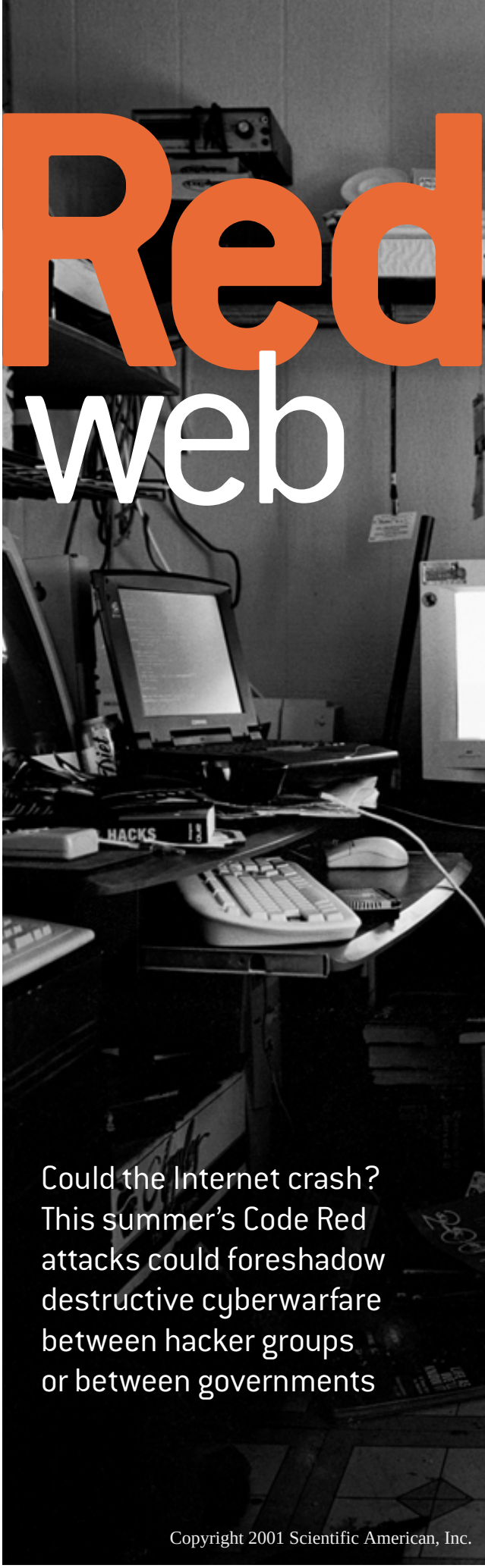
Code Red for the web



Could the Internet crash? This summer's Code Red attacks could foreshadow destructive cyberwarfare between hacker groups or between governments

"Imagine a cold that kills. It spreads rapidly and indiscriminately through droplets in the air, and you think you're absolutely healthy until you begin to sneeze. Your only protection is complete, impossible isolation."

Jane Jorgensen, principal scientist at Information Extraction & Transport in Arlington, Va., which researches Internet epidemiology for the Defense Advanced Research Projects Agency, isn't describing the latest flu outbreak but an affliction that affects the Web. One such computer disease emerged this past July and August, and it has computer security researchers more worried about the integrity of the Internet than ever before. The consternation was caused by Code Red, a Web worm, an electronic ailment akin to computerized snakebite. Code Red infects Microsoft Internet Information Servers (IIS). Whereas home computers typically use other systems, many of the most popular Web sites run on IIS. In two lightning-fast strikes, Code Red managed to infiltrate hundreds of thousands of IIS servers in only a few hours, slowing the Internet's operations. Although Code Red's effects have waned, patching the security holes in the estimated six million Microsoft IIS Web servers worldwide and repairing the damage inflicted by the worm have cost billions of dollars.

What really disturbs system administrators and other experts, however, is the idea that Code Red may be a harbinger of more virulent Internet plagues. In the past, Web defacements were perpetrated by people breaking into sites individually—the cyberwarfare equivalent of dropping propaganda leaflets on targets. But computer researchers dread the arrival of better-designed automated attack worms that could degrade or even demolish the World Wide Web.

