
HOSPITAL
BANK
Electronic Worm

A REPORTER AT LARGE

THE DOOMSDAY CLICK

How easily could a hacker bring the world to a standstill?

BY MICHAEL SPECTER

Like at least several hundred thousand other people around the world, I found a surprise waiting in my E-mail on February 12th. I was in Southern California, and when I turned on my laptop there was a promising message from my wife, who was in Rome. At first glance, nothing seemed amiss: the subject line was slightly mistyped, the body of the message said simply, "Hi Check This!," and all seemed well within the vaguely suspended rules of electronic grammar. A picture of the Russian tennis model Anna Kournikova appeared to be attached to the message. People may argue about her skills on the court, but as a cyberian pinup queen Ms. Kournikova enjoys an uncontested reign.

I opened the mail eagerly—but found no picture. Instead, an electronic worm ripped through my computer. Within thirty seconds, it had worked its way to the inner registry of my hard drive, headed toward my Microsoft Outlook address book, and discharged its viral load onto all eight hundred and forty-seven entries. As a final act, the worm slipped a signature—ONTHEFLY—into my Windows registry (and into every other copy of Windows that it infected), along with enigmatic instructions for the computer to connect itself automatically to a Dutch Web site every year on January 26th.

Because my family and I live in Europe, where this particularly hardy virus began to spread, and my wife's office computer is connected permanently to the Internet, she became a sort of digital Typhoid Mary. She unwittingly took out an entire cluster of computers at the Harvard Medical School, incapacitated laptops owned by the New York *Times*, and caused damage and confusion at film companies, publishing houses, and magazines, as well as among hundreds of acquaintances. The virus, it turned out, was created by a twenty-year-old Dutch student with a particular fondness for Ms. Kournikova, and although it cascaded through the Internet with unusual velocity, the outbreak was hardly unique. In 1999, Melissa quickly became the most widespread virus of its time, infecting more than a million computers. Then, last May, the Love Bug caused a pandemic in cyberspace, striking forty-five million computers in twenty countries and costing billions of dollars in damage.

Harassment by computer viruses has so far been regarded largely as a nuisance. It is rapidly becoming more serious, however, as the world's most critical institutions—banks, hospitals, and governments among them—place their clients' personal details online. The Net was never envisioned as a security vault, and as its importance has grown so have its weaknesses. The federally funded Computer Emergency Response Team, at Carnegie Mellon University, which follows electronic attacks more closely than any other organization does, reported about ten thousand cases of corporate hacking in the United States in 1999 and more than twenty thousand cases in 2000. Those are the ones that we know about; most companies would never speak publicly. As you read this, there are at least fifty thousand computer viruses crawling across the junglelike vines of the World Wide Web, and hundreds more are created each day.

American intelligence officials recently were startled to learn that hackers had broken into the Sandia National Laboratory, in New Mexico, and copied highly classified information from computers there. In the aftermath of the spy-plane collision over the South China Sea, Chi-

ILLUSTRATION BY GERALD SCARFE

"The Internet is waiting for its Chernobyl," one scientist says, "and I don't think we'll be waiting much longer; we are running too close to the edge."

nese hackers struck fiercely at American Web sites, leaving messages like "Hack the USA" and "For our pilot Wang," the latter referring to the fighter pilot who died. Before a truce was declared, early in May, this particular cyberwar had escalated considerably, with hundreds of Web defacements, including some at the White House, the F.B.I., and NASA. (To increase the intensity of the assault, which the F.B.I. said involved "millions" of attempts to break into American sites, the Chinese side assembled an exhaustive archive of the most esoteric hacking tools—at www.cnhonker.com. It remains available to anybody with Web access and Chinese-language skills.)

These are mostly games, of course, but they hint at something more profound: sophisticated terrorists (or hostile governments) now have the ability to crash satellite systems, to wage economic warfare by unplugging the Federal Reserve system from Wall Street, even to disrupt the movements of ships at sea. Electric power plants, water systems, and hospitals—and the thousands of computers that guide ambulances, police dispatch units, fire brigades, and transportation switches—are all becoming susceptible to potentially crippling attacks.

