Article #1

IS YOUR COMPUTER

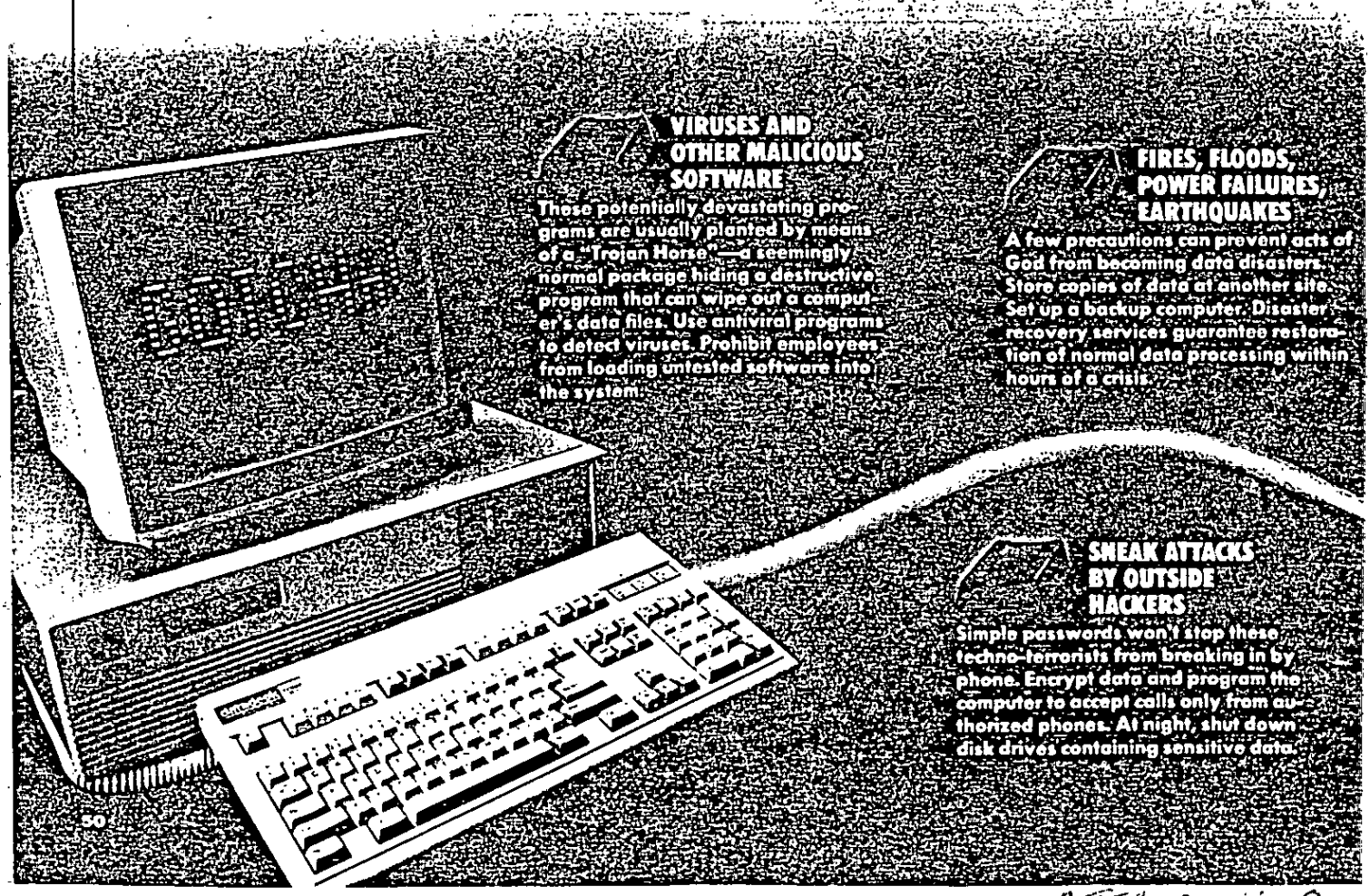
HACKERS, HIGH-TECH BANDITS, AND DISASTERS COST BUSINESS BILLIONS—AND AS

Donald Gene Burleson resented authority. He denounced federal income taxes as unconstitutional and boasted that he hadn't paid any since 1970. The pudgy, 40-year-old programmer also complained that his salary at USPA & IRA Co., a Fort Worth securities trading firm, was too low. He often had heated arguments with superiors. "He was so fanatical about everything," says former co-worker Patricia Hayden. But she adds: "He could do anything with a computer."

Evidently he could. Two days after USPA fired him in 1985, the company alleges, Burleson entered its headquarters and planted a program that once each month would wipe out all records of sales commissions. USPA discovered the break-in two days later. But it lost 168,000 records before disabling the program. Burleson is now awaiting trial on charges of "harmful access to a computer," a felony in Texas. If convicted, he faces up to 10 years in jail.

VIOLENT SHUTDOWN. The Burleson caper is just one in a string of recent events that point to the alarming vulnerability of computer systems—and the businesses and government agencies that rely on them. Hackers have invaded sophisticated data networks—even those at the Pentagon. Accidents, such as the May 8 fire at an Illinois Bell switching station outside Chicago, have disrupted communications in entire towns for weeks at a time. But experts agree that the No. 1 threat, which accounts for at least 80% of security breaches, is internal: "The real problem is errors, omissions, or well-thought-out acts by individuals who have authorized access to data," says Lawrence L. Wills, who's in charge of selling data security software for IBM.

Whether the fault lies with a disgruntled employee, a hacker, simple human ineptitude, or a natural disaster, disabling a vital computer and communications system can be as easy as cutting a critical power line or typing a few commands on a keyboard. The threat is eloquently simple: Computer networks and the information they handle are assets a company can't do without. But often they aren't adequately protected, and the consequences of that exposure can be disastrous. Without computers, "we cannot run our plants, we cannot schedule, we cannot bill or collect money for our product, we can't design our product," says G. N. Simonds, executive director of management information systems at Chrysler Corp. "In essence, we



SECURE?

PCs PROLIFERATE, THE PROBLEM CAN ONLY GROW WORSE

very quickly shut the company down."

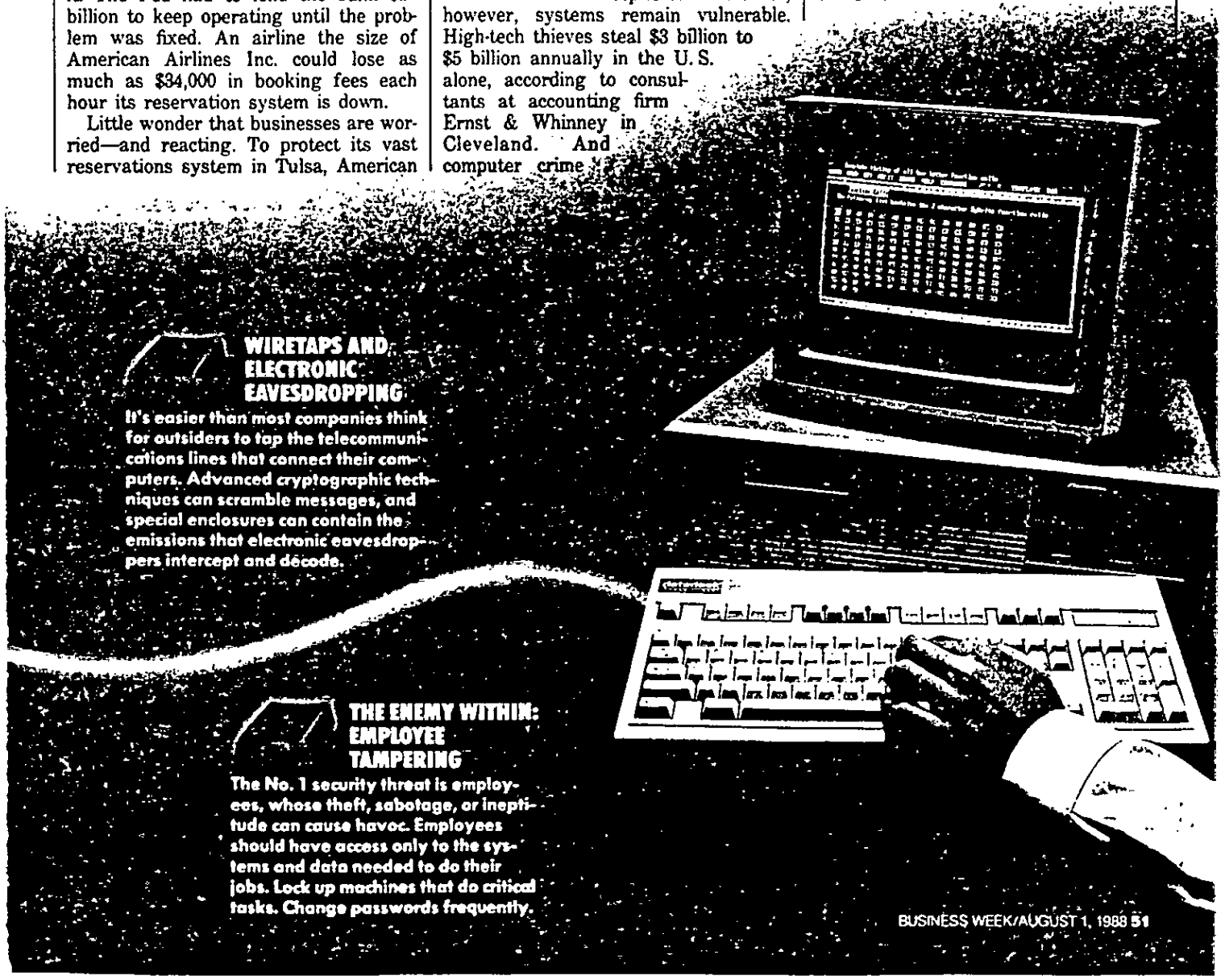
The potential for trouble is even greater in the service industries that now dominate the economy. Every workday, U.S. computer networks transmit close to $1 trillion among financial institutions, an amount equal to 25% of the gross national product. When a software problem fouled up record-keeping in Bank of New York's government securities trading operations in 1985, other banks temporarily stopped trading with it. The Fed had to lend the bank $24 billion to keep operating until the problem was fixed. An airline the size of American Airlines Inc. could lose as much as $34,000 in booking fees each hour its reservation system is down.

Little wonder that businesses are worried—and reacting. To protect its vast reservations system in Tulsa, American built a $34 million underground facility with foot-thick concrete walls and a 42-inch-thick ceiling. Anyone who scales the barbed wire faces a security system that includes a retina scanner, a James Bondian device that detects unauthorized personnel by the unfamiliar pattern of blood vessels in their eyeballs. Indeed, a booming industry has developed to help protect computers, ranging from scores of consultants to sellers of hardware and software impediments to intruders.

'HELL OF A MESS.' Despite such defenses, however, systems remain vulnerable. High-tech thieves steal $3 billion to $5 billion annually in the U.S. alone, according to consultants at accounting firm Ernst & Whinney in Cleveland. And computer crime pays well: In an average stickup, security experts say, a bank robber grabs $5,000. By contrast, the average electronic heist nets $500,000. In electronic funds networks, "you have $15,000-a-year clerks transferring $25 million a day," says Ronald Hale, research manager at the Bank Administration Institute in Chicago. For some, the temptation is too great.