Further, some researchers worry that Code Red was merely a test of the type of computer programs that any government could use to crash the Internet in times of war. This past spring's online skirmishes over the U.S. spy plane incident with China emphasize the dangers. Full-scale cyberwarfare could cause untold damage to the industrialized world [see "What Happens if the Internet Crashes?" on page 45]. These secret assaults could even enlist your PC as a pawn, making it a "zombie" that participates in the next round of computerized carnage.

BY CAROLYN MEINEL • Photographs by Ethan Hill

AMERICAN HACKERS are being enlisted to help fight the U.S. government's cyberwars.

Save for the scales on which these computer assaults are waged, individual hacking and governmental cyberwarfare are essentially two sides of the same electronically disruptive coin. Unfortunately, it's hard to tell the difference between them until it's too late.

Often popularly lumped in with viruses, Code Red and some similar pests such as Melissa and SirCam are more accurately called worms in the hacker lexicon. Mimicking the actions of its biological namesake, a software virus must incorporate itself into another program to run and replicate. A computer worm differs in that it is a self-replicating, self-contained program. Worms frequently are far more infectious than viruses. The Code Red worm is especially dangerous because it conducted what are called distributed denial of service (DDoS) attacks, which overwhelm Internet computers with a deluge of junk communications.

During its July peak, Code Red menaced the Web by consuming its bandwidth, or data-transmission capacity. "In cyberwarfare, bandwidth is a weapon," says Greggory Peck, a senior security engineer for FC Business Systems in Springfield, Va., which works to defend U.S. government clients against computer crime. In a DDoS attack, a control computer commands many zombies to throw garbage traffic at a victim in an attempt to use up all available bandwidth. This kind of assault first made the news last year when DDoS attacks laid low Yahoo, eBay and other dot-coms.

More than 359,000 servers were infected with the CODE RED WORM in less than 14 HOURS.

WEB WATCHER David Moore monitored the rapid spread of Code Red.

These earlier DDoS incidents mustered just hundreds to, at most, thousands of zombies. That's because attackers had to break into each prospective zombie by hand. Code Red, being a worm, spreads automatically—and exponentially. This feature provides it with hundreds of times more zombies and hence hundreds of times more power to saturate all available Internet bandwidth rapidly.

The initial outbreak of Code Red contagion was not much more than a case of the sniffles. In the five days after it appeared on July 12, it reached only about 20,000 out of the estimated half a million susceptible IIS computer servers. It wasn't until five days afterward that Ryan Permeh and Marc Maiffret of eEye Digital Security in Aliso Viejo, Calif., a supplier of security software for Microsoft servers, discovered the worm and alerted the world to its existence.

On July 19 the worm reemerged in a more venomous form. "More than 359,000 servers were infected with the Code Red worm in less than 14 hours," says David Moore, senior technical manager at the Cooperative Association for Internet Data Analysis in La Jolla, Calif., a government- and industry-supported organization that surveys and maps the Net's server population. The traffic jam

What Happens if the Internet Crashes?

WHAT WOULD BE the consequences if the Internet failed in the face of a hacking onslaught? They would be far worse than not being able to make bids on eBay—potentially affecting product manufacturing and deliveries, bank transactions, telephony and more. Should it occur five years from now, the results could be a lot more severe.

Today many businesses use the World Wide Web to order parts and arrange shipments. A collapse of the system would interrupt just-in-time manufacturing, in which components reach the production line within a day or two of being used, to save on inventory costs. Many retail stores also rely on the Web to keep their shelves stocked. Within days, they could start to empty.

By then you may not be able to use your checkbook or ATM card either, as many banks are using the Internet instead of dedicated lines to save money. Other economic institutions such as Wall Street are said to be more susceptible to hackers corrupting trading data than to a shutdown of the system. The latter eventuality would be met by closing down the market.