None of that ever bothered me. Not long ago, however, I decided to see for myself what it would take to cause harm on the Internet: to release a virus, crash a computer system, obliterate privacy, and destroy the data that we have come to rely on. I began slowly, by collecting viruses, worms, bugs, and other purely malicious pieces of software as if they were rare butterflies. (The definitions of these creatures vary, but a worm is a tiny program that can copy itself. A virus, although equally damaging, simply infects other programs.) I have two giant hard drives on my computer, and within weeks I had turned one of them into a laboratory for the most dangerous viruses on the Internet: the Melissa virus, Happy99.exe, the Love Bug, among others, are floating around cyberspace, and I have copies of all of them, carefully tucked away on disks, like tarantulas suspended in aspic, or the last archival strains of smallpox.

With help from far more practiced hands, I learned to watch the world's computer traffic glide through the phone lines, or burst in packets of microwave radiation between thousands of switches and servers. It didn't take long for me to see what computer-security experts have known for years: any fool can enter, alter, and destroy even the most seemingly impregnable Web sites. There are dozens of scanner programs on the Internet, which make it possible to stalk the Web for hidden weaknesses. They offer the digital equivalent of sneaking from house to house trying doorknobs to see if the doors are locked. And, if you know what you are doing, you can sit in Rome (or Baghdad, for that matter) and check a few hundred thousand American doorknobs an hour. It's not even against the law. You don't have to know how to write, or even understand, the code to wreck it. And, if you can't get into a site, you can always overwhelm a company simply by inundating it with E-mail messages from so many sources that its computers collapse under the weight of the traffic. The most insidious efforts are often silent: a smart hacker can infiltrate and plant "trapdoors" nearly anywhere, and then return undetected at any time.

"To do this stuff is utterly trivial," Peter G. Neumann, who is a principal scientist at SRI International, the technological consulting firm, told me. "Every other kid can do it, and we know that. That isn't what worries me." Neumann, who is sixty-eight, has worked at and advised many of the nation's most important universities and government institutions, from the Navy and Harvard to the highly secretive National Security Agency. Mostly as a hobby, he moderates a forum on the Internet and produces a running list called "Illustrative Risks to the Public in the Use of Computer Systems and Related Technologies," which is the most frightening collection of random dangers I have ever seen. "What worries me is the big one," Neumann said, as we sat in his office in Menlo Park, California, one day. "People don't like to talk about this, because it's seen as encouraging the enemy, but absolutely everything is riddled with security flaws. Hackers can get into our most important systems in minutes, sometimes in seconds.

"And they do," he added. "The Internet is waiting for its Chernobyl, and I don't think we will be waiting much longer; we are running too close to the edge. When a third of the computer drives in America are wiped out in a single day, when the banking and commerce system is overcome, or the power grids and emergency-response systems of twenty states shut down because of a malicious computer attack, maybe then people will think about what's going on here."

The word "hacker" long ago lost its Yiddish meaning, as a person so inept at making furniture that he might as well do it with an axe. In the late nineteen-sixties and early seventies, it came to signify another sort of person: someone particularly skilled at computer programming, and so delighted to do it that the enterprise became an end in itself. Hackers were noble geeks; they came out only at night, could get into nearly any network, disturb nothing, leave no fingerprints, and move on. It was an important part of their ethic that hackers should do no harm.

That changed on November 2, 1988, when a graduate student at Cornell named Robert Tappan Morris unwittingly carried out the hack heard round the world, letting slip a worm that shut down ten per cent of all the computers on what would soon be called the Internet. Morris, who today teaches at M.I.T. and whose father was a senior computer-security official at the National Security Agency, had the dubious honor to be among the first Americans convicted under the Computer Fraud and Abuse Act. He has always said that he meant no harm, and the evidence supports him. Nonetheless, Morris's mistake not only infected thousands of networks but completely altered the public view of hackers. Computer people will tell you that the proper term for a person who disturbs the peace of the online universe is "cracker"; but nobody uses it. In the minds of the public, hackers are bad guys.

"You don't hack for harm—you hack for honor," Gerrie Mansur was telling me as we stood in the center of Amsterdam one evening last month, at sunset, watching boatloads of tourists inch their way toward the flower market on the Amstel River. I had gone there, in part, to speak with the man who set loose the Kournikova virus, but also to learn how easy it really would be to spread mischief on the Internet. Gerrie promised to show me. He and his pals Viper and Dimitri collected me at my hotel in a new Volkswagen Lupo that the Internet firm Viper works for had just bought for him. Viper is twenty-one and Dimitri is nineteen,

and they consider Gerrie, who is twenty-six, their mentor. Gerrie and Viper live near each other in Haarlem, the provincial capital, north of Amsterdam, and they both wore the iconic hacker uniform: jeans, black leather jacket, Gap-style big T-shirt, and the odd, clunky shoes that have become the signature of a certain type of cool urban male. Dimitri lives in Delft, which is more than an hour away, but, since all three exist mainly online, distance doesn't play a large role in their lives.

