IN-61
43058
P13

Stopping Computer Crimes

Peter J. Denning

28 Nov 89

RIACS Technical Report TR-89.47

NASA Cooperative Agreement Number NCC 2-387

Research Institute for Advanced Computer Science
An Institute of the Universities Space Research Association

Stopping Computer Crimes

Peter J. Denning

Research Institute for Advanced Computer Science
NASA Ames Research Center

RIACS Technical Report TR-89.47
28 Nov 89

Two new books about intrusions and viruses remind us that attacks against our computers on networks are the actions of human beings. Cliff Stoll's book about the wily hacker who spent a year beginning August 1986 attempting to use the Lawrence Berkeley Computer as a stepping-stone for access to military secrets is a spy thriller that illustrates the weaknesses of our password systems and the difficulties in compiling evidence against a hacker engaged in espionage. Pamela Kane's book about viruses that attack IBM PC computers shows that viruses are the modern version of the old problem of Trojan horse attack. It discusses the most famous viruses and their countermeasures, and it comes with a floppy disk of utility programs that will disinfect your PC and thwart future attack.

This is a preprint of the column *The Science of Computing* for
American Scientist 78, No. 1 (January-February 1990).

Work reported herein was supported in part by Cooperative Agreement NCC 2-387
between the National Aeronautics and Space Administration (NASA)
and the Universities Space Research Association (USRA).

Stopping Computer Crimes

Peter J. Denning

Research Institute for Advanced Computer Science

28 Nov 89

It was early Friday October 13, 1989, in Baltimore. My taxi driver and I got into a discussion of the misfortunes that might befall the world that day. I asked him if he'd seen the newspaper headlines about the computer viruses that might strike that day.

"Yeah, I've seen those headlines. What the heck is a computer virus anyway?" he asked.

"It's a program that gets into your personal computer when you don't expect it, and then it does something nasty like wiping out your files," I responded.

"But how can a computer catch a virus? Does somebody sneeze on it?" he asked, almost snickering.

"These aren't the usual viruses that you catch by contact with someone else," I said. "They spread when you take a floppy disk from an infected computer and insert it into an uninfected one. They can also spread over the telephone network -- computers dial each other up all the time these days, you know."

"You mean those things aren't germs? They're created intentionally by people?" he asked in a troubled tone.

"Exactly," I replied.

"Why would anyone do that?" he exclaimed.

Why would anyone do that? This is one of the most important questions that we face as we enter the twenty-first century, a crowded world that will be linked tightly by networks of computers, a world that cannot work without the cooperation of many people. Our world already contains people who will steal information from computers attached to a network, people who will settle a grudge by attacking someone's computers, and an expanding culture of young people who fancy themselves explorers of vast electronic hinterlands that beckon to the adventurous. Primed by the ideas of modern science fiction novels like William Gibson's *Neuromancer*, these self- styled "cyberpunks" view computer networks as the new frontier of individuality, a hidden universe through which their disembodied presences can roam forever.

Network intruders -- some would call themselves explorers or liberators -- have found ways of using networks to dial into remote computers, browse through their contents, and work their way into other computers. They have become skilled at cracking the password protocols that guard computers and adept at tricking the operating systems into giving them superuser or system manager privileges. They have also created programs called worms and viruses that carry out these actions unattended and replicate themselves endlessly -- electronic surrogates that can prowl the network independent of their creators. We can expect steady increases in acts of crime, espionage, vandalism, and political terrorism by computer in the years ahead.

The phenomenon of widespread electronic intrusion is very recent. It is made possible by the proliferation of personal computers and their connection to electronic networks. Although technically sophisticated, intrusions are always the acts of human beings. They occur against the background of a modern discourse that values individual rights more highly than compromise and anonymity more than accountability. They can be controlled by a combination of technical safeguards -- a sort of network immune system -- and hygienic procedures for using computers. But they cannot be eliminated.

Newspapers tell tales of growing public concern about the integrity and privacy of information stored in computers. As electronic networking spreads around the globe, making possible new international interactions and breaching barriers of language and time, so rise the risks of damage to valuable information and the anxiety over attacks by intruders, worms, and viruses. These concerns actually run much deeper than simple protection of information. In a world of global markets, people are forming new communities supported by networks of computers. Intrusions undermine the trust that binds a community together and threaten its very existence: intruders challenge the way we work together in a networked world.