In early July, a group of insiders wired $54 million from the London office of Union Bank of

PHOTOGRAPHS BY TED MORRISON, ILLUSTRATION BY RALPH WERNI



WIRETAPS AND ELECTRONIC EAVESDROPPING

It's easier than most companies think for outsiders to tap the telecommunications lines that connect their computers. Advanced cryptographic techniques can scramble messages, and special enclosures can contain the emissions that electronic eavesdroppers intercept and decode.

THE ENEMY WITHIN: EMPLOYEE TAMPERING

The No. 1 security threat is employees, whose theft, sabotage, or ineptitude can cause havoc. Employees should have access only to the systems and data needed to do their jobs. Lock up machines that do critical tasks. Change passwords frequently.

Switzerland to another Swiss bank, complete with the correct authorization codes. A malfunction in the second bank's computer delayed the transaction, and auditors discovered it and froze the funds before they could be collected. First National Bank of Chicago foiled a $70 million embezzlement scheme last May only because the two employees who masterminded it made a dumb mistake: They tried to overdraw on the accounts they were stealing from.

Often, even hackers depend on inside help. A band of teenage programmers, calling themselves "phrackers," has been giving fits to Pacific Bell and other phone companies with a simple con game. Posing as fellow employees, they call phone company representatives and cajole them into releasing computer passwords. Says one 17-year-old phracker: "It works surprisingly well." Inside the phone company computer, phrackers cause mayhem by disconnecting service to customers or changing work orders.

Now changes in computer technology are making mischief easier. Increasingly, minicomputers and personal computers are being spread through offices and networked together. Such "distributed processing" multiplies the potential points of access. "When computerization was centralized, the computers were in one room behind locked doors," says Edwin B. Heinlein, a computer security consultant in San Rafael, Calif. "Now it's a hell of a mess." With 33 million desktop machines in use, hundreds of thousands of individuals have acquired the technical skill to "penetrate most systems," says Gerald E. Mitchell, director of data security at IDS Financial Services Inc. in Minneapolis.

Using international phone links, a group of West German hackers took repeated strolls through NASA computers last summer, as well as through several U. S. military networks. NASA spent three months changing passwords and clearing out "trap door" programs that the intruders had planted to give them access. Another German hacker spent nearly two years cruising through unclassified data in U. S. Defense Dept. and other research computers around the world until he was stopped last year. And last May, NASA's Jet Propulsion Laboratory in Pasadena, Calif., was invaded by hackers yet to be identified.

Even companies with good security have run into a new and insidious problem: the computer virus. Like microorganisms, these replicate and spread. They're tiny bits of software, often quickly written, that hide in larger programs and then pounce unpredictably. Some simply deliver a surprise message on the screen. Others can wipe out every shred of information in a computer.

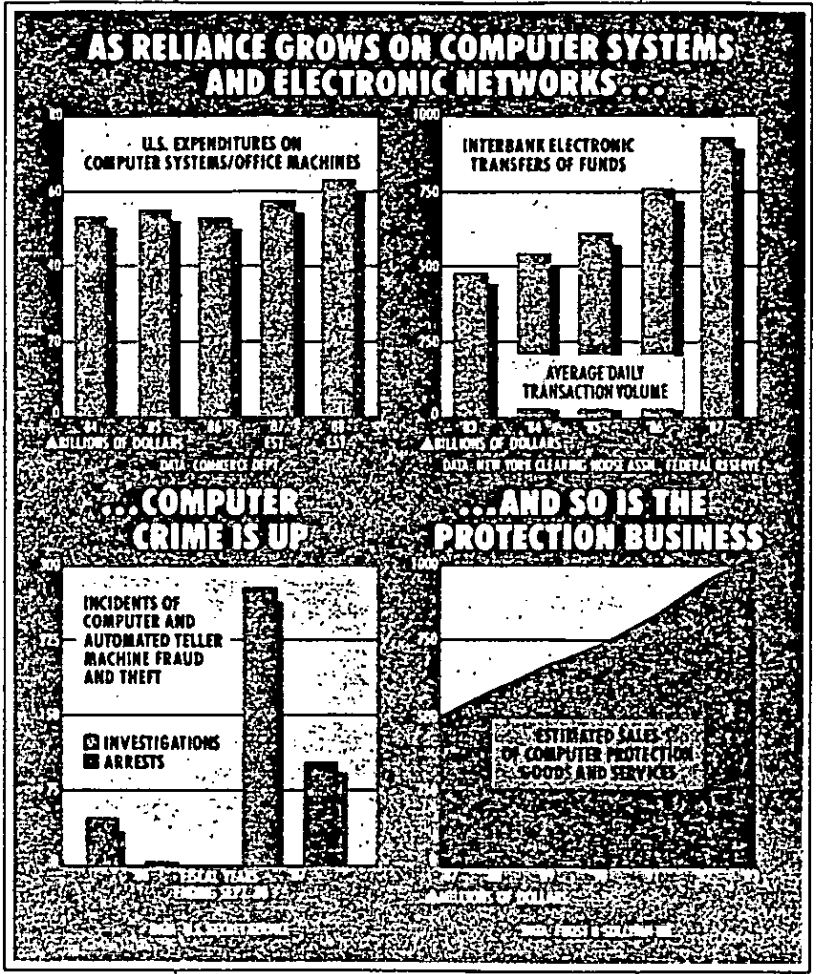
What especially worries corporate computer managers is that somehow these destructive programs could migrate to mainframe computers and do serious damage to the most sensitive corporate data. Says Jeffrey M. Hoffman, a computer specialist at Atlantic Richfield Co.: "The PC world is the lightly protected gateway to the host computer world." Although most large computer systems employ mechanisms that isolate computer code, reducing the opportunity for a virus to spread, the threat exists—even for Big Blue. Although the company plays down the incident, last December a virus-like program infiltrated IBM's 145-country electronic mail network, forcing the entire system to be shut down.

When such incidents occur, the victim company often has failed to employ some surprisingly simple measures. Experts say, for instance, that companies should outlaw such mundane passwords as a birthday or a spouse's name. NASA concedes that it was using "inappropriate" passwords that were easy to guess. IBM's Wills urges companies to remind workers not to log on to a computer and then leave it unattended, nor share passwords with co-workers. He is also a proponent of written computer security policies, complete with security clearances.

NEED TO KNOW. IBM has five classes of data, from unclassified, with no restrictions, to "registered IBM confidential," available only to employees with a predetermined need to know. After last year's incident, which began when a West German law student sent a self-replicating Christmas greeting into a European academic research network, IBM tightened controls over its electronic networks.

It's crucial, say experts, to treat computer security as a management, not a technology, problem. For example, programs running on Marine Midland Bank's central computer are "encapsulated" so that employees can use only what's needed to perform their jobs—and can't browse through the system.

Physical barriers are important, too, and there are lots of new ones. Electronic card keys, or "smart cards," with embedded microchip memories and processors, are starting to be used as I. D. cards for workers. They can be programmed with volumes of personal data and authorization codes that are hard to fake. Some smart cards change passwords every 60 seconds. But even such cards have a flaw: They can be stolen. More secure, some experts think, are biometric devices, which identify people according to physical quirks. Machines'



ERIC HOFFMAN

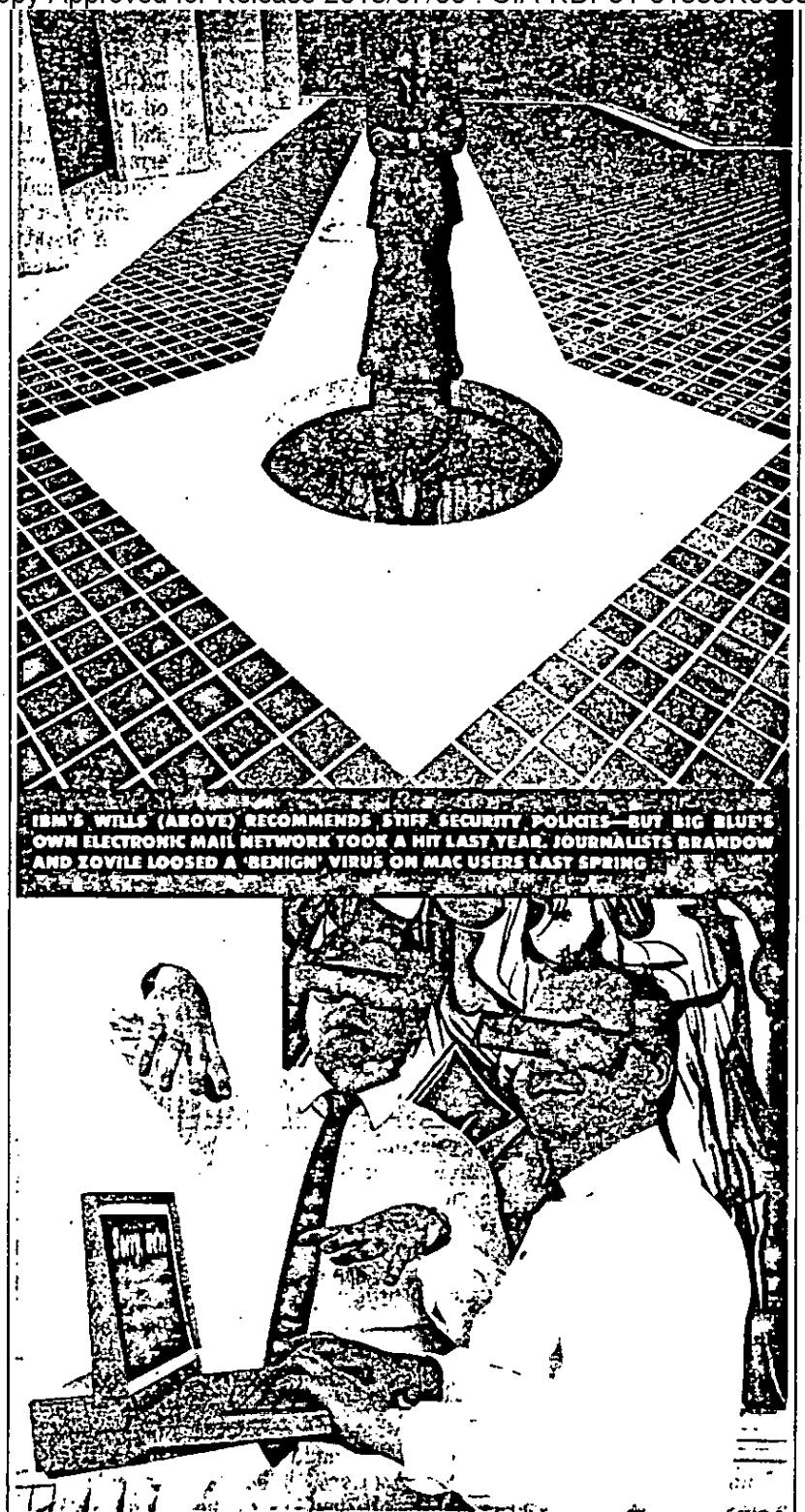
can now scan voice inflections, hand prints, even typing habits.