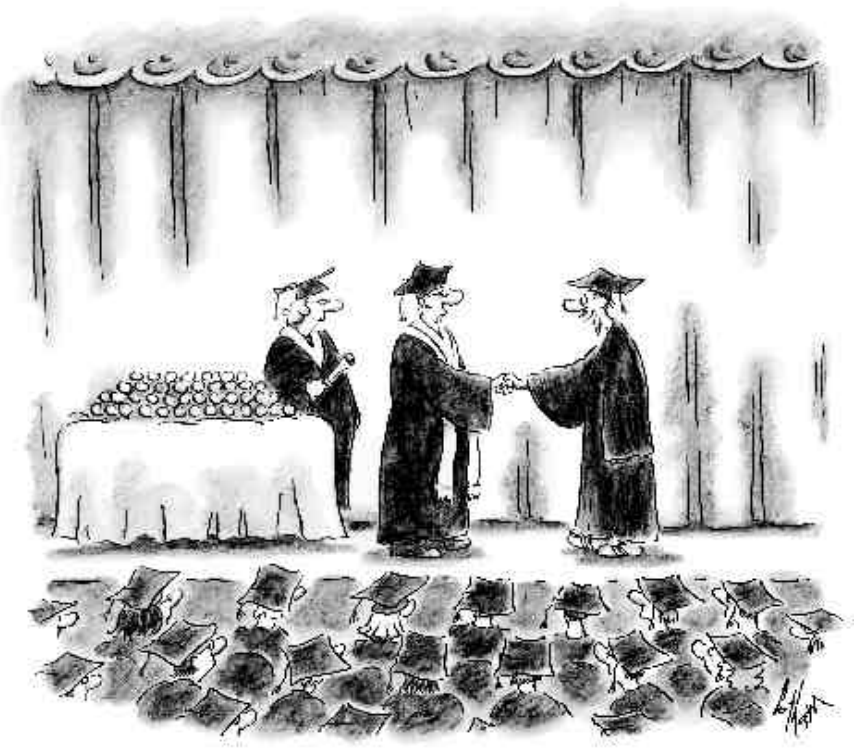
Dimitri—his full name is Dimitri Van de Glessen—is a soft-spoken and spindly young man who is all bones, green eyes, spiky red-brown hair, and acne. He made international headlines a few months ago when he hacked the Microsoft corporate servers. He is still angry about the publicity, though, because he feels that he didn't get proper credit. First, he simply broke into one of the main event servers, which are essentially electronic billboards, and added a text file with the words "Hack the planet." Microsoft failed to respond, and Dimitri took that personally. So he went back in, got hold of a password with more significant access to data, and put up an entirely new page on the site that read, "Patching your system is very hard, huh?" He then forwarded the page to journalists, along with the information that he was able to break in through a weakness that Microsoft could have fixed had it bothered to use its own software. That got the company's attention, and in the end Dimitri met with some Microsoft employees, showed them their problem, and all was forgotten. (At least, until his bosses in the Netherlands found out; once his private activities became public, Dimitri was out of a job.)

He didn't seem to mind. He quit school a while ago, and he makes some money doing security for, among other places, a chain of Dutch night clubs. Since he lives with his parents, his cash needs are minimal. Dimitri would be an obvious casting choice for "Revenge of the Nerds"; his home page shows him at a disco hovering triumphantly between two women both of whom are wearing halter tops and big smiles. He looks very much like a young man who has just won the lottery.

Viper (a cyberspace nom de hack, but the only name he would permit me to print) is more seasoned than Dimitri. Until the week I came to town, his best-known hack was the Beienkorf mall, one of the biggest shopping centers in the Netherlands. "There were sixty thousand open credit cards just sitting there—every piece of information you could possibly want," Viper told me. "I sent the whole database to Gerrie." Gerrie often functions as an information broker in that hazy space between hackers and the hacked. "It was on TV, and one day later that server was secure." Like a lot of hackers, Viper thinks of himself as a kind of Robin Hood, who breaks the law only to sound the alarm. But he also views vulnerable Web sites, particularly those of big corporations, the way a mischievous teen-ager might see an empty convertible with the keys in the ignition.