The growing world network shares many characteristics with biological organisms, especially an astronomical number of connections among a large number of simple components. The overall system can exhibit behaviors that cannot be seen in an analysis of its separate components. Like their biological counterparts, computer networks can suffer disorders from small organisms that create local malfunctions; in large numbers, these organisms can produce network-wide disorder. For this reason, the attacks against networks of computers have biological analogies, and two of them, worms and viruses,

are designated by explicit biological terminology *(1)*.

The distinction between a virus and a worm is fine. Both are forms of automated intrusion. Both propagate copies of themselves to other systems. Both are capable of damage and may delay inflicting it until long after the infection. The main difference is that a virus attempts to hide copies of itself inside other, legitimate programs, whereas a worm appears as a separate program -- but worms can disguise themselves, as did the Internet worm of 1988 *(2)*. You may hear the terms used interchangeably in the trade and even the in professional press. No matter: they are virtually indistinguishable.

Security experts refer to the programs left behind by intruders, worms, and viruses as logic bombs and Trojan horses. A logic bomb is a program that damages or discloses files after an appointed interval or at an appointed time; it can evade detection by waiting to perform its deeds many hours, weeks, or months after it has been implanted. Favorite dates include Fridays the thirteenth, April Fool's Day, and Halloween. A Trojan horse is a program that performs an apparently useful function but contains a hidden logic bomb. Its name recalls the legendary sneak attack by the Greek army at Troy.

Two recent books on this subject are worth making an effort to find. The first is Clifford Stoll's *The Cuckoo's Egg (3)*. Stoll writes with flair, wit, and disarming honesty in the style of a detective story. He refers to the Trojan horses left by the intruder he was tracking as "cuckoo's eggs," an allusion to the cuckoo's habit of tricking other birds into raising its young by laying its eggs in their nests.

A 75-cent discrepancy in the accounting records of the computer at the Lawrence Berkeley Laboratory (LBL) in August 1986 at drew Stoll into an investigation that revealed an account not created by the system administrator. With the support of his lab

director, Stoll embarked on a quest to identify the intruder and turn him over to the authorities. He quickly discovered that this intruder returned to the LBL system frequently, carefully covering his tracks to evade observation by system managers; for example, the intruder checked whether any system manager was logged in when he himself logged in; once in, he checked whether any of the files he had left behind to ease his return had been altered. Having satisifed himself that he was not being observed, the intruder set about trying to break into accounts on military computers attached to a portion of the Research Internet called the Milnet *(2,4)*. It should be noted that none of these computers contains classified information.

Stoll set up a monitoring system that tapped the incoming lines on the computer side of the modem, alerted him by phone beeper when the intruder logged in, and captured the intruder's every keystroke on a line printer -- all this invisible to the intruder. Stoll then began working with the technicians of the telephone company and of Tymnet, an international data network, to trace the incoming calls; he discovered that they were coming by a tortuous path from a Mitre Corporation computer in Virginia, across AT&T long lines to a Tymnet dialin port in Oakland, and then across Tymnet to the LBL computer. When Stoll reported his findings to system administrators at Mitre, they shut down their modems and broke the path.

In the final weeks of 1986, the intruder found another path over Tymnet to the LBL computer and resumed his explorations of the Milnet. Stoll and his Tymnet colleague traced the intruder's calls to a computer in West Germany. To lure the intruder into staying long enough for the German authorities to locate the originating phone, Stoll set up a sting operation by creating files documenting an imaginary project called SDINET,

a network supposedly connecting classified military computers doing SDI research. He even planted an electronic mail message from the system programmer saying, "I've concealed the SDI network port, and I doubt that many people will discover it." The intruder spent many hours beginning in January 1987 copying the files from this project and hunting for access to the SDI network -- hours that enabled Stoll and his helpers to trace the calls to Hannover, West Germany. In June of that year, the West German authorities arrested Markus Hess and charged him with international espionage and selling military secrets to the KGB. Hess was allied with members of the West German Computer Chaos Club, who were supplying pilfered information to the KGB in return for money and drugs. After nearly a year of suspense and intrigue, Stoll's "wily hacker" was caught.

None of this was easy. The FBI eschewed involvement because there was no actual compromise of national security and no loss of property. The CIA and NSA eventually got involved as observers when Stoll was able to prove that the intruder sought military information. Only after much cajoling of these agencies by Stoll and LBL officials were the search warrants needed to perform the tracing of phone calls issued. The legal actions against Hess and other members of the Chaos Club are still under way today.