Still, common sense may be the best protection—and less intrusive. For example, USPA could have thwarted Donald Gene Burleson by thinking faster. The company procrastinated before changing its computer passwords, a crucial mistake: As a computer security officer, Burleson was one of three people at the company who knew everyone's password.

COVER-UP. A similar mistake caught up with Wollongong Group, a software company in Palo Alto, Calif. Ming Jyh Hsieh, a 38-year-old Taiwanese émigré who worked as a customer support representative, was fired in late 1987. Two months later, Wollongong noticed that someone was logging on to its computers at night via modem. Some files had been copied or damaged. After tracing the calls to Hsieh's nearby home, police seized her personal computer, along with disks containing Wollongong's proprietary software, estimated to be worth millions of dollars. She was arrested, charged with illegal access to computers, and if convicted faces up to five years in prison.

Wollongong had crippled Hsieh's access code but the company suspects that she somehow obtained another worker's. Since the incident, Wollongong periodically changes passwords and account numbers. "Any company that doesn't is asking to be kicked," says Norman Lombino, Wollongong's marketing communications manager.

One advantage for computer crooks is that their victims often keep quiet, notes consultant Robert H. Courtney Jr. Statistics are hard to come by. But experts estimate that only 20% to 50% of computer crimes are ever reported. Particularly for banks, a successful fraud is a public relations disaster. Burleson's break-in at USPA might never have come to light had he not sued for back pay—thus encouraging a countersuit. "No one wants to display their managerial shortcomings," says Courtney. In one extreme case, Courtney says, an insurance company executive used his PC to scan claim records needed to commit a $13 million fraud. The company found out and fired him. But to avoid a scandal, it gave him a lavish going-away party.



IBM'S WILLS (ABOVE) RECOMMENDS STIFF SECURITY POLICIES—BUT BIG BLUE'S OWN ELECTRONIC MAIL NETWORK TOOK A HIT LAST YEAR. JOURNALISTS BRANDOW AND ZOVILE LOOSED A 'BENIGN' VIRUS ON MAC USERS LAST SPRING

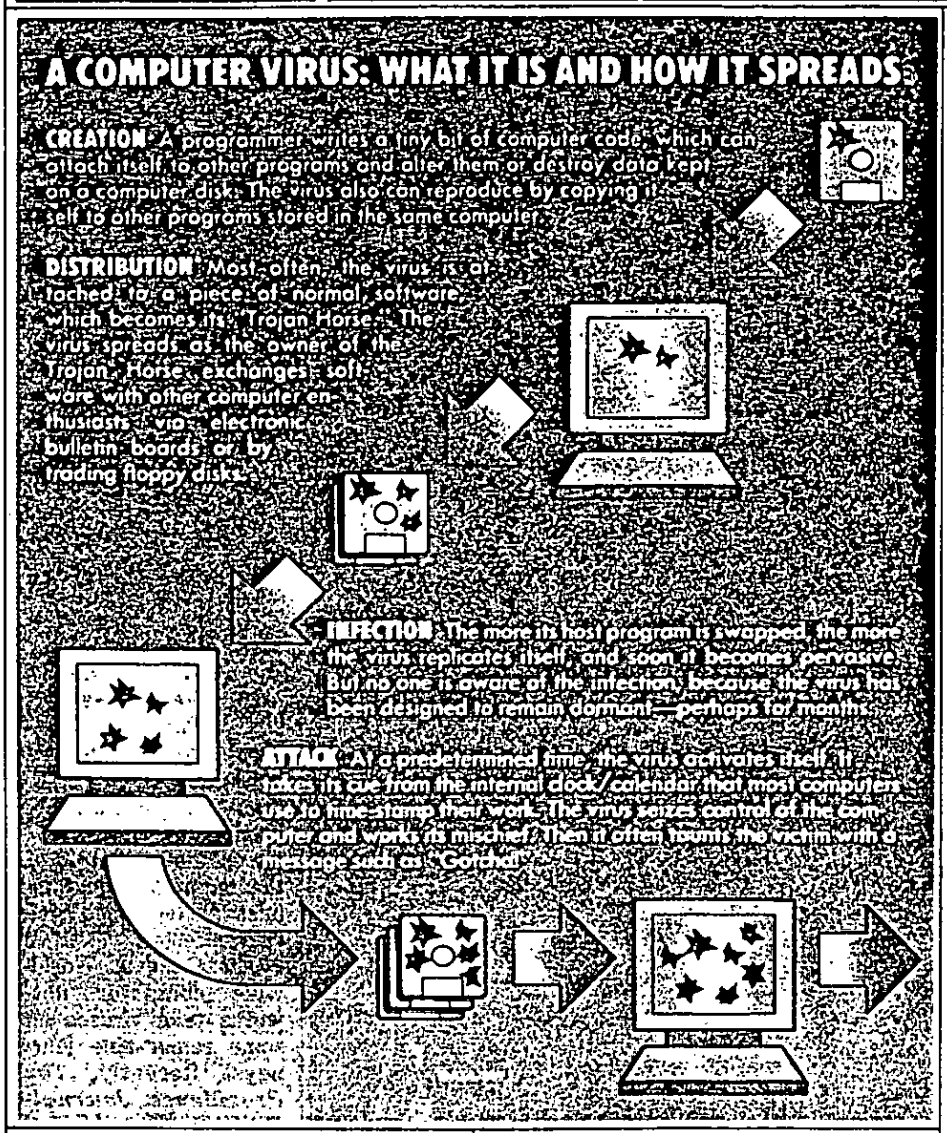
PHOTOGRAPHS BY ITOH BOTTOM) CLAUDIO EDINGER/GAMMA LIAISON. JONATHAN WENK

Bringing the problem into the open may be the only way to improve security, however. Take viruses. These wily programs most often find their way into corporate computer systems when an employee inadvertently introduces them. Computer enthusiasts from New York to New Delhi use electronic bulletin boards on communications networks such as The Source to "chat" by computer. One of their favorite pastimes is swapping programs—any one of which can include a virus that attaches itself to other programs in a computer.

No one knows how many viruses have been planted. But John D. McAfee, a virus expert at InterPath Corp., a security consulting firm in Santa Clara, Calif., says there have already been 250,000 outbreaks. He estimates that 40 of the nation's largest industrial companies have been infected.

PAKISTANI FLU. Worldwide computer networks take viruses on some remarkable journeys. Recently, *The Providence Journal-Bulletin* was infected by the Pakistani Brain—two years after that program began circulating. Nobody knows how it got to Rhode Island. But before it was through, it had infected 100 of the paper's personal computer hard disks. Basit Farooq Alvi, a 19-year-old programmer from Punjab province, says he wrote the virus not to destroy data but as a warning to would-be software pirates. The virus would interfere only with bootlegged copies of his package, a program for physicians. Other programmers, however, have given it a pernicious twist: Now versions of the brain often carry instructions to wipe out data files. And some of these versions have spread to Israel, Europe, and the U. S.

Even a well-meant virus can have unfortunate side effects. Richard R. Bran-



dow, the 24-year-old publisher of a Montreal computer magazine, and co-worker Pierre M. Zovilé created a benign virus to dramatize the pervasiveness of software piracy. Point proved: In two months, Brandow says, illegal copying had transferred the virus to 350,000 Macintoshes around the world. When the internal clocks on these machines hit last Mar. 2, the first birthday of the Mac II computer, each machine displayed Brandow's "universal message of peace to all Macintosh users."

'SAFE SEX.' It was a nice thought. But Marc Canter, president of a small Chicago software publisher, says that Zovile's virus wasn't innocuous. It caused Canter's computer to crash and infected disks that he supplied to software producer Aldus Corp. in Seattle. For three days, Aldus unwittingly transferred the virus onto copies of its Freehand illustration program on its assembly lines. Aldus pulled back the tainted disks, but not before some got to customers.

As with many computer security problems, the chief weapon against viruses is employee awareness, says Arco's Hoffman. After a virus invaded Macs at Arco's Dallas office, then spread to another Arco office in Anchorage, the company told employees not to use software of questionable origin. "It's the PC equivalent of safe sex," says Hoffman.

There also are more than a dozen "vaccine" programs, including Interferon, a package that Robert J. Woodhead, an Ithaca (N.Y.) author of computer games, offers free. Woodhead says each virus has a unique pattern, which his software can identify. It then erases the virus. Another method, in use at Lehigh University's computer labs since a virus struck there last winter, is to test suspicious software by setting the computer clock to Christmas, New Year's, or April Fools' Day—dates on which many viruses are set to detonate.

Viruses have caused such consternation that Congress is mulling tougher federal laws. A House bill introduced on July 14 would make it a federal crime to insert a malicious virus into a computer. Basic computer-crime laws are already on the books in 48 states, and business and industry leaders are looking for government agencies to set guidelines for security standards. Under the Computer Security Act of 1987, the National Bureau of Standards is charged with doing that. But agency budget cuts are expected to slow the process, industry officials say. In Japan, meantime, the government gives a tax break to companies purchasing facilities and hardware to guard their systems.

Even without such incentives, U.S. companies are spending huge sums on computer chastity belts. They can be anything from software to control access to the mainframe, costing $35,000 a copy, to hardware that scrambles data so it can't be understood if a phone line is tapped. In 1982 only 10% of IBM mainframes had data security software, according to a survey by market researcher Computer Intelligence. Now the figure is 35%.

To foil hackers, many companies are installing dial-back systems on computers. These ensure that an incoming call is from an authorized number. A large mainframe may have hundreds of "ports" for remote computers—with call-back units costing $600 to $700 per port. Additional encryption hardware can cost $1,200 per communications line. With the most to lose, banks are a big market for such equipment. They disguise data by encrypting it, and many use message-authentication techniques to ensure that what is received over phone lines matches what was sent.

MODEM MELTDOWN. In the wake of the Chicago fire, there's also new interest in "disaster recovery"—restoring operations after fires, floods, earthquakes, or sabotage. For years, companies have shipped computer tapes with sensitive records to vaults such as that run by Data Mountain Inc. in Phoenix, where gun-toting guards watch over a 2,000-square-foot room chiseled out of rock.

But the phone company blaze in the Chicago suburb of Hinsdale lent a new urgency to such planning. "The story has gotten out to Europe, Asia, and Australia," says Dave Haeckel, a principal with Arthur Andersen & Co., a Big Eight accounting firm that does computer consulting. That's been a boon for disaster recovery specialists such as Comdisco Inc. "I've never seen anything like this," says Raymond Hipp, president of Comdisco Disaster, which collects fees of $100 million annually from 1,000 customers to maintain backup systems. Comdisco says it can restore computer service in 24 hours.

Such a promise may be worthless if

ROB DOYLE

phone lines have melted, as they did in Hinsdale. "Nobody had really focused on the lack of redundancy in the Bell operating companies' networks," notes Hipp. Local phone companies relay computer signals to a long-distance carrier such as American Telephone & Telegraph Co. or a data network such as Tymnet, which relays the signal to a local phone company that picks it up for the customer. Without that last link, the most sophisticated computer network may be useless.

Most of the time, phone company backup systems route calls around trouble spots. But in Hinsdale, a worst-case scenario occurred. The automated phone switching facility was unstaffed and lacked the kind of fire-suppression system used in computer centers. There was no alarm at the local fire station, because Illinois Bell feared that the fire department couldn't put out a computer fire without causing excessive damage.