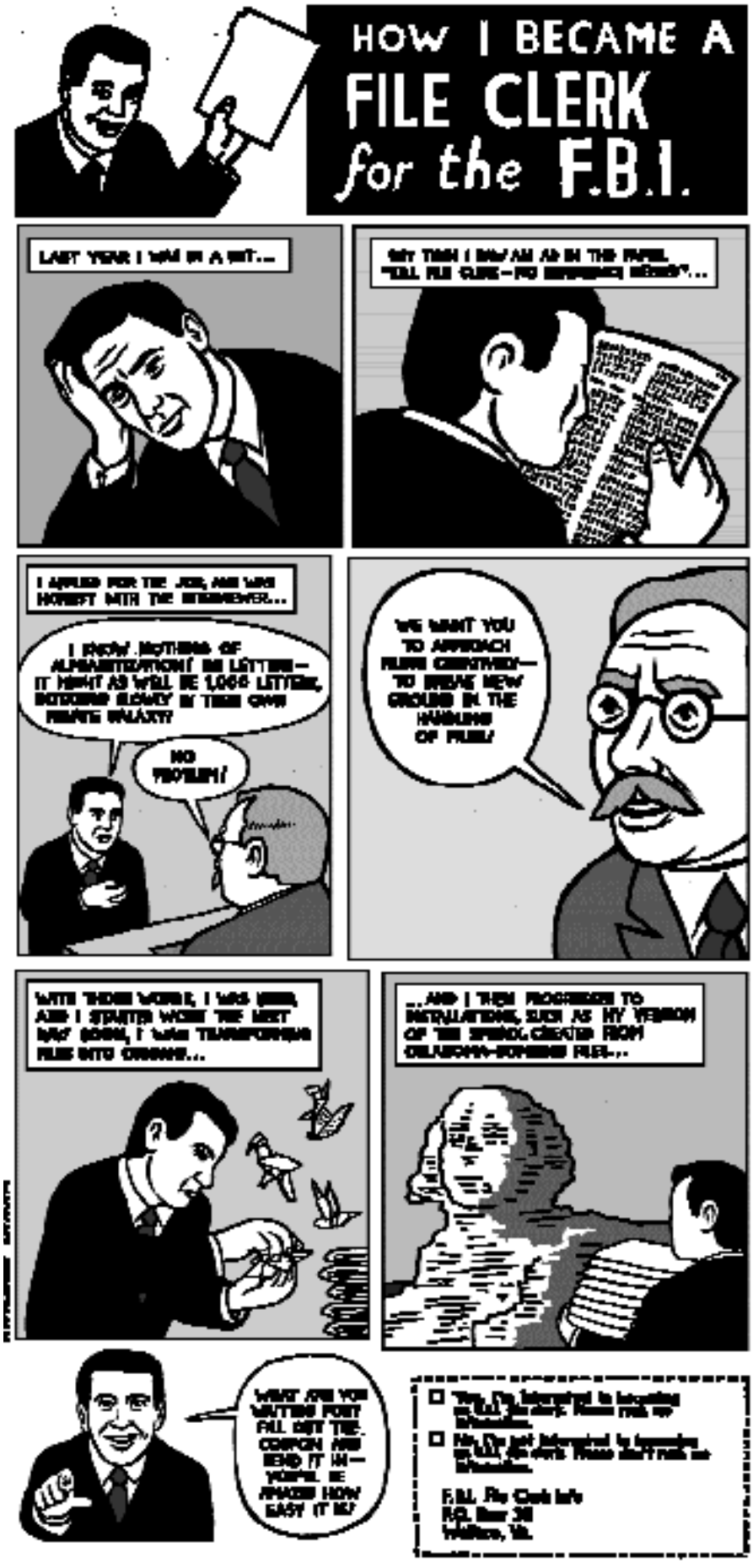
A few days before I arrived in Amsterdam, Viper had scored his biggest hack yet. "I was just sniffing around the Web when I saw it," he told me. (In cyberspace, "sniffing" is a technical term. It's how people learn whether a site can be hacked. Think of it as a surveillance flight over enemy territory. There is also anti-sniffing. That's how people listen for the people who are listening; it's a bit like radar.) In April, Viper sniffed out some surprising weaknesses at the corporate servers of Real Networks, the giant Seattle company that streams audio and video services over the Internet to millions of customers. "I went over to real.com and it was absolutely, completely naked," Viper told me, after E-mailing me a file that he said would allow me to enter and alter many programs in the company's customer-service directory. It is one of the peculiarities of theft in cyberspace that you can steal a copy of a file without tipping anyone off or having to disturb the file itself. "Every person—name, phone number, address. Anything those idiots at real.com thought was worth having I have," Viper said. "E-mail. Real-world addresses. It wasn't even encrypted." (Two weeks later, from an anonymous Web site, Viper mailed real.com details of its problem. He also told me that he had deleted the five-gigabyte database from his hard drive.)