Whereas most phones would still work if the Web went down today, experts say that may change a few years from now. Internet telephony started as a way for geek hobbyists to get free long-distance phone calls. Now, however, many calls that originate from an ordinary phone travel part of the way over the public Internet.

Meanwhile unclassified communications of the U.S. Armed Services go through NIPRNET (Non-Secure Internet Protocol Router Network), which uses public Internet communications. The Department of Defense is now "immensely dependent" on NIPRNET, according to Greggory Peck, a senior security engineer for FC Business Systems in Springfield, Va., which provides computer services to the federal government.

Many people ask whether airliners might start falling out of the sky if the World Wide Web crashes. The Federal Aviation Administration's air-traffic control system is sufficiently antiquated that it is in no danger of being held hostage to the Internet.—*C.M.*

generated by so many computers attempting to co-opt other machines began to overload the capacity of the Internet. By midafternoon, the Internet Storm Center at incidents.org—the computer security industry's watchdog for Internet health—was reporting "orange alert" status. This is one step below its most dire condition, red alert, which signals a breakdown.

Then, at midnight, all Code Red zombies quit searching for new victims. Instead they all focused on flooding one of the servers that hosts the White House Web site with junk connections, threatening its shutdown. "The White House essentially turned off one of its two DNS servers, saying that any requests to whitehouse.gov should be rerouted to the other server," says Jimmy Kuo, a Network Associates McAfee fellow who assisted the White House in finding a solution. Basically, the system administrators dumped all communications addressed to the compromised server. As it turned out, Code Red couldn't cope with the altered Internet protocol address and waged war on the inactive site. "The public didn't notice anything, because any requests went to the other server," Kuo says.

By the close of July 20, all existing Code Red zombies went into a preprogrammed eternal sleep. As the worms lodge only in each computer's RAM memory, which is purged when the machine shuts down, all it took was a reboot to eradicate their remnants. Case closed.

Or was it? A few days later analysts at eEye revealed that if someone were to release a new copy of Code Red at any time between the first through the 19th day of any month (the trigger dates coded in by the original hacker), the infection would take off again.

Over the next 10 days computer security volunteers worked to notify Microsoft IIS users of the vulnerability of their servers. On July 29 the White House held a press conference to implore people to protect their IIS servers against Code Red's attacks. "The mass traffic associated with this worm's propagation could degrade the functioning of the Internet," warned Ronald L. Dick, director of the FBI's National Infrastructure Protection Center. By the next day Code Red was all over the news.

The second coming of Code Red was, as expected, weaker than the first. On August 1, it infected approximately 175,000 servers—nearly all those susceptible and about half the total of the previous episode. A slower infection rate and fewer vulnerable servers held Internet disruptions to a minimum. After a while, the second attack subsided.

But that was not the end. Yet another worm was unleashed on August 4 using the same break-in method as Code Red. The new worm, dubbed Code Red II, installed a backdoor allowing a master hacker to direct the activities of victim computers at will. The worm degraded intranets with "arp storms" (floods of Ethernet packets) and hunted for new victims. In short order, Code Red II disabled parts of the Web-based e-mail provider Hotmail, several cable and digital subscriber-line (DSL) Internet providers and part of the Associated Press news distribution system. As time passed, Code Red II managed to infect many corporate and college intranets. Halfway through August, Code Red II disabled some Hong Kong government internal servers. The most common victim computers were personal Web servers run by Windows 2000 Professional. This rash of disruptions prompted incidents.org to again declare an orange alert. Experts estimate that 500,000 internal servers were compromised.