The result: Thousands of homes and businesses, including headquarters offices of McDonald's Corp. and Motorola Corp., were cut off. Large businesses restored communications with emergency microwave radio systems. But seven local businesses have filed lawsuits to recover losses caused by the outage.

Computer customers, as well, want better security features from hardware and software suppliers. Many companies are considering making AT&T's Unix software—or its derivatives—a standard to smooth the connections between different brands of machines. But since Unix was designed to make it easy for computers to share files and programs, it's also susceptible to break-ins, says Judith S. Hurwitz, editor of *Unix in the Office*, a newsletter.

For instance, phrackers in California, after cracking the password system on

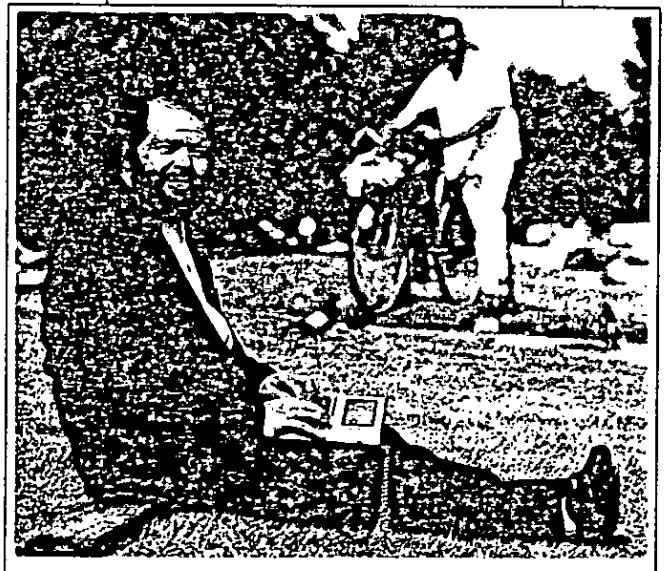
A GERMAN HACKERS' CLUB THAT PROMOTES CREATIVE CHAOS

West German computer hacker Bernd Fix holds the economic equivalent of a nuclear bomb in his head. The University of Heidelberg astrophysics student claims it took him only 20 hours to write a virus that could destroy all information in a mainframe computer—erasing tens of thousands of pages in minutes. In the wrong hands, it could cripple companies, the IRS, even the Pentagon. Fix has no such plans: He says he wrote the program as an intellectual exercise—"for the experience of doing it." He has since encrypted it so that it can't be used by others.

Welcome to the oddball world of hacking, German style. Fix, 26, is a member of the Hamburg-based Chaos Computer Club, a group of 300 hackers who, says Herwart "Wau" Holland, the club's founder and leader, are a far cry from the teenage thrill-seekers who prowl U. S. computer networks. Despite the club's name, Holland, 36, says it's against electronic mischief. His goal is more serious: increasing the flow of public information. In West Germany, environmental and scientific data, census figures, and government reports are costly and difficult to get. "It's not a very democratic system," Holland says. Not until Chaos gets involved.

Holland's weekly newsletter, circulation 3,000, and his "Hacker's Bible," 25,000 copies sold, are filled with tips on breaking into computer systems around the world. "We believe we have the right of access to information, and we take it," says Holland. During the Chernobyl nuclear disaster, he says, German officials "fed the public a lot of false [reassuring] statements." By purloining hidden data, "we made sure the press was well informed"—a claim that German reporters confirm.

FORBIDDEN FUN. Chaos members, who meet weekly, hold an annual convention, and pay dues of $66 a year, revel in showing up West Germany's obstinate bureaucracies. In 1984, Chaos uncovered a security hole in the videotex system that the German telephone authority, the Deutsche Bundespost, was building. When the agency ignored club warnings that messages in a customer's private electronic mailbox weren't secure, Chaos members set out to prove the point. They logged on to computers at Hamburger Sparkasse, a savings bank, and programmed them to make thousands of videotex calls to Chaos headquarters on one weekend. After only two days of this, the bank owed the Bundespost $75,000 in telephone charges. Uncaught, Chaos revealed its stunt on Nov. 19, the birthday of Bundespost Minister Christian Schwartz-Schilling. Both the bank and the Bundespost now say the break-in was a fluke.



HOLLAND: "WE HAVE THE RIGHT OF ACCESS TO INFORMATION"

The incident fits with Holland's goal "of changing structures in society. Everything in Germany is so overly organized." He adds: "Some people throw bombs. It's more effective to find the absurdities and make people laugh."

Like hackers everywhere, however, Chaos members can't resist a challenge. And that sometimes means treading near the edge of West German law, which prohibits manipulating or destroying data, both foreign and domestic, or breaking into "extra secure" systems, which are undefined. Holland denies that the club was behind a NASA break-in last year. Chaos members may have done it, he concedes, though none has confessed. But he adds: "We do not encourage illegal acts."

That's an assertion that critics often discount, given the club's key role in promoting hacking—and its record of never having expelled anyone for unsportsmanlike conduct. Still, Holland, who traded his blue jeans for blue suits when he started a typesetting business 18 months ago, knows that hacking can hurt. Three years ago, fellow enthusiasts stole his password to a German data network and published it in the tabloid *Bild Zeitung*. Soon gleeful computer fanatics had racked up $1,500 in charges to Holland's account. "I was broke at the time, and this incident made an impression on a lot of hackers who knew me," he says.

Nonetheless, there's still the matter of all that closely held government information. And until it's more public, Chaos most likely will fill the void.

By Gail Schares in Heidelberg

one Unix computer last year, used the same approach to unlock Unix-based systems at phone companies all over the country. Now AT&T is making Unix more secure. Similarly, Digital Equipment Corp. says it has patched software holes that let West German Chaos Club members break into its VAX computers.

HIGH-TECH HIJACKING. Concern over computer security will mount as companies do more electronic transactions. In the $55 billion textile business, for instance, sales data, new orders, shipment information, inventory receipts, and invoices are beginning to flow directly from one company's computer to another's via a pipeline called Electronic Data Interchange. Other companies, such as auto parts makers, are using EDI to send items directly to customers, bypassing warehouses. The potential for fraud and theft is huge. "There have always been attempts to divert products," says Peter Browne, president of Profile Analysis, a Ridgefield (Conn.) consulting firm. "Now it can be done electronically."

Corporations are left in a bind: They need to expand computerized information and transaction-processing systems to compete. But the more they do, the greater their risk. "Our society must do something to control the problem," says Ernest A. Conrads, director of corporate security at Westinghouse Electric Corp. "If not, our information system can't grow the way technology will allow us to." In the long run, that could have more profound economic consequences than all the hackers, viruses, and disaster-induced computer failures combined.

By Katherine M. Hafner in New York, with Geoff Lewis in New York, Kevin Kelly in Dallas, Maria Shao in San Francisco, Chuck Hawkins in Toronto, Paul Angiolillo in Boston, and bureau reports

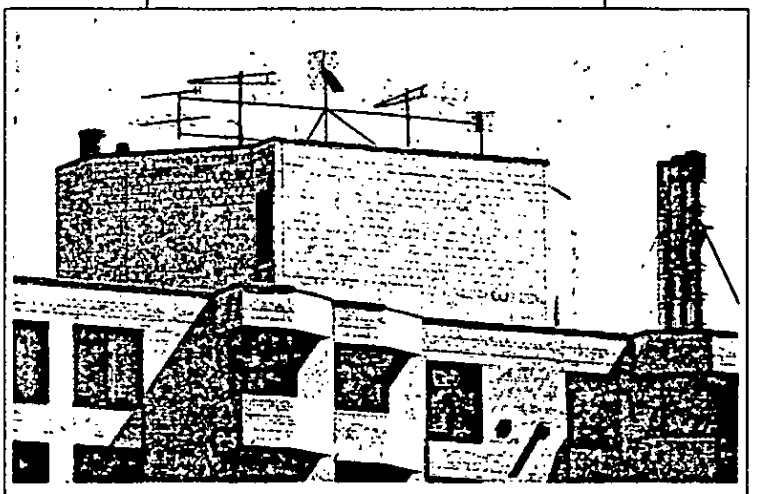
HOW UNCLE SAM'S CLOAK-AND-DATA BOYS ARE FIGHTING BACK

Breaking into computer systems might be a lark for hackers. But penetration of government computers—particularly military systems—is a deadly serious matter for the National Security Agency (NSA) and for counterintelligence agents at the Federal Bureau of Investigation. After all, who's to say whether a break-in is a hacker's harmless prank or an attempt by Soviet spies to steal defense secrets?

The supersecret NSA, an arm of the Pentagon that for many years didn't even exist officially, has a double-edged mission. It gathers electronic intelligence from the Soviet bloc by intercepting and decoding telecommunications traffic, including signals sent from spy satellites. And to prevent foreign nations from doing the same to the U.S., the NSA spends untold millions devising sophisticated cryptographic codes and trustworthy computer systems.

Protecting government computer systems is becoming increasingly taxing. Intelligence organizations, the military, and other federal agencies now operate more than 100,000 computer sites—most with multiple computers and communications links. Many thousands of additional computers used by defense contractors and high-tech manufacturers hold data that the Administration doesn't want leaked.

The Soviets leave no stone unturned in their hunt for the tiniest morsels of information. Even a routine electronic mail message between a defense supplier and a bank might provide an important clue. That's why the Soviet missions in Washington, New York, and San Francisco bristle with antennae. They pick up phone conversations and data transmissions relayed by cellular radio and microwave links. In Cuba, a giant KGB-operated dish pulls in signals beamed down from satellites to any point in the lower 48 states. And Soviet snoop ships monitor both coasts from just outside U.S. territorial waters. One intelligence expert estimates that the Soviets listen in on more than half of all U.S. telecommunications traffic, one way or another.



ALL EARS: SOVIET EMBASSY IN WASHINGTON

SPOOK-PROOF. Because almost any transmission runs a high risk of being intercepted, Washington goes to great lengths to protect its secrets. Its most secure lines are fiber-optic cables buried deep below the surface and sealed in gas-filled pipes. There are no connections to outside phones, so no hacker can gain access. If a spy cuts a pipe to tap the cable, the drop in gas pressure instantly sounds an alarm.

But buried cables are of no use in communicating with ships or planes. So the NSA has developed elaborate cryptographic ciphers for turning English into digital gibberish. These codes are so convoluted that any given string of characters, such as this sentence, would never yield two identical series of encoded characters. The cipher is changed frequently, so that the digital code for an "e" in one word might mean "k" in the next.

To decode such a message, you need the key: the starting cipher plus the formula for switching to the next variant. For computers that handle the most sensitive information, crypto keys are created in pairs, then delivered by courier to the two computer sites. So even if the key for the link between the Pentagon and a particular base is copied, it won't help decode traffic between any other points.

Still, nothing offers total protection. Just as private-sector computer crime is usually traced to employees, the NSA's worst fear is that turncoats will sell cryptographic secrets. Crypto details are so secret that even the names used to classify them are classified. That's why federal officials say that former Navy radiomen Jerry A. Whitworth and John A. Walker Jr., who for years passed top-secret crypto materials to the KGB, did more harm than any other spies in decades. Officials estimate that the Kremlin used its ill-gotten gain to decode 1 million military messages. That could make it the computer crime of the century—so far.