Gerrie's biggest claim to hacker glory came last October, when he crashed into the global server for Nasdaq, which holds passwords to the main stock-exchange database. He told me that he was doing a security scan for a client when he stumbled upon a potentially devastating weakness in the computer code. Technicians said at the time that Gerrie must have



"To what do I owe this honor?"

• •



slipped in through a hole known as the Source Fragment Disclosure Vulnerability. Gerrie told me that they were mistaken: "It was clean. No footprints." Speaking like a chess player, he said, "I took the system in two moves." Gerrie, who is not averse to publicity, informed officials of Nasdaq and made public the problems, which have since been patched. (Hackers, by the way, love patches, because they often fail. "It's always the weakest spot," Viper told me, "just like on a tire.")

I had agreed to accompany the three to dinner, and then to go on to an Internet café where I could watch them "work." They debated for a while, and eventually chose Burger King over McDonald's. Earlier that day, Gerrie told me that he would bring Dimitri, because he was a "Microsoft hacker"; I had foolishly assumed that meant that Dimitri was somebody who hacked *for* Microsoft. "Why would I ever do anything for them?" he practically shrieked, while lingering over his second Whopper. "They will tell you that their software is safe to use, and they say that Linux"—a free open-source operating system that is an increasingly popular alternative to Windows—"is only for hobbyists. That's the most dishonest and arrogant thing in the world. So I want to let people know something: if you use Microsoft products, I can take you down. And so can anyone with a brain."

This refrain is as old as Microsoft itself, and I had heard it from people far more prominent than Dimitri. There is always a compromise between convenience and security, and, in trying to make products like Windows, Word, and Outlook attractive to as many people as possible, Microsoft, like most companies, has chosen convenience. But more features mean more lines of computer code, and thus more risk. (Windows 3.1, which was released in 1992, consisted of three million lines. Windows 2000 has about forty-two million lines. Security experts say that any program with one bug in ten thousand lines is unusually well written. If that is true, Windows 2000 would still have roughly forty-two hundred bugs.)

At dinner, the three told me how offended they were when they learned that the man who released the Kournikova virus was Dutch. They considered it clumsy, graceless, and rude. They were amazed

when I admitted that I had wanted to meet him. It turns out that the young man, whose sign-on was ONTHEFLY but whose name is protected under Dutch privacy laws, was a "skriptkiddy," somebody who makes a virus by following a recipe from a kit. It is like making brownies from a mix, but requires even less skill.

Skriptkiddies are all over the Internet, and there is an astounding variety of tools like the one used to create the Kournikova virus; in my collection, for instance, I have the Mass Destruction Library, the China Town Macro Word Virus, the Spamicidal Trojan Batch Creator, and Nuke's Randomic Life Generator, among others. For one-stop shopping, nothing quite beats the Hack Attack Web site. There you can find nukers, sniffers, spoofers, flooders, and all sorts of mail bombs, viruses, and other programs that do nothing but harm. The VBS Worm Generator, which was used to make Kournikova—and was written by an Argentine who goes by the name of K—has been downloaded more than fifteen thousand times from just one popular site, VX Heavens, according to that site's administrator. Yet, only days after the outbreak, the mayor of Sneek, the small town where the Dutch hacker lives, said publicly that anyone smart enough to whip up pandemonium on that scale must be smart enough to deserve a job. "Can you believe that asshole?" Viper asked as we headed out the door of Burger King. "That's the level of talent we are dealing with here. A five-year-old can do what he did."