In mid-August, Computer Economics, a security research company, said that Code Red had cost $2 billion in damage. By the time it is fully purged from the Internet, the computer attack will probably rank among the most expensive in histo-

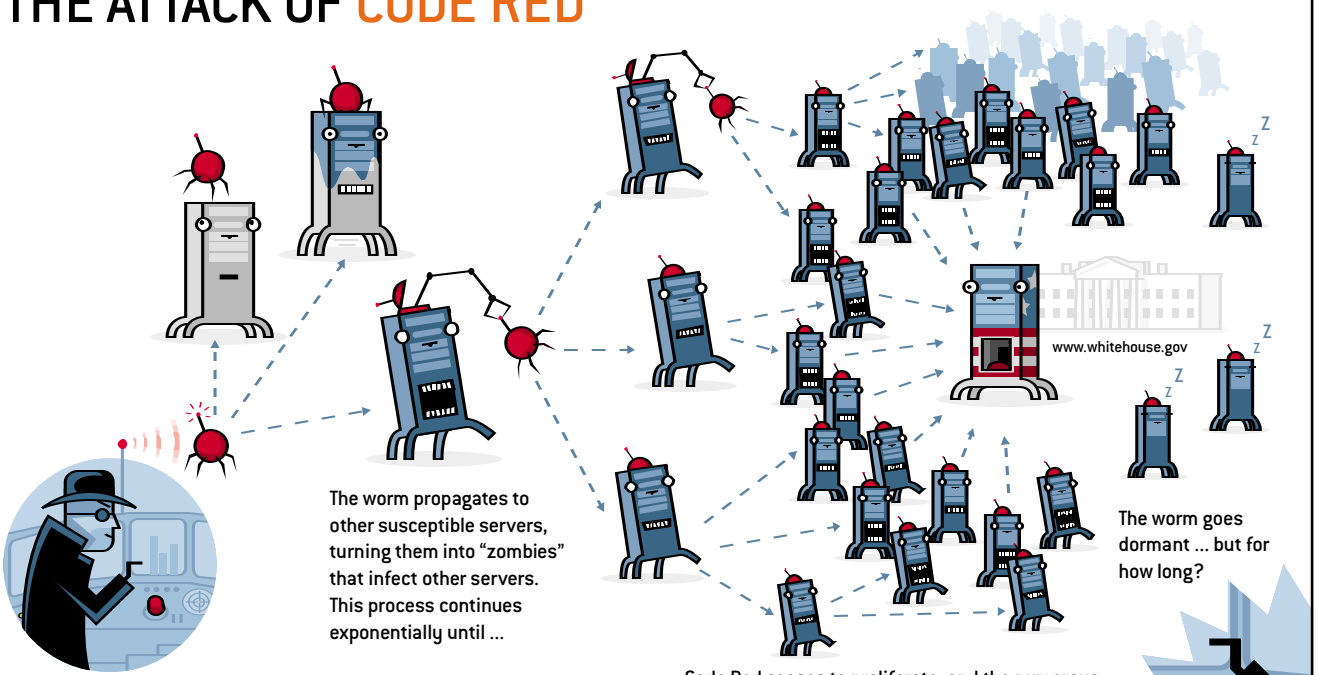
THE AUTHOR

CAROLYN MEINEL writes frequently about computer security. Based in Sandia Park, N.M., she is the author of *The Happy Hacker* and *Überhacker! How to Break into Computers*. Meinel's upcoming book, *War in Cyberspace,* examines Internet warfare. Her Web site, happyhacker.org, is a resource for home computer users.

Code Red internet worms

CODE RED is an Internet worm that infects unprotected Microsoft Internet Information Servers (IIS), on which many popular Web sites run. During the summer, the worm's secret assaults turned IIS computers into "zombies" that conducted what is called a distributed denial of service attack on the White House Web site, attempting to overwhelm it by flooding it with garbage communications. More effective worms have the potential to saturate the Web's data-transmission capacity, possibly disabling the Internet.