By Otis Port in New York

WALTER CALAHAN

Every year as winter approaches, people brace themselves for the flu season. They take precautions that will help them stay healthy, or at least minimize the symptoms: lots of fluids, large doses of vitamin C and sometimes flu shots. If you're human—like most of us are—they're pretty good deterrents. If you're a computer—like most of us aren't—you've got a problem. Unless, however, you're a computer user—like most of us are—in which case you may face exposure to the latest PC ailment as well: software viruses.

None of us probably ever thought of flu viruses affecting machinery, but this year that's changed. In the last few months, the personal computer community has lapsed into its own flu season that knows not the bounds of winter or cold weather. The talk of viruses has been rampant, with cases reported across the United States, in Canada, Israel, Germany and Great Britain.

In reality, though, few viruses have actually been found. The media hype surrounding viruses has tended to distort the situation. Nonetheless, the warning is clear: we all need to be aware of the potential damage a "virus" can cause and implement appropriate safeguards against the problem.

A virus is a small program that indeed operates much the same as the common flu virus. In the right environment, it can be highly contagious, moving rapidly from PC to PC. It can spread in many different ways, but typically it is embedded in an innocent program such as a disk utility. When the utility is run, the virus program searches for target programs. When it finds them, it embeds itself and waits for some predetermined event such as a date, time or operation. When the system triggers that particular event, the virus attacks and erases whatever data it can find. The real danger is twofold: the virus remains hidden until it strikes and it is designed to spread before it acts.

Viruses are not new to the computer industry. In 1980, researchers at the Xerox Palo Alto Research Center (PARC) devised a virus-type program designed to spread through a network looking for idle machines that could help solve large problems. The program eventually got away from them, invading central processing units and locking up even the active workstations on the network. The researchers ultimately regained control by writing a "vaccine" program that erased all traces of the virus.

In September, 1984, Dr. Frederick Cohen of the University of Cincinnati warned about the threat of computer viruses in a paper presented to a computer conference in Toronto, Canada. According to Dr. Cohen, most mainframe computer systems can generally be subverted by a virus in the space of an hour. His paper drew wider attention in March, 1985, when *Scientific American* published a letter from two Italian programmers in its "Computer Recreation" column. The letter gave a virtual blueprint for a virus that could attack personal computers.

TIME BOMBS

Last fall in Israel, a virus spread widely over a two-month period, the apparent expression of a political protest. The virus contained a "time bomb" designed to go off Friday, May 13, 1988, on the 40th anniversary of the last days of Palestine; the state of Israel was established on May 14, 1948. Fortunately, a flaw in the virus led to its early discovery in December. The flaw caused the virus to repeatedly infect target programs until they grew so large that they filled all available storage space. The virus itself caused the infected computer system to slow to one-fifth its normal speed and to randomly display garbage on the screen.

Another virus was discovered last December at Lehigh University in Pennsylvania. Dubbed the Lehigh Virus, the program was designed to infect all Command.Com files on whatever peripherals it found. Whenever an internal command (Type, Copy, Delete, etc) was executed, the program immediately looked for other Command.Coms to infect. When it found one, the original virus implemented a counter. When the counter reached four, the original virus deleted everything it could. It didn't just execute a normal DEL to erase a directory entry, however—it totally erased the file-allocation table, boot tracks, directory and more. Lehigh students lost several hundred diskettes' worth of information before the MIS department discovered the cause.

The ease with which viruses can spread through networks is causing major concern among computer professionals. It was a rapidly spreading virus known as the "Christmas Virus" that caused IBM to shut its network down for several hours last year. The work of a West German student, the program was designed to look like a computerized Christmas card. When run, it would move undetected into a user's files and send copies of itself to everyone with whom the user had exchanged messages. Originating at the European link of Bitnet, the world's largest academic network, the program eventually spread to five continents, including into IBM's own massive network, flooding its systems with the Christmas Virus. While the program was not destructive, it did cause significant system degradation, eventually requiring a system shutdown in order to remove all traces of it.

Virus infections haven't been limited to the IBM world. In February, a virus was discovered in a HyperCard stack (HyperCard is a freeform database application for the Macintosh, with its information arranged into stacks) on the CompuServe network. The virus, written by the Canadian magazine *MACMAG*, was programmed to send a message of world peace on March 2, 1988, the first anniversary of the Macintosh II computer. After CompuServe alerted its users of the virus, there were reports of it in Italy, Belgium and France, as well as in most areas of the U.S.

This particular virus also became the first known virus to infect commercial software. A contractor for Aldus Corporation apparently came into contact with infected software while traveling in Canada. Running the software just once on his system was enough to spread the virus to his hard disk. At the time, he was working on training software for Aldus; the virus infected the disk he sent them as well. From there, it spread through Aldus, eventually getting onto the disk duplicating equipment used for its FreeHand program.

IMPLICATIONS FOR NETWORKS

Though viruses have a limited effect on single-user machines, they can cause quite serious problems for a network. Imagine, for instance, a network administrator placing the latest version of a handy utility he has used for years in a general-access directory. Various "power" users then access the utility. As the virus goes out and copies itself to all the Command.Com files it can find, its counter is activated, triggering the virus to erase everything it can access.

When the complaint calls start coming in, the last thing the administrator will look to is the utility he's been using for years. At first, users are likely to be suspect; as the virus continues to spread, attention will shift to the next most common element, the network server software.

A VIRUS ORIGINATING IN WEST GERMANY AND BEARING CHRISTMAS GREETINGS EVENTUALLY SPREAD TO FIVE CONTINENTS.

Article # 2 (cont)

RUSS GREENBERG HAS DARED ANYONE WHO WRITES VIRUSES TO TRY TO DESTROY HIS BULLETIN BOARD SYSTEM. SOME HAVE TRIED —NONE SUCCESSFULLY.

One symptom that should help identify a virus to a network administrator is the manner in which data corruption occurs. Most viruses do not appear to be written with networks in mind, so when the damage is done, it is usually limited to the floppy and hard disk drives on a single user's machine. According to Russ Greenberg, an authority on viruses, most of them directly access the PC hardware when they corrupt data. When a PC is connected to a network, it is addressed through software added to DOS. When a virus does its work through DOS, all devices connected to that PC are corrupted. As noted, to date no virus has been encountered that was specifically written for PC networks.

What can be done to keep a virus off of a network? The initial tendency is to suggest banning all public domain software and unauthorized programs. It's an unrealistic approach, however, because, as we saw with the Aldus virus, it is possible for a virus to infect virtually any type of software without being detected. On a network with many users requiring full access, a software ban would also be difficult to enforce. Every user has favorite utilities, so trying to ban outside programs could force at least some users "underground," and outside programs might still be used anyway. A better route would be to publish guidelines for the use of outside programs.

A program of network security awareness is another effective measure. It requires getting everyone involved, because network security is only as good as its weakest link. In a large network, you may want to designate an individual in each department to be responsible for security in that area.

NETWORK SECURITY

Even with well-planned security guidelines, a virus (or an unhappy employee) can still corrupt your data. The ultimate resort is to use backups. Horror stories abound about companies losing thousands of dollars worth of data, yet the fact remains that many users and administrators alike don't worry about backup until they actually encounter the problem of restoring lost data. *You can never back up your system often enough.* Even after your data is safely backed up onto a tape or cartridge, verify that it is indeed there. If you don't have a regular backup program, develop one *(see sidebar)*, and stick to it.

Although the hope is that you never experience a virus destroying your system's data, the recent flurry of symptoms have served to increase our awareness of the threat. Now, as we move from single-user machines to networks capable of storing gigabytes of data, we need to adopt the measures that can and will protect the integrity of our data. Mainframe computer systems have had such safeguards for years. By adopting similar guidelines and taking reasonable measures, we can protect our systems from most threats and still enjoy the freedom of sharing data with others.

Rick Bunzel is Manager of Core Course Development at 3Com Corporation.

FIVE GUIDELINES FOR KEEPING YOUR NETWORK HEALTHY

1. Write-protect boot diskettes. Many viruses attack Command.Com files and a simple way to protect boot diskettes is to make sure a program can't write to it. The write-protect tab on a diskette is a physical device, so it is difficult to bypass.

2. Do not give network users more network access than they require. A local area network gives us plenty of data access, and when a virus is triggered it can potentially delete or corrupt every directory that a user can write to or delete files from. All users should review their sharenames and links and ask themselves: Do I need to have Read/Write/Create access? Do I need to maintain that network directory link? Can I link to network directories as the need arises?

3. Maintain at least several generations of backup tapes. Due to their nature, it is possible for a virus to hide in your system for several weeks or more before it is discovered. Before you restore a tape, you will want to go back to your last reliable backup and start restoring from there. And last but not least, archive tapes on a regular basis. Tape is cheap in comparison to the cost of rebuilding data from scratch.

4. Do not use new programs (or updated versions) unless they have been in the public domain for at least four weeks. On most bulletin board systems, users can check the message board to see if anyone has commented on a particular program. Most bulletin boards also contain a file called "The Dirty Dozen." This file alerts users about programs that are known to be a "Trojan" (programs that act instantly to corrupt data) and potential viruses.

5. All programs should be tested with utilities such as CHK4BOMB or BOMBSQUAD. These public domain utilities examine code for potentially dangerous disk activity such as a command to format a disk or to delete a directory.

STEPS THE BULLETIN BOARDS ARE TAKING TO AVOID AN EPIDEMIC

The electronic bulletin board systems (BBS) industry is concerned about the potential damage that viruses or "Trojan" programs could cause, and so BBS operators have been aggressively policing themselves. Two operators in particular have gone to great lengths to stop foul play.

Russ Greenberg, the operator of a bulletin board in New York, has written a program called Flu-Shot that counters viruses. Since December of last year an estimated 25,000 users have added the program to their systems. Greenberg challenges anyone who writes viruses or hidden bomb programs to upload any program they want in an effort to destroy his bulletin board system. So far, a few have tried, without success.

This year, Greenberg has released three versions of Flu-Shot. The current version, Flu-Shot+, has become a shareware program with a slight twist. Normally, shareware authors ask the user to send them a contribution if they like and use the author's program. Greenberg is willing to donate users' contributions to their favorite charity.

Eric Newhouse, System Operator of the CrestBBS, authored the current "Dirty Dozen Upload Program Alert List." Distributed via bulletin boards across the country, the "Dirty Dozen" was originally created by a BBS system operator named Tom Neff, who kept it as a simple list. It has evolved over three years to become a comprehensive document that lists pirate programs (copyrighted programs distributed without the author's knowledge) as well as Trojan and virus programs. The listing also includes instructions on how to handle a program that has corrupted data and a glossary of commonly used BBS terms.

Russ Greenberg can be contacted at (212) 889-6431; Eric Newhouse can be reached at CrestBBS at (213) 471-2518.

—Rick Bunzel

Computer Viruses Can be Hazardous

In recent months, a great deal of interest and concern has been generated by the appearance of several computer viruses in both IBM PC's and Apple Macintoshes. Such programs have two primary characteristics: 1) They spread themselves from machine to machine using self-reproducing code, infecting other systems and stashing away code into as many "carriers" as possible. 2) They exhibit the "symptoms" intended by the author of the virus. This could be any number of things, even the erasure of one's disk on a specific date.

