virus was picked up. Ferret is available on electronic bulletin boards such as CompuServe and MacNET. (*MacWeek*, April 26, 1988.)

KillScores — Unlocks locked files, disinfects, and leaves files unlocked. (comp.risks May 11, 1988.)

Vaccine — By Don Brown at CE Software, Inc., Mar. 19, 1988. It enables your computer's operating system to detect alterations to the code of your system files and applications. It requires your permission for any such alterations. If your system is already infected when you install Vaccine, there will be no warning from Vaccine that the virus exists. If Vaccine is installed on a sterile system and the Scores virus is introduced later, Vaccine will only warn of the virus attack; it will not prevent infection. Vaccine is available free on electronic bulletin boards such as CompuServe and Genie.

Interferon — Written by Robert Woodhead. A shareware program that detects and claims to recognize "signals" that viruses give off when they are present, Interferon was intended to complement the Vaccine program from CE Software of Des Moines, Iowa. Interferon is available on electronic bulletin boards.

Softlog (Asky Inc., Milpitas, CA. Licensed to corporations in lots of 100 units for $2,400.) — Matches the current size of computer files against their previous size, and thus detects any unauthorized additional material, such as a parasite.

Truss — For UNIX systems, it allows the system administrator to examine any process and observe the activities of any user logging in from a remote site. Truss attaches to a login shell (the part of the computer that handles the commands a user needs to login to the bulletin board). Truss can also freeze a process and allow a debugger more detailed information about the errant process.

Data Physician ($199 from Digital Dispatch, 1580 Rice Creek Road, Minneapolis, MN 55432; 612/571-7400) — The granddaddy of virus remedies, it detects and in some cases eliminates viruses. Makes careful measurements of a computer's programs and data files to detect any alien computer codes. It includes:

Data MD — One portion of Data Physician, which creates a list of computer data files to be protected and watches them while the computer is in operation.

Antigen — Attaches itself to an individual computer program and checks it for viruses each time it's used. To remove a virus, Antigen erases the bytes of computer data that weren't in the program earlier.

Padlock — Prevents anything from being written on a storage disk unless the computer operator pushes a button to give permission.

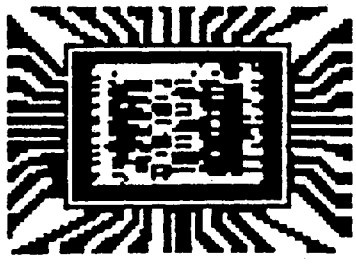
Data Physician works on IBM PC and UNIX systems.

Disk Defender ($199, Elek-tek, 6557 N. Lincoln Ave., Chicago, IL 60645; 800/621-1269) — Director Technologies, Inc. developed this product, which write-protects in hardware all or part of a personal computer hard disk. This protects the operating system and commonly used programs from viruses.

Virus RX — Developed by Apple (but sold through local dealers), this is a detection tool to determine whether a system has been infected by the Scores virus, and if so, which applications have been affected. It lists damaged applications, invisible files, altered system files, and altered applications. Virus Rx reports different levels of concern from simple comments to "dangerous" to "fatal." It first lists damaged applications — those that have not been infected by the virus, but will not work and should probably be removed. This program is available through Apple dealers, AppleLink, and through some users'-group bulletin boards.

Forgery Detector — Designers are now working on software that analyzes a program's style, in a similar fashion to handwriting analysis. It can then detect when "foreign" code is added to a particular program. It may also be able to determine the author of a virus. (*The Cincinnati Post*, Feb. 1, 1988.)

Pirate Detector Virus — This one keeps track of software duplication. It tells you how many copies of a program have been made, and alerts you to illegal or viral program duplication. (*New York Times*, Jan. 31, 1988.) ■



SPECIAL INAUGURAL REPRINT ISSUE: INFORMATION ENVIRONMENT TOOLS AND IDEAS Whole Earth Review Dedicated to the Incoming Administration 20 January 1996 - Link Page

Previous	A Village Called The WELL (Fall 1988)
Next	Getting Over the Information Economy (interview by James Walsh) (Summer 1988)

Return to Electronic Index Page