THE ATTACK OF CODE RED

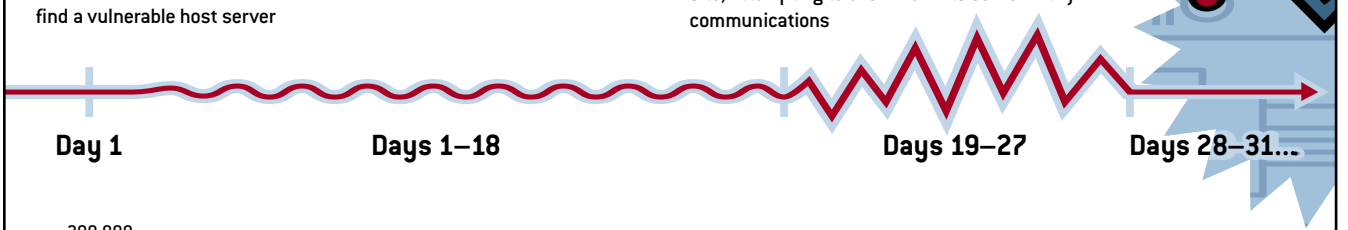


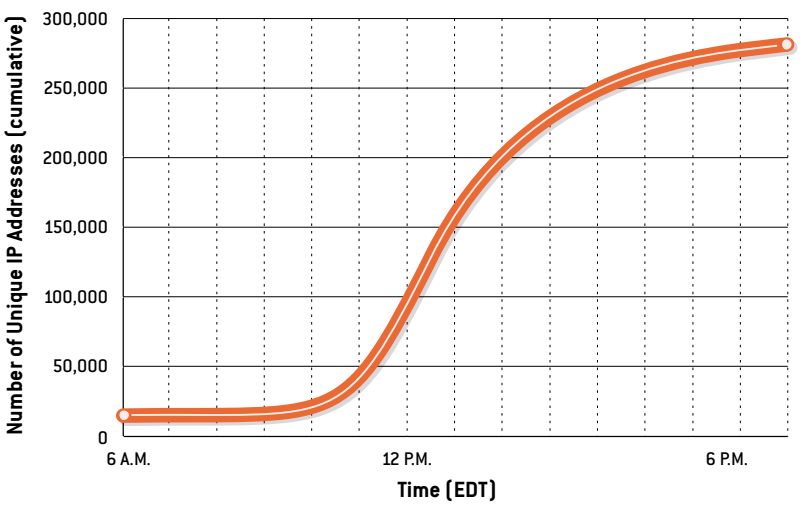
A malicious hacker sends the Code Red worm out onto the Internet to find a vulnerable host server

The worm propagates to other susceptible servers, turning them into "zombies" that infect other servers. This process continues exponentially until ...

... Code Red ceases to proliferate, and the numerous zombie servers turn to attack the White House Web site, attempting to overwhelm its server with junk communications

The worm goes dormant ... but for how long?





INTERNET PROTOCOL ADDRESSES INFECTED BY CODE RED

RAPID RISE—During a 12-hour period on July 19, 2001, the number of Internet protocol addresses compromised by the first large-scale assault of the Code Red worm surged from around 16,000 to about 280,000. After its initial spread, Code Red went dormant. Soon thereafter, however, a reinfection caused another, smaller outbreak. Experts estimate that the worm's attacks and the following Code Red II outburst will cost several billion dollars to rectify.

ry. Nearly $9 billion was spent to fight last year's LoveLetter virus, and 1999's Melissa worm assault cost $1 billion to repair.

Of course, Code Red isn't the only worm out there. Some of them are aimed at home computers. A worm called W32/Leaves, for example, permits a remote attacker to control infected PCs in a coordinated fashion, enabling synchronized waves of attacks. (Although Code Red II allows this possibility as well, it lacks the coding that enables remote control.) The Computer Emergency Response Team, a federally funded watchdog organization at Carnegie Mellon University, has received reports of more than 23,000 W32/Leaves zombies. The current total is unknown, but as W32/Leaves continues to propagate, the infected population will probably grow significantly. In July, Britain's Scotland Yard charged an unidentified 24-year-old man with creating W32/Leaves.