Viruses have been designed to attack mainframes, minicomputers and desktop microcomputers, and they aren't partial to any particular brand name. One of the more recent mainframe incidents was a virus that invaded IBM's mail system and brought it to its knees for a couple of days. IBM PC users have experienced viruses for several years, most commonly through the COMMAND.COM file.

Viruses are not all meant to be damaging. The programmer may just want to prove he can do it and have the satisfaction of some notoriety. The Macintosh community got their first taste this winter. The "MacMag virus" was put on a national bulletin board system hidden in a HyperCard stack. It displayed a "universal message of peace" on one's computer on March 2, then removed itself.

Most viruses spread via public bulletin board systems and are hidden in public domain programs. "Sexy Ladies," distributed at MacWorld Expo in San Francisco, erased whatever hard disk or floppy disk it was on when it was launched!

Virus Hunting

When your computer begins to do things out of the ordinary, or when it stops being able to do things it has always done in the past, a virus may be involved. However, corrupted system files can also lead to similar symptoms. When problems occur, they are much more likely to be the result of non-virus difficulties. When you have excluded normal problem areas, you should look into the possibility that your system has been infected by a virus.

Use a general disk editor to look for invisible files. Unless you have an application that creates them, every such file is suspect. Also, a general check of all the files in your system for resources that don't belong in those files is well worth the effort. A virus might infect any and all applications, system files, or COMMAND.COM and AUTOEXEC.BAT files. A virus might corrupt any file on an infected volume or system, including system files, documents, applications, *etc.* Some viruses insidiously alter numeric values within spreadsheets just slightly.

The use of networks can easily enhance the spread of a virus. Different scenarios are possible, with the simplest being a public domain area on a server from which everyone gets public information. Also, shared applications residing on a server could become infected, which would then infect every machine on which they were run.

Vaccination

The following precautions help prevent problems:

Write-protect your master diskettes. This prevents a virus from spreading to your original disks. Disk locking mechanisms are typically hardware based—viruses can't infect locked disks!

Protect your networks. Network administrators should not allow just anyone to put software on the server. Applications on a network server should come only from known good masters.

Be wary of public domain software. It should be checked quite thoroughly on an isolated system for any infections before being used on production systems. This also protects one from "Trojan Horse" programs such as "Sexy Ladies."

Quarantine infected systems. If a system is identified as infected with a virus, immediately isolate (quarantine) it from other systems. This means disconnecting it from any network and not allowing anyone to take any files from the exposed system to another system. Once the system has been "disinfected," the files can be copied or moved.

Article #4

Computer viruses—Your PC could be at risk!

A PC coordinator "swat team" is being formed to deal, on a company-wide basis, with problems related to computer "viruses."

Computer "viruses" are so-called because they behave like viruses that invade the human body: they are mischief-making programs that get into computers, propagate and spread—in some cases "lethally," wiping out entire contents of hard disks.

Computers can be exposed to "viruses" in a variety of ways: from freeware or shareware downloadable from bulletin boards, from software acquired from friends, or from shareware ordered by mail.

Following are some suggestions offered by security experts:

✔ Don't download executable programs for use at work. Avoid the the following known contaminated public bulletin board PC programs:

ARC (not the GE version)
ARC513
ARC600
DISCSCAN.EXE
DOSKNOWS.EXE
EGABTR
FILER.EXE
LIST60
QMDM110.EXE
QMDM110A.ARC
QUIKBBS.COM
SECRET.BAS
STRIPES.EXE
VDIR.COM

✔ Use only site licensed software and software that comes in factory sealed containers from reputable dealers.

✔ Never run your system from the original program disks. Always make a backup of the software and put the originals in a safe place. If you have to reinstall software, you want to guarantee that it is not infected.

✔ Do not use public domain software.

✔ Do not accept copied or pirated software.

✔ Never allow an unfamiliar disk to be put on your system.

✔ Back up your data files often, for disaster recovery. All applications, including operating system files, must be deleted to remove viruses.

A Macintosh virus called *SCORES* has been found within Apple and a number of government agencies in Washington. To determine if your Macintosh has been infected, follow these procedures:

1. Open the system folder and locate the notepad file and scrapbook file.
2. Examine the icons used on these files and check that they resemble the small Macintoshes seen on the system and finder icons.
3. If they do not, and instead resemble the standard Macintosh document icon (an upright piece of paper with the upper right corner folded forward), your computer is infected.

If your Macintosh computer is infected, a program is available that will attempt to eradicate the virus from any infected files. A program named *Vaccine* will alert you if a virus tries to attack your computer. ■

If you have questions or feedback on computer "viruses," please contact your local PC coordinator.

Computer Viruses

Or, Do You Know Where Your Software's Been?

by Mark Hiatt

There's been a lot of talk lately about "The Computer Virus Problem." The newspapers and TV networks have carried stories about "infections" and the problems that result when trying to clean an "infected" system.

However, there is just as much talk that the whole virus scare is like an urban legend (like the poodle in the microwave). . . hard to pin down as a fact. But whether the threat is real or imagined, it is better to be informed about these things. . . just in case.

So, what is a computer virus (also referred to as a Trojan Horse)? Usually, it is a piece of code within a program that has nothing to do with the program itself. It copies itself onto other programs or system files and often "sleeps" until a certain date or event occurs. Because it copies itself onto other files, it can easily jump from disk to disk. If you use more than one computer, say one at work and a similar machine at home, you could carry an infected disk from one to the other and spread the problem around the office.

"The newspapers and TV networks have carried stories about large mainframe systems becoming infected."

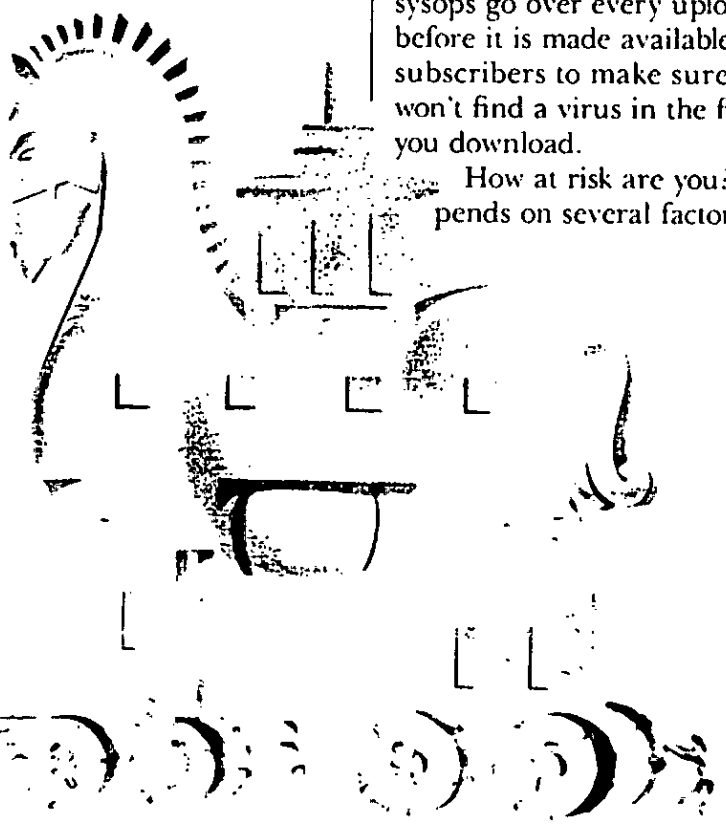
The name "Virus" stems from this contagious quality in the program. Just as a child picks up a cold at school and brings it home, where a parent gets it and takes it to the office—a computer virus can be caught from a disk a friend gives you or from a local BBS and spread to machines in your user's group, workplace and beyond.

A computer virus may be relatively benign, rising up now and again to flash a nasty picture or cause your machine to beep. That's not serious, just an annoyance (unless you're showing the boss your latest spreadsheet figures). However, a virus can also be vicious—lurking on your system for just the right situation, waiting to erase the files on your hard disk—and that can be several megabytes of data.

On GEnie's RoundTables, the sysops go over every upload before it is made available to subscribers to make sure you won't find a virus in the files you download.

How at risk are you? It depends on several factors. Do

(over)



(Continued from page 3)

you trade or share software with friends? Do you log onto several local BBS systems? If you do, do you download a lot of files? Do you put these files directly on your hard disk, if you own one? You may be at risk if you answer yes to any of these questions. Another big factor is the type of computer you own and the software available for it.

But what do you do if you don't write programs, can't read programming languages and wouldn't know a core-dump from the city dump? There is probably an anti-virus program on GEnie in your computer's RT library. Many of these are very thorough and are either free or shareware.

Charles Strom, of the IBM RT recommends "Flushot" (FSP-12.Arc), CHK4BOMB and STRINGS to owners of IBM (and compatible) computers, and assures IBMers that the paranoia is not warranted by what the IBM sysops have seen so far. Still, Charles says that you can search their software library for the keywords "Trojan" (as in Trojan Horse) or "Virus." These will turn up dozens of files dealing with protection.

"GEnie sysops go over every upload before they are made available to subscribers."

David Kozinn (also an IBM sysop) adds that many programmers are taking the threat into account, by including virus-checking routines in their programs. If something tries to attach itself to one of these new programs, it's detected. Over at the Apple II Library, check into "Apple.Rx" from ProSel's Glen Bredon. It's a shareware program that Tom Weishaar, Apple II Manager recommends.

If you own a Macintosh, try "Vaccine" from CESoftware's Don Brown. It's a free file you place in your System folder and forget about—until it finds something questionable. Then you can quit what you're doing and have a look, or ignore the warning and proceed at your own risk. Bart Barton says that a search of the Library will turn up other anti-virus programs as well.

"Never put a disk in your machine unless you're sure of where it's been."

What do you do if you're infected? In most cases, simply destroying the affected software will do the trick (you do still have the originals, right?).

Of course, you'll want to stop sharing or trading software, and it would be a good idea to let your friends know, so they can check for themselves. Once you've restored everything from the originals, you should be alright again. But be careful not to contaminate your original disks, otherwise you'll just end up making multiple copies of the virus.

What can you do to make sure you're not at risk? We can learn a lesson from Dr. Ruth Westheimer here—stay monogamous and use protection! Don't share software with just anyone, and never put a disk in your machine unless you're sure of where it's been!

Rx for Computer Viruses

Several anti-virus programs are available on GEnie. These can be found in the machine-specific RoundTables. Below is a list of programs you can download from the RT libraries which provide virus-checking routines. However, files are frequently updated, if you have trouble finding these, try searching the RT libraries under the keyword TROJAN or VIRUS.