We wandered over to the Freeworld Internet Café, which bills itself as the oldest of the many Internet cafés in Amsterdam. A gust of marijuana smoke rolled past as we swung open the door. Inside, there was loud house-rock music and a few middle-aged hippies rolling joints (which are for sale in any Amsterdam coffee shop). The patrons were in the middle of an animated discussion about the distinctions between locally grown hydroponic weed and imports from Thailand. We rented time on three computers and sat in a semicircle, with me as a spectator in the middle. Gerrie refused to break the law, but the others had no such qualms. (With my permission, however, he did hack into my personal Web site—www.michaelspecter.com. That took him all of thirty seconds.)

As soon as they were seated, the three began to scour the Internet, probing for weaknesses. Effortlessly, they lifted passwords from local Internet-service providers, downloaded software that helped them scan portals into important Web sites, and began, almost randomly, to click their way from San Francisco to Seoul. Along the way, they stopped off at major corporations, universities, and official government Web sites.

After demonstrating how he could alter my Web pages and delete, rewrite, or edit what I had posted there, Gerrie (again at my request) starting sniffing out the *New Yorker* site. He used, among other tools, Netcraft, which is a Web site that helps companies make quick assessments of blatant vulnerabilities. Like all such software, it is intended for defensive purposes but can also be used to attack. (The best program, Nessus, can even be found on government Web sites. I got my copy from NASA. It's a defensive scanning program, but hackers use it every day.) "It would take about four minutes to bring this down," Gerrie told me, after a cursory examination of newyorker.com. "Maybe less." Gerrie doesn't normally use big scanner programs like Nessus. To him they are like training wheels—and are also easy to detect. He prefers to look at the code himself, line by line, doing what is called a hand scan. "Any systems person with a brain will see a big scanner coming," he said. "It's like turning on the radar. You can't miss it. If you want to leave no footprints, you have to be sneaky. A hand scan is still the best scan." He sat back and ordered a rum-and-tonic.

Dimitri suddenly yelped. "I have root on the L.A.P.D.!" he shouted, before remembering that he was in a public café and was breaking the law. He had gained access to the fundamental data used by the Los Angeles Police Department. (The Web sites of the New York and Los Angeles Police Departments are favorite targets of foreign hackers who watch a lot of American television.) A savvy organization will segregate its public Web site from any internal system that holds sensitive data. But here, too, one must trade safety for convenience. Online databases have changed the business world. Not only can customers follow their FedEx packages as they travel across the world; people have come to expect the route to be available at all times. That kind of access has also been of great aid to law-enforcement agencies. Yet, if a police officer can sit in his cruiser and examine a person's arrest history on a city or a federal database, it's a good bet that other people can do it, too.

Dimitri worked quickly, pilfering a unique address (each computer, when connected to the Internet, has one, like a license plate) and then arranging it so that anyone who traced him would think he was in France. This complicated maneuver is called "laundering the connection." Soon he had defiled the home page of the L.A.P.D. and posted the altered page in its place. That's a felony in America, but although the Netherlands has similar laws, nobody has ever been sent to jail there for hacking. After a few minutes, Dimitri restored the police page to its original condition.

Viper was busy at the next computer, crashing into one of the largest Internet-service providers in the Netherlands. "Yo!" Gerrie said loudly, with delight. "You got their jewels." I watched as hundreds of names scrolled by, along with credit-card information and data about spending behavior. How hard, I wondered, would it have been to get this information if the passwords had been protected? That produced a collective laugh. "I'll show you," Viper said, and after poking around Asia for a few minutes we ended up at the Web site of Kookmin University, in South Korea, a highly regarded institution with a solid technical reputation. "There are two thousand passwords in this file," he said, after a few more minutes of rooting around in the university directories. "And they are all encrypted."

Cheap and widely available encryption was supposed to guarantee privacy for normal users, and it certainly does help. Yet what is true in the physical world remains evident here, too: throw enough brute force at any lock and you will crack it. (In this case, the force would be a computer program that simply worked through millions of possible password combinations.) Viper got hold of two fairly simple decryption programs called LophtCrack and Nutcracker. LophtCrack was written by a crew of "white hat" hackers, with roots at M.I.T., who called themselves Lopht Heavy Industries. The Lopht people astonished Capitol Hill a couple of years ago by stating at a hearing that it would be dangerous to use the Internet for any vital service like air-traffic

control. They also claimed that they could bring down the whole network in less than an hour. Nobody seemed to doubt them. In one well-publicized success, not long after that, Lopht identified a flaw in Windows that made it possible to decode an entire registry of user passwords in twenty-six hours. It was a task that Microsoft had claimed would take more than five thousand years of constant labor.