The second book I am recommending is Pamela Kane's *V.I.R.U.S.: Vital Information Resources under Siege (5).* This book gives a history of computer viruses with special attention to their effects in the world of IBM PCs with the MS/DOS operating system. It is accompanied by a 5-1/4" floppy disk inside the back cover, which provides a suite of ten programs -- the "Dr. Panda Utilities" -- that the reader can install on his PC for viral detection, removal, and recovery. I have not tried these programs

myself and cannot endorse them here.

Kane recounts stories of Trojan horses, simple viruses, and break-ins from early computers to today, a reminder that the problem of securing our information resources from attack is quite old. Never letting us forget that human beings were responsible, Kane discusses some of their motives: embezzlement, espionage, extortion, fraud, hacking, piracy, revenge, and theft. She tells the stories of the first headline-winning PC viruses and worms. One of these was called the "(c) Brain" virus because it relabeled infected diskettes with this string. It originated in the Brain Computer Services store in Lahore, Pakistan, in 1986, purportedly as a way to get even with Americans who were using pirated copyright software. It apparently did no harm beyond reducing memory space by about 7K bytes. Variations of this virus still infect disks today. The Lehigh virus appeared on the campus of Lehigh University shortly before Thanksgiving 1987; it infected floppy disks in the same way as the (c) Brain virus but destroyed the directory of files on a disk after the fourth infection. Many students and faculty lost files to this virus. A worm appeared in the IBM BITNET network at Christmas-time 1987, displayed a Christmas message, and mailed copies of itself to others on the users' mailing lists; the clogged network had to be shut down to purge all copies. The most famous worm, released by a Cornell graduate student into the Research Internet on November 2, 1988, infected nearly 3,000 computers and caused widespread disruption (but no destruction) before it was stopped *(2)*.

Kane looks behind the scenes at the hacker culture to show readers the kind of thinking that guides the actions of those who break into computers. We learn that some hackers consider exploring the invisible parts of telephone and computer networks as fun,

a challenge to be undertaken in the face of risk. Others say they are doing society a favor by exploring the weaknesses of these systems and exposing them before a real criminal does serious harm. Still others say they are protecting society by revealing large corporate and government databases about individuals. Many engage in "phone phreaking," the act of using free telephone calls to gain access to remote computers. Once in, they mostly just look around, but sometimes they steal data and programs for distribution via bulletin boards.

The second half of Kane's book is a description of the means by which viruses operate and the ways the Dr. Panda Utilities can thwart them; it is written at a level that most PC users can understand. An appendix gives a complete security checklist for a PC. The most important safeguard: maintain adequate backups. Another appendix is a list of all viruses known in mid-1989 that attack PCs.

These books make it easy to see that some straightforward technological fixes would greatly reduce future threats. But technological fixes are not the answer; they are valid only until someone launches a kind of new attack. Changes in the ways we use computers, however, will reduce our exposure to our own and others' frailties *(4,6)*.

The books also remind us that worms and viruses are mere programs. They are not capable of intelligent action, as envisaged by another taxi driver who spoke to me late that same Friday: "You know, everyone thinks we got off light on those computer viruses that were supposed to attack today. Everyone thinks it was a hoax. But the viruses outwitted them. They got into the stock market computers. That's what caused the crash today. I know!"

References

1. P. J. Denning. 1988. Computer viruses. *American Scientist 76*, 3 (May-June). 236-238.

2. P. Denning. 1989. The internet worm. *American Scientist 77*, 2 (March-April). 126-128.

3. C. Stoll. 1989. *The Cuckoo's Egg*. Doubleday.

4. P. Denning. 1989. The ARPANET After Twenty Years. *American Scientist 77*, 6 (November-December). 530-534.

5. P. Kane. 1989. *V.I.R.U.S.: Vital Information Resources Under Siege*. Bantam Books.

6. P. Denning. 1989. Worldnet. *American Scientist 77*, 4 (September-October). 432-434.

hydra.riacs.edu:pjd

Ditroff

Fri Dec 15 09:32:42 1989

ps4 / LW N230-121 x6363

```
ps4 hydra.riacs.edu:pjd  Job: Ditroff  Date: Fri Dec 15 09:32:42 1989

ps4 hydra.riacs.edu:pjd  Job: Ditroff  Date: Fri Dec 15 09:32:42 1989

ps4 hydra.riacs.edu:pjd  Job: Ditroff  Date: Fri Dec 15 09:32:42 1989

ps4 hydra.riacs.edu:pjd  Job: Ditroff  Date: Fri Dec 15 09:32:42 1989
```