Roundtable	File Name
IBM	Flushot (FSP-12, Arc) CHK4BOMB STRINGS
Apple II	Apple.Rx
Macintosh	Vaccine
Atari	Protect.Acc
Amiga	Trojan_Horse_Warning

STAT

PC MAGAZINE

FIRST LOOKS

Confronting the Growing Threat of Harmful Computer Software Viruses

PC ANALYSIS

BY JIM SEYMOUR AND JONATHAN MATZKIN

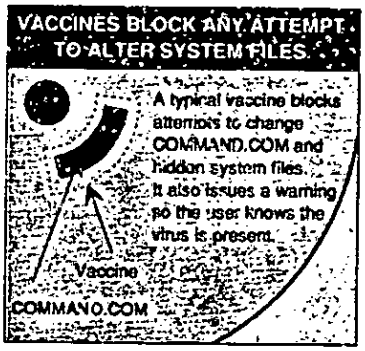
Now you see it; now you don't. Or maybe you never really saw it at all.

That will-o'-the-wisp nature of computer viruses, and the incredible difficulty of proving their role in the loss or destruction of data, have made tracking them down, defeating them, and protecting against them incredibly difficult.

It is so easy to lose data in a computer system—any computer, from a PC to a Cray supercomputer—that often, over the last few months, what was almost certainly operator error, or magnetic media wear, or power-line fluctuations, or any of a hundred other quite normal if no less frustrating events, has been misidentified as the work of computer viruses.

But that is not the whole story.

The skeptics insist that the computer virus alarms heard this spring are overstated. That skepticism has been fed by wild and unconfirmed reports, impossible to track down, of such infections as one that supposedly brought the Unix systems of a telecommunications giant to their knees, or a "PLO" virus aimed at shutting down the Israeli defense computer system.



It isn't surprising that these stories should have persuaded the skeptics that viruses are cruel jokes, this year's brand of black humor.

But the skeptics are wrong.

Computer viruses, written specifically to destroy programs and data residing in personal computers, are real and have been widely distributed. Many PC users have lost important work, at substantial cost.

Viruses exist.

The bad news: they can represent a clear and present danger to the programs and data stored on your computer's disks. But there's good news: you can avoid viruses through reasonable measures, and counterviral products are available to help detect viruses lurking on your disks and to protect against future infections.

Kenneth VanWyk knows computer viruses are real, because he's been fighting them. A Senior Consultant at Lehigh

(continues on page 34)

Why It's Time to Talk About Viruses

Over the last three months, the computer-virus story has ripped through the computer community like a prairie fire. Reports of program- and data-killing viruses have made for sensational reading in daily papers, business magazines, and some computer publications.

Many of those stories have been grotesquely exaggerated, while others have gone to the opposite extreme, denying the existence of viruses or branding them as bizarre hackers' jokes.

At *PC Magazine*, we, too, have worried about computer viruses. We have had our own encounters with them. But too many of the stories we have seen and heard were self-evidently false. Too few facts supported claims of viral disasters.

We have investigated every report we have found of computer virus infections. We have talked with those who believe they have suffered through those infections, with those who have beaten them back, and with those who have created programs to detect and, sometimes, defeat viruses.

And we have learned the chilling truth: computer viruses are very real threats. We have satisfied ourselves of their existence, of their very real damage, and of the importance of alerting computer users.

Even though we acknowledge that turning the light of publicity on those who take pleasure in destroying the work of others will inevitably encourage some of these vandals, we cannot turn away from a responsibility to warn our readers.

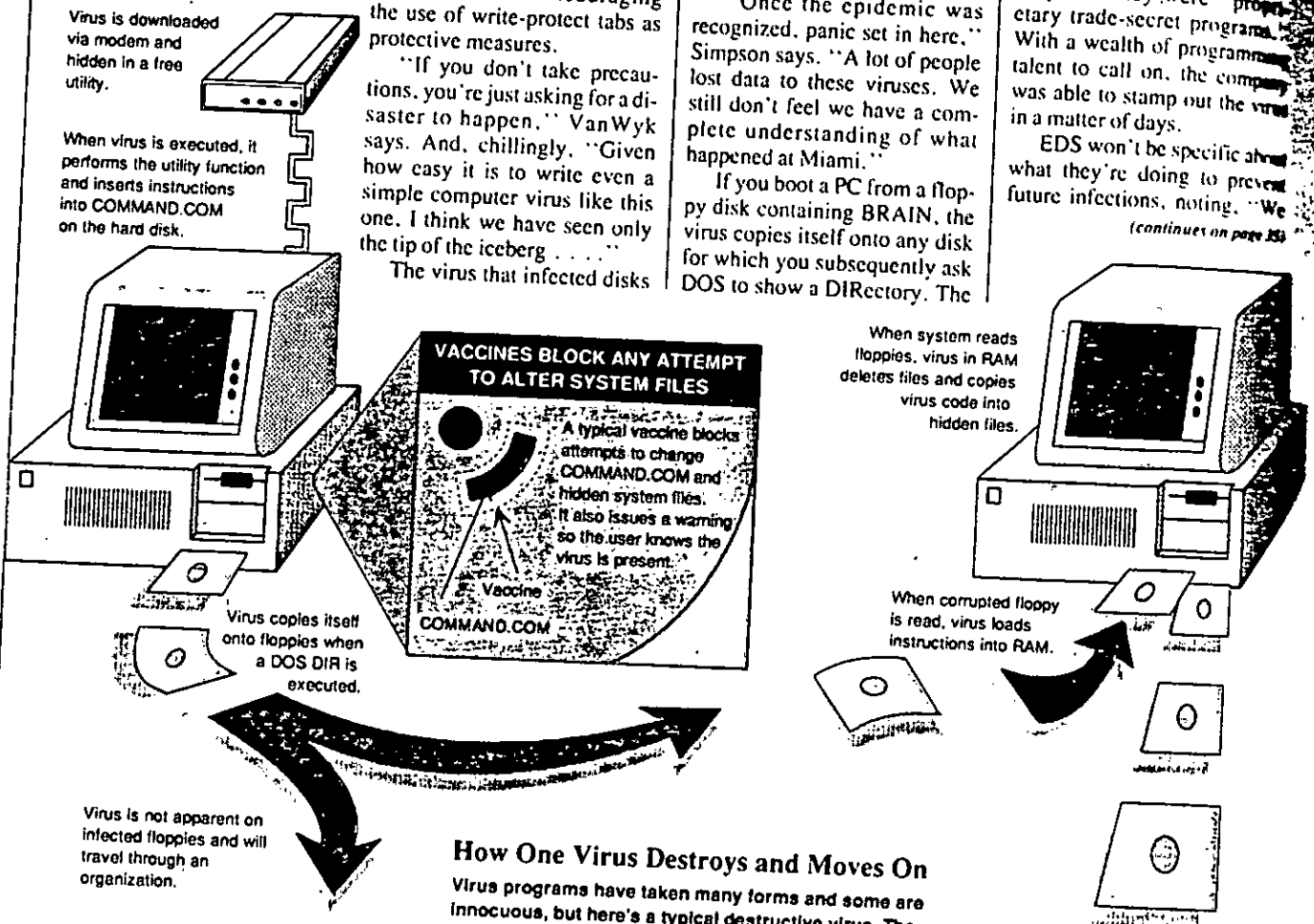
And to help them counter that risk. Because this has got to stop.

In the words of Don Brown, whose efforts to stop the SCORES virus on the Macintosh have been a beacon for others, "The whole thrust of the personal computer has been bringing control of the computer to the user. Viruses steal that control away, and replace it with fear, uncertainty, and doubt. Why would anyone want to take such a gigantic step backwards?"

Why, indeed?

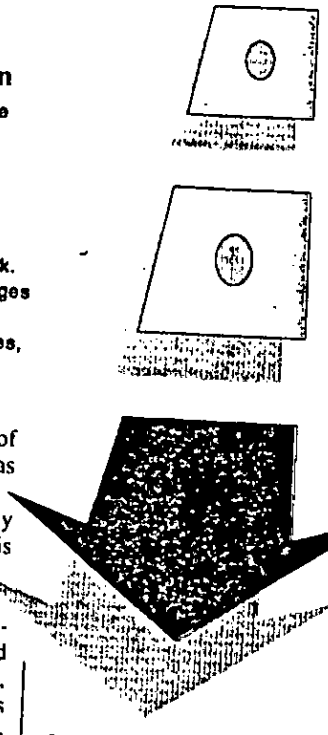
—The Editors

HANDS-ON INDEX



How One Virus Destroys and Moves On

Virus programs have taken many forms and some are innocuous, but here's a typical destructive virus. The author alters a popular public-domain or shareware program offered on a public bulletin board to include the virus code. The host program runs as expected after it's downloaded, but the virus sets off on a different path, targeting the system files on a hard disk. Most vaccine programs are designed to prevent changes to the system files. They'll also flash a warning that the active program is attempting to make such changes, a sign that this is a program you want to erase immediately.



Since data loss occurs, infected floppies may lead to discovery of virus, but tracking virus to original system may no longer be possible.

Viruses

(continued from page 33)

University's Computing Center, VanWyk has seen hundreds of IBM PC users' floppy disks erased by a runaway virus launched by a computer vandal.

"This thing was discovered about two days before Thanksgiving break last fall," VanWyk recalls. "If some students had not discovered it then, and people had gone home for the break, it could have gotten a lot worse. Because if students had taken infected floppy disks home with them it could have gone a lot farther . . . to their home machines, and from there, with Mom and Dad into their offices."

Lehigh has developed its own "vaccine," a program that checks the COMMAND.COM file at boot-up and, if it finds the virus, writes over that part of the disk. And the university has also begun using "notchless" floppy disks and encouraging the use of write-protect tabs as protective measures.

"If you don't take precautions, you're just asking for a disaster to happen," VanWyk says. And, chillingly, "Given how easy it is to write even a simple computer virus like this one, I think we have seen only the tip of the iceberg . . . ."

The virus that infected disks at Lehigh was typical of simple viral code. About 300 bytes of assembler, it looked for the COMMAND.COM file present in DOS and attached itself to it. It was then spread by duplication of that disk, or insertion of that disk into a PC with a bootable hard disk. Later, the virus began its dirty work, erasing the disk.

Then Miami University was hit by another virus, BRAIN. Joe Simpson, Assistant Manager of Academic Computing Services at Miami, had to deal simultaneously with BRAIN on the university's PCs and SCORES, yet another strain, on its Macintoshes.

"Once the epidemic was recognized, panic set in here," Simpson says. "A lot of people lost data to these viruses. We still don't feel we have a complete understanding of what happened at Miami."

If you boot a PC from a floppy disk containing BRAIN, the virus copies itself onto any disk for which you subsequently ask DOS to show a DIRectory. The strain that infected hundreds of disks at Miami University was relatively benign.

SCORES, the most widely distributed Macintosh virus, is much more pernicious. It looks for specific programming "signatures." It has appeared at many academic and business computing centers, from NASA to the huge Texas computer firm EDS (a subsidiary of General Motors).

At EDS, two dozen Macs were quickly infected with SCORES. The programs it was affecting were first developed at EDS; the company won't talk about those programs, saying only that they were "proprietary trade-secret programs." With a wealth of programming talent to call on, the company was able to stamp out the virus in a matter of days.

EDS won't be specific about what they're doing to prevent future infections, noting, "We

(continues on page 35)

Viruses

(continued from page 34)

have security and other measures in effect: we wouldn't want to go into those. One of the things we sell a customer is our ability to secure our customers' data, so we're very, very cautious with that."

Exactly. Which is why few businesses that have been attacked by viruses will even acknowledge the problem, let alone say how they countered it—or what they've done to protect against future infections.