To decrypt Kookmin University's passwords, Viper used Nutcracker, and while he bounded across the Internet the program crunched away in the background. Fifteen minutes and six seconds later, the results were in: Nutcracker had opened thirty-nine of the roughly two thousand passwords on its first pass. It was embarrassing to look at them, because so many students, even at a university that focusses much attention on computers and technology, had obviously never given a thought to data security. The passwords were obvious: 1234, abcde, abc123, mom123. Many people say they don't really care about passwords, because, hey, who is going to steal my recipe for lemon-meringue pie? Fifteen years ago, when a desktop computer functioned mostly as a typewriter, that was a valid argument. The connected world has made such sentiments naïve, however; if just one employee at a large company dials into the network and uses a weak password (such as the word "password" itself, which is among the most common), any precaution taken by others will mean nothing.

My head was starting to spin, but Gerrie wasn't done with me yet. "You wanted to see how that Kournikova virus works," he said. "Why don't you sit here?" I moved over so I could type, and he took us to a collection of viruses, worms, and Trojan horses. Quickly, he downloaded the kit used by the student who made Kournikova and set it up on the machine. "What do you want to call it?" he asked. Before I could answer, he typed in newyorker.com. "Let's see how hard it is to flood the world with the newyorker.com virus," he said, smiling a bit more than I would have liked. I clicked on a file and a nice graphical form popped out. After that, I had only to follow the dots. When did I want to release the virus? was the first question. I typed a date. Next, it asked what I wanted on the subject line of the message that would be sent. I typed the words "Lance Armstrong." Then it asked whether I wanted to send the virus as an attachment to an E-mail message or as a Web page. Did I want to infect chat rooms? And what about encryption? (The Kournikova virus was encrypted, and this made it harder for standard antivirus software to sniff it out.) There was one final question on the form. Erase hard disk? I stared at Gerrie. "All you have to do is check it," he explained, "and it will erase the disk instead of copying the entries." I checked it. "Congratulations." Gerrie smiled. "You have just created a virus that will erase the hard drive of anyone dumb enough to open it. Maybe the mayor of Sneek will give you a job, too."

That evening in the Freeworld Café changed my view of the Internet. I still use it to buy merchandise (as I continue to hand my credit cards over to people I have never met), but the battle between hackers and everyone else has begun to seem like an arms race that the bad guys are destined to win. Nonetheless, there has been promising research, particularly in designing software that functions like the human immune system. The immune system recognizes things that don't belong in our bodies, and it does a remarkable job of repelling intruders. Several researchers, most notably Stephanie Forrest and Steven Hofmeyr, at the University of New Mexico, are developing highly sophisticated software to do just that for computer networks. They have had some impressive preliminary success, but even Hofmeyr says that such software will never completely deter committed criminals. (After all, viruses can overcome even the healthiest of immune systems.) Some security experts argue that too much reliance on technical solutions might even create a Maginot Line mentality, lulling people into the belief that their computers are safe.

"Computer security is a forty-year-old discipline," Bruce Schneier told me not long ago. Schneier created two of the most heavily used encryption algorithms, and his recent book on digital security, "Secrets & Lies," is perhaps the best popular exploration of the subject. "Every year, there is new research, new technology, and new products," he said. "Really good research, really good technology, and really good products. Yet every year the situation gets worse. Much worse. The Internet is just too complex to secure."

So Schneier decided to stop trying. Instead, he started Counterpane Internet Security, which relies on the skills of humans, flawed and inconsistent as they are, to manage the risks. Counterpane installs a special warning box—a Sentry—in every computer network it monitors. The sentries funnel information to a central knowledge base that keeps track of each client's idiosyncrasies. "We are like a fire brigade," Schneier told me. "Or an emergency room. In the real world, this kind of expertise is always farmed out."

When I described the ease with which my hacker companions in Amsterdam had rampaged through the Web—and my certainty that far worse went on each day—he laughed. "Does that surprise you?" he asked. "Yes, somebody can destroy the Internet in about half an hour. I know maybe a hundred people who could do it. But people can destroy the physical world, too. Can you walk into a hardware store and say, 'Please sell me a device that prevents murder'? Society has done pretty well in preventing murder, however, even though there is no absolute or technological solution for that, or for shoplifting or mugging.