"Almost any computer, operating system or software you may buy contains weaknesses that the manufacturer knows lets hackers break in," says Larry Leibrock, a leading researcher in computer forensics and associate dean for technology of the business school of the University of Texas at Austin. Future "federal regulation could require that vendors take the initiative to contact customers and help them upgrade their products to fix security flaws," he continues. "Today, however, it is up to each consumer to hunt down and fix the many ways hackers and cyberwarriors exploit to abuse their computers."

World Cyberwars

BEYOND THE THREAT posed by malicious hacker programs is the danger of Internet attacks conducted in a concerted fashion by top computer talent spurred to act by international events. The cyberbattles that broke out over the collision of a Chinese fighter plane that collided with a U.S. Navy EP-3E spy plane this past April give a hint of how such a conflict might play out.

According to accounts in the press, the hacker exchanges began when negotiations for the release of American hostages stalled. On April 9 and 10, attackers defaced two Chinese Web sites with slurs, insults and even threats of nuclear war. During the following week, American hackers hit dozens more Chinese sites. Those supporting China responded by disfiguring one obscure U.S. Navy Web site.

China, however, held a weapon in reserve. In late March the National Infrastructure Protection Center had warned of a new worm on the loose: the 1i0n Worm. Lion, the hacker who founded the hacker group H.U.C. (Honkers Union of China), has taken credit for writing it. Unlike the initial Code Red's preprogrammed zombies, 1i0n's zombies accept new commands from a central computer. Also, 1i0n infects Linux computers, which means it can masquerade as any computer on the Net. This property makes it hard to track down infected servers.

Meanwhile pro-U.S. hack attacks escalated. The official Chinese publication, *People's Daily*, reported that "by the end of April over 600 Chinese Web sites had come under fire." In contrast, Chinese hackers had hit only three U.S. sites during the same period.

In the next few days the Chinese hacker groups H.U.C., Redcrack, China Net Force, China Tianyu and Redhackers assaulted a dozen American Web sites with slogans such as "Attack anti-Chinese arrogance!" On the first of May several DDoS strikes were initiated. Over the next week Chinese hackers took credit for wrecking about 1,000 additional American Web sites.

On May 7 China acknowledged its responsibility for the DDoS attacks and called for peace in a *People's Daily* news story. It ran: "The Chinese hackers were also urged to call off all irrational actions and turn their enthusiasm into strength to build up the country and safeguard world peace."

U.S. law-enforcement agencies, the White House and U.S. hacker organizations never objected to the American side of this cyberconflict, although the FBI's infrastructure center had warned of "the potential for increased hacker activity directed at U.S. systems."

How to Wage Covert Cyberwarfare

IN VIEW OF the spy-plane episode, some commentators have wondered whether the U.S. federal government encouraged American hackers to become agents of cyberwar. After all, the U.S. has worked with private groups to wage covert warfare before, as in the Iran/Contra scandal. And links between the two communities have been reported. It's difficult, however, to say exactly how strong the connection between hackers and the government might be. Clearly, the murky world of hacking doesn't often lend itself to certainty. And because it is the policy of the U.S. National Security Agency and various Defense Department cyberwarfare organizations not to comment on Web security matters, these relationships cannot be confirmed. Still, the indications are at least suggestive.

Consider the history of Fred Villella, now an independent computer consultant. According to numerous press reports and his own statements, Villella took part in counterterrorism activities in the 1970s. In 1996 he hired hackers of the Dis Org Crew to help him conduct training sessions on the hacker threat for federal agencies. This gang also helps to staff the world's largest annual hacker convention, Def Con.

Erik Ginorio (known to the hacker world as Bronc Buster) publicly took credit for defacing a Chinese government Web site on human rights in October

Code Red II installed a backdoor allowing a MASTER HACKER to direct victim computers at will.

1998. This act is illegal under U.S. law. Not only was Ginorio not prosecuted, he says Villella offered him a job. Villella could not be reached for comment.