Would you leave *your* money in a bank that had its computer system corrupted by outside software?

Moreover, no company wants to become, through foolish claims of invulnerability, The Big Test—the number-one target of those loosing these viruses on the world.

Harold Highland, Editor in Chief of *Computers & Security* magazine and a recognized expert, says it well: "My recommendation to a corporate entity would be to deny it immediately. I have advised industry that if anything like this happens, and you can kill it by denying it, kill it.

"Even the government agencies will deny it. If you go back to the invasion of NASA's physics space network, last September when they were penetrated by the Hamburg Chaos Club, and the club announced that they had planted viruses, the NASA director of data security admitted that there was a penetration and the planting of viruses.

"But within one week the story came back that, yes, there was a penetration, but there are no viruses. And since then it has been denied that there is a virus."

What to do?

One corporate answer has been to ban shareware, freeware, or other programs that have been downloaded from bulletin boards. That's the new company policy at a Fortune 50 multinational petroleum company. The company has had scores of reports of viral infections from PC-using employees, though it has not yet been able to confirm that viruses were, in fact, responsible for the incidents.

To forestall the threat, and to calm the nerves of skittish executives, the company issued a formal policy banning downloaded software.

In academic computing settings—long the target of such vandalism, though rarely so maliciously and destructively as we have seen this spring—that kind of ban won't stand up. So colleges and universities have been trying to get faculty and students to use write-protected floppy disks, and to install so-called "vaccine" programs. (See antivirus program reviews, page 36.)

Few individual PC owners will want to deny themselves the wealth of useful software available from bulletin boards, and while write-proofing your bootable floppies may be a good step, it's inconvenient and hardly a complete answer.

Common-sense measures, such as not loading new public-domain and shareware programs from unknown sources, certainly help. Most user-group disk librarians are now inoculating library disks against viral infections; if your group isn't on guard against viruses, find out why it isn't. And stop using library disks until you are satisfied that adequate security is in place.

Finally, you should consider one of the various vaccine programs. They can go a long way towards protecting your disks as well as your peace of mind. But none are complete answers, and none guarantee that you won't fall victim to the next round of cleverness in this escalating germ warfare.

Lehigh's Kenneth VanWyk again: "If you as a user recognize the vulnerabilities of the antivirus package you're using and don't rely on it 100 per cent, then there is certainly a place for these antivirus programs. The problem comes in when a user says, 'Oh, I'm running XYZ antivirus software—nothing can happen to me.'"

A sense of invulnerability can be a very dangerous thing these days in computing.

Finally, you should consider one of the various vaccine programs. They can go a long way towards protecting your disks as well as your peace of mind.

How Vaccine Programs Work

Virus programs replicate themselves. Run one and it will infect other programs on your system. Share one of those programs with friends and the virus will infect *their* systems.

If it did nothing else, a virus would still slow your work. Each infected file grows, sometimes repeatedly, so it loads slower. But most viruses include added malicious features. After they've infected your whole system, or on a given date, they may reformat your hard disk, corrupt data files, or simply cause constant small problems.

Antivirus programs attempt to foil viruses by keeping them out of your system, preventing them from replicating if they *do* get in, and blocking their malicious tricks. A good antivirus will also protect against "Trojan Horse" programs—these are like viruses without the ability to replicate. And it will protect you from *accidentally* damaging your data.

Antivirus programs work on many different levels. Some common techniques include the following.

KEEPING VIRUSES OUT

Approved Program List: Block any program not on the list. Naturally, this doesn't stop you from accidentally approving an infected program.

Known Virus Check: Scan all executable files for known viruses.

Suspicious Text Search: Display all text strings in a program. If you see "Arf, arf, GOTCHA!", don't run it!

Suspicious Code Search: Check for suspicious commands such as low-level disk writes.

Approved TSR List: Warn if any program not on the list attempts to terminate and stay resident.

PREVENTING REPLICATION

Write-Protection: Prevent writing to protected files. This should be more than merely setting the Read-Only flag.

Signature Check: Take a "signature" of all approved programs and compare the program with the signature.

Run-Time Signature Check: Whenever DOS loads a program, check it against the signature. Block it if it doesn't match.

BLOCKING MALICIOUS TRICKS

Disk Access Lockout: Allow access only through DOS file functions. This will prevent reformatting and erasure of the File Allocation Table.

FAT Copy: Save a copy of the File Allocation Table in case a virus manages to damage it. Various "unformat" programs already provide this protection.

CMOS Copy: Save a copy of the CMOS information just in case a virus does manage to damage it.

Hard Disk Lock: Temporarily block all access to the hard disk while testing suspect software. Easiest to do on AT-class machines.

—Neil J. Rubenking

Antivirus Programs Fight Data Loss

HANDS ON

BY NEIL J. RUBENKING

FLUSHOT PLUS

Antivirus programs are aggravating by nature because they can prevent you from doing perfectly normal tasks like formatting a floppy disk. *Flushot Plus*, from Software Concepts Design, provides flexibility to offset the annoyance. You can tell it to allow low-level disk access *only* until the end of the next program. That will let you run FORMAT without interruption, for example. You can also turn its protection on and off easily.

Flushot Plus is shareware, but it has more features than many commercial programs. These include approved TSR list, write-protection, read-protection, signature check, runtime signature check, disk access lockout, FAT copy, and CMOS copy.

The FLUSHOT.DAT data table lists the types of files you want to write-protect or read-protect, along with any exceptions to the type. For example, you could write-protect all .COM files except those in the "DEVELOP" subdirectory. The table also lists your approved TSRs and any files you want signature-checked. You're advised to hide this data file under a different name to avoid "smart viruses" targeted to damage it.

VACCINE, VERSION 1.2

FoundationWare's *Vaccine* provides a six-part protection program:

1) Installation and Check-Up: Checks out your hard disk arrangement and adds useful commands to your AUTOEXEC.BAT and CONFIG.SYS files. Makes listed executable files read-only.

2) Boot-Time Quality Assurance: Signature check.

3) Runtime Quality Assurance: Runtime signature check.

4) Surveillance: Disk access lockout.

5) Bomb Shelter: Hard disk lock...

6) Critical Disk: FAT copy and CMOS copy. If a virus does damage your system, reboot with the Critical disk for no-hands restoration.

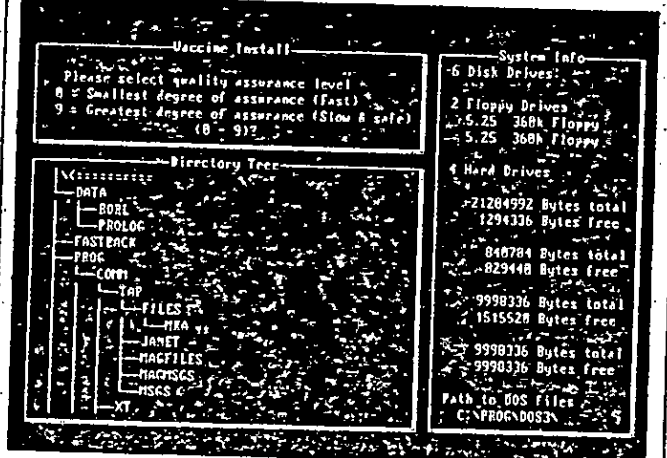
Vaccine protects all files with your chosen extensions. This is handy, since a virus could as well infect an overlay file as the main .COM or .EXE file. The Runtime module checks any file that DOS loads for execution, but only listed files get checked at boot-up.

No question, *Vaccine* will increase your boot-up time. The signature check can take several minutes, and every utility in your AUTOEXEC.BAT gets checked as it loads. Each time you add a new program you have to use the original *Vaccine* disk to approve it, and every handy utility you run will take a little longer. For a programmer it's even worse. Recompiling your program changes an executable file, which *Vaccine* flags as viruslike activity. *Vaccine* will be most useful to the millions of "office" PCs.

Indeed, FoundationWare has targeted the corporate market. With *Vaccine*, the system administrator can lock out non-approved programs. The program does require a system administrator—someone to take care of approving new programs, handling critical disks, and managing software updates. This vaccine is strict, but it will protect your system.

MACE VACCINE

Mace Vaccine, from Paul Mace Software, offers two levels of protection. At level 1, it gives write-protection to system files, the boot sector, and the partition table. It also guards against common tricks that disable the root directory. Protection level 2 adds disk access lockout. *Mace Vaccine* is best used with the *Mace Utilities*, which include a FAT copy and restore program. The program is simple and the documentation just one page, but for $20 you *do* get a degree of protection.



FoundationWare's Vaccine *checks all of your directories.*

VACCINE, VERSION 2.0

WorldWide Data's *Vaccine* consists of three programs:

ANTIDOTE—Known virus check.

CHECKUP—Signature check.

VACCINE—Approved TSR list and disk access lockout.

ANTIDOTE is fast and clean. In just a few minutes it scanned over 300 executable files on my system and flagged 10 simulated infected programs. WorldWide Data will provide "booster shots"—updates to ANTIDOTE that handle any newly discovered viruses. CHECKUP takes more time checking its signature file. Both programs check only .COM and .EXE files, so viruses that target overlays or other executable files will get past this version.

The WorldWide Data *Vaccine* programs are unobtrusive. They only scan for known viruses or checks your signature file when you ask. The manual is short, but the programs are simple enough to operate. Used systematically, they should protect against any virus that attacks .COM or .EXE files. If a virus or Trojan Horse does invade your system, they will at least prevent it from trashing your hard disk.

List Price: *Flushot Plus*, Version 1.2, Shareware registration, $10. **Requires:** 10K RAM (RAM-resident size); IBM PC, XT, AT, AT386, or PS/2, or 100-percent compatible; DOS 2.0 or later. Not copy protected. Software Concepts Design, Ross M. Greenberg, 594 Third Ave., New York, NY 10016; (212) 889-6438 (electronic BBS).

CIRCLE 445 ON READER SERVICE CARD

List Price: *Vaccine*, Version 1.2, $189. **Requires:** Minimum 384K RAM (RAM-resident size 1K); one hard and one floppy disk drive; IBM PC, XT, AT, AT386, or PS/2, or 100-percent compatible; DOS 2.1 or later. Not copy protected. FoundationWare, 2135 Renrock Rd., Cleveland, OH 44118; (800) PC-CURES; (216) 932-7717.

CIRCLE 446 ON READER SERVICE CARD

List Price: *Mace Vaccine*, $20. **Requires:** 4K RAM (RAM-resident size); hard disk; IBM PC, XT, AT, AT386, or PS/2, or 100-percent compatible; DOS 2.1 through 3.31. Not copy protected. Paul Mace Software, 400 Williamson Way, Ashland, OR 97520; (800) 523-0258.

CIRCLE 447 ON READER SERVICE CARD

List Price: *Vaccine*, Version 2.0, $79.95 **Requires:** 4K RAM (RAM-resident size); IBM PC, XT, AT, AT386, or PS/2, or 100-percent compatible; DOS 2.0 or later. Not copy protected. WorldWide Data, 17 Battery Pl., New York, NY 10004; (800) 643-3000, ext. 123; (212) 422-4100.

CIRCLE 448 ON READER SERVICE CARD