"When you buy a safe, it comes with a rating," he went on. "It's a code: 30TL—thirty minutes, tools. 60TRTL—sixty minutes, torch and tools. What this means is that a professional safecracker, with safecracking tools and an oxyacetylene torch, will break open the safe in an hour. If an alarm doesn't sound and guards don't come running within that hour, the safe is worthless. The safe buys you time; but you have to spend it wisely." Schneier argues that the global reach of the Internet makes alarms and guards even more valuable in cyberspace than on terra firma. "One of the problems with the Internet is that we are living in a society of warlords. If laws matter in America, maybe they don't in Amsterdam or North Korea or Belgrade. We have been doing security for two thousand years, and the best stuff we have come up with is alarms and guards."

The first thing that struck me as I walked through the door of the company's Secure Operations Center, in Mountain View, California (there is an identical facility in northern Virginia), was the Buck Rogers decoder rings my escorts needed to get back into the se-

cure part of the building. You must also pass through a biometric screen that examines the precise geometry of your hand. All Counterpane's critical systems are redundant; the company operates its own power generator, and the data it stores are mirrored at its center in northern Virginia. Counterpane technicians sit inside a featureless gray building that looks like a slightly more modern version of a Strategic Air Command control room. When something worrisome pops up, a machine sounds an ominous *bing*, after which it's not that hard to imagine the country moving rapidly to Defcon 3.

We spoke in a conference room, eating sandwiches, while I learned the rationale that a monitoring service uses to attract customers (many of whom pay twelve thousand dollars or more each month for this digital protection). "Most companies of any reasonable size will get some sort of serious intrusion about once a year," Elizabeth Zwicky, who is Counterpane's director of information technology, told me. "But it depends who they are: real estate in cyberspace has neighborhoods, and they vary just as they do everywhere else. There are places you could leave your keys in the car and places where you would want bars on the windows."

After a while, she stopped talking, stared at the darkened conference-room window, and said, "We are about to go transparent." Somebody flicked a light switch, and it was as if a television screen had been transformed into a giant picture window. The control room lay before us, along with three analysts, a set of computers, and several large screens filled with lights flashing to register potential problems faced by clients. A stream of incomprehensible data ran across one screen, and, although the comparison has been made before, it was hard to look at that flood of lights and not shout, as I did, "There really is a Matrix!"

I had asked Schneier if there was a logic to the problems the company encountered. "God, no," he replied. "What we find just proves that the Net can never be secure." Not long ago, for instance, a company that Counterpane was monitoring suddenly appeared to have an enormous new computer network. It turned out that one of the employees was working from home. The man's wife worked for another major corporation, and they had set up a home network to link the family computers. "When this guy dialled into the office, he was linked to his wife, and she was linked to her company," Schneier said. "So they were all linked together. We fixed it, but it's a reminder. There is just too much out there—you can't protect it all."

I never did meet the man who released the Kournikova virus (and whose notoriety was unearned). But I did write to K, who also goes by the name Kalamar, and lives in Argentina, where he maintains a Web site devoted to viruses, worms, and other malicious code. Police say he is the man who created the kit that was used to make the Kournikova virus (and others).

"I'm not talking anymore," K wrote in response to my first E-mail. "Too much trouble." I sent him another, asking why he thought it was acceptable to write viruses. Most people, when asked that question, say it's for research, which is never true. Or they say that they didn't mean it or that the whole thing went too far. Not K.

"I have had some problems and I don't want to make this bigger, so I'll just stay out of the scene for a while," he wrote back. "But if you are so concerned about the safety of the Internet, why don't you talk to the people who make it dangerous? And that's not me. I don't write software, I am just showing you how bad it all is. People think this stuff is all free and easy. It's not free at all. Eventually people will realize that."

I don't play with my worms or viruses anymore—nor do I recommend it. When I was in Amsterdam, I asked Gerrie to send me a copy of the virus that we had created at the café, the one that destroys your hard drive if you open it. I wanted to be sure that it was real, and when I saw it, alive, on my laptop I deleted it and promptly forgot about it. I use the portable only when I'm travelling, though, and as soon as I got home I absent-mindedly began to make my way through the E-mail that had gathered on my main computer. Before I knew it, I had clicked on an extra copy of the newyorker.com virus, which did its job as advertised. If you have never tried this, don't. It's amazing how rapidly everything you've saved can disappear from your hard drive forever. ♦

"Hi. My name is Barry, and I check my E-mail two to three hundred times a day."