In another hacker-government connection, Secure Computing in San Jose, Calif., became a sponsor of Def Con in 1996. According to its 10-K reports to the U.S. Securities and Exchange Commission, Secure Computing was created at the direction of the National Security Agency, the supersecret code-breaking and surveillance arm of the U.S. government. Two years after that, Secure Computing hired the owner of Def Con, Jeff Moss. Several former Villella instructors also staffed and managed Def Con.

Questionable things happen at Def Cons. At the 1999 Def Con, for example, the Cult of the Dead Cow, a hacker gang headquartered in Lubbock, Tex., put on a mediagenic show to promote its Back Orifice 2000 break-in program. Gang members extolled the benefits of "hacking to change the world," claiming that eight-year-olds could use this program to break into Windows servers.

Meanwhile Pieter Zatko, a Boston-area hacker-entrepreneur and a member of the gang, was onstage promoting a software plug-in for sale that increased the power of Back Orifice 2000. According to the Cult's Web site, Back Orifice 2000 was downloaded 128,776 times in the following weeks. On February 15, 2000, President Bill Clinton honored Zatko for his efforts by inviting him to the White House Meeting on Internet Security. Afterward Zatko remained with a small group to chat with the president.

Every year Def Con holds a "Meet the Feds" panel. At its 2000 meeting, Arthur L. Money, former U.S. assistant secretary of defense for command, control, communications and intelligence, told the crowd, "If you are extremely talented and you are wondering what you'd like to do with the rest of your life—join us and help us educate our people [government personnel]."

In 1997 Moss launched the Black Hat Briefings. In hacker lingo, a black hat is a computer criminal. Theoretically, these meetings are intended to train people in computer security. They bear considerable similarity to Def Con, however, only with a $1,000 price tag per attendee. Their talks often appear to be more tutorials in how to commit crime than defend against it. For example, at one session attendees

What Can Be Done to Defend the Web?

AS POGO the comic-strip character said, "We have met the enemy and he is us." One of the weakest links in protecting the Internet is the home PC user. Cybernetic worms—self-replicating hacker software that can wreak havoc on Internet operations—can turn personal computers into "zombies," or slave agents that help to destroy other computer operations. Of particular concern are worms that can conduct effectively targeted distributed denial of service (DDoS) attacks, in which zombie computers deluge a Web site with useless communications.

Computer professionals are being asked to get the word out to home users to check for zombies. "That's because our worst Internet nightmare is the grandma who uses her DSL [high-bandwidth-capacity digital subscriber line that is always connected] to shop on eBay," says Greggory Peck of FC Business Systems, which provides computer services to the federal government. High bandwidth means that a home zombie can pump lots of junk into the Internet, swamping targeted Web sites.

You may think your home computer is safe from assault because it runs automatic virus updates or because you registered your software and receive vendor e-mails about product upgrades. Guess again. Few vendors feel obligated to help users keep hackers out. That's why it's important for home users to install firewalls.

Complicating the safety issue, most new PCs will soon be running the Windows XP operating system, which enables "raw sockets." Sockets are software constructions that generate the packets (the smallest data-transmission units) that transfer information across networks. With raw sockets technology, packets can be crafted in an arbitrary manner even if that violates safeguarding protocols. Raw sockets, for example, enabled the 1i0n worm to hide on Linux servers by forging Internet addresses (*see preceding page*). They also allow hackers to create malformed packets that will crash a receiving computer.

Beyond the home PC, another approach to defending the Web is to arrest more computer criminals. Nowadays, though, dangerous attackers may operate through a chain of compromised computers, with one or more being located across national borders. To obtain evidence in these cases requires cooperation among the law-enforcement agencies of two or more countries.

International pursuit of computer criminals would be made easier by adoption of the "Convention on Cyber-crime" now under consideration by the 44 nations of the Council of Europe, which includes the U.S., Canada and Japan. Part of the treaty would also criminalize possession or creation of computer crime instructions or programs except for the authorized testing or protection of a computer system. (The text of the Cyber-crime Treaty is available at conventions.coe.int/treaty/EN/projets/cybercrime.htm)

These restraints are controversial, though. At least 35 lobby groups, including the Electronic Frontier Foundation and the Global Internet Liberty Campaign, oppose the treaty because they believe it would restrict freedom of speech and invade personal privacy. It's hard to find antidotes to viruses and worms if researchers cannot study copies of them on their computers.

Another solution is to require that Internet servers be secure. For example, the U.S. Federal Trade Commission proposed a regulation in July that requires financial service companies to guard their networks against "anticipated threats." This is only a small step in the right direction. —*C.M.*

NET VIROLOGIST Mark A. Ludwig writes about computer viruses and worms at his rural Arizona home.

learned about "Evidence-Eliminator," billed as being able to "defeat the exact same forensic software as used by the U.S. Secret Service, Customs Department and Los Angeles Police Department."

It should be noted that the U.S. government does have a formal means to wage cyberwar. On October 1, 2000, the U.S. Space Command took charge of the Computer Network Attack mission for the Department of Defense. In addition, the U.S. Air Force runs its Information Warfare Center research group, located in San Antonio.

Get enough zombies attacking enough targets, and the ENTIRE INTERNET could become unusable.

Given these resources, why would the U.S. and China encourage cybermilitias? "It's very simple. If you have an unofficial army, you can disclaim them at any time," says Mark A. Ludwig, author of *The Little Black Book of Computer Viruses* and the upcoming *The Little Black Book of Internet Viruses*. "If your military guys are doing it and you are traced back, the egg's on your face."

Wherever it came from, the Code Red assault was just a taste of what a concerted cyberwar could become. "I think we can agree that it was not an attempt at cyberwar. The worm was far too noisy and easily detected to be much more than graffiti/vandalism and a proof-of-concept," says Harlan Carvey, an independent computer security consultant based in Virginia.

Stuart Staniford, president of Silicon Defense in Eureka, Calif., notes, however, that if the zombie computers "had a long target list and a control mechanism to allow dynamic retargeting, [they] could have DDoSed [servers] used to map addresses to contact information, the ones used to distribute patches, the ones belonging to companies that analyze worms or distribute incident response information. Code Red illustrates that it's not much harder for a worm to get *all* the vulnerable systems than it is to get some of them. It just has to spread fast enough."

Code Red already offers deadly leverage for nefarious operators, according to Marc Maiffret, who bills himself as "chief hacking officer" of eEye: "The way the [Code Red] worm is written, it could allow online vandals to build a list of infected systems and later take control of them."

Get enough zombies attacking enough targets, and the entire Internet could become unusable. Even the normal mechanisms for repairing it—downloads of instructions and programs to fix zombies and the ability to shut off rogue network elements—could become unworkable. In addition, hackers constantly publicize new ways to break into computers that could be used by new worms. A determined attacker could throw one devastating worm after another into the Internet, hitting the system every time it struggled back and eventually overpowering it.

"We know how [crashing the Internet] can be done right," says Richard E. Smith, a researcher with Secure Computing and author of the newly published book *Authentication*. "What I've found particularly disquieting is how little public fuss there's been [about Code Red]. The general press has spun the story as being an unsuccessful attack on the White House as opposed to being a successful attack on several hundred thousand servers: 'Ha, ha, we dodged the bullet!' A cynic might say this demonstrates how 'intrusion tolerant' IIS is—the sites are all penetrated but aren't disrupted enough to upset the owners or generate much press comment. The rest of us are waiting for the other shoe to drop." SA

MORE TO EXPLORE

The Computer Emergency Response Team's Guide to Home Network Security: **www.cert.org/tech_tips/home_networks.htm**

The Internet Storm Center: **www.incidents.org**

The National Infrastructure Protection Center: **www.nipc.gov**

The Cooperative Association for Internet Data Analysis: **www.caida.org**

Microsoft Windows NT, 2000 and XP security information: **www.ntbugtraq.org**

Free security test for home computers: **grc.com** and **security2.norton.com/us/home.asp**

Microsoft Windows NT, 2000 and XP information: **www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/current.asp**