

Denial-of-Service Attacks Rip the Internet

Lee Garber

The Internet community is trying to cope with the series of distributed denial-of-service attacks that shut down some of the world's most high-profile and frequently visited Web sites, including Yahoo and Amazon.com, in February.

The attacks, which observers say cost victims millions of dollars, sent shock waves through the industry because they crippled some of the world's premier e-commerce sites.

And the problem was even worse than many people realize because more companies were attacked than those mentioned in the media, said Stephen Northcutt, director of the Global Incident Analysis Center (GIAC), an organization that conducts research and education programs on system administration, networking, and security.

For example, he said, "I have not [read] about any attacks outside the United States, but I had people tell me that sites were hit in London." Northcutt said many companies don't want to admit they've been attacked because they are worried about bad press and copycat attacks.

"DDoS attacks constitute one of the single greatest threats facing businesses involved in electronic . . . commerce because an attack can completely shut down a Web site," said Morgan Wright, director of Rapid Emergency Action Crisis Team (REACT) services for Global Integrity, an information-security firm.

It is the nature of the attacks, as well as their scope, that has many people worried. In most of the cases, the perpetrators of the DDoS attacks planted daemons on perhaps thousands of intermediate computers, called *zombies*, which were then used as unwitting



accomplices to flood and subsequently overwhelm defenseless Web servers with huge amounts of traffic.

This use by hackers of vulnerable systems to attack other, better defended systems demonstrated just how dependent Web-based organizations are on other organizations for security, despite their having spent billions of dollars on firewalls, intrusion-detection systems, network vulnerability scanners, and encryption technology.

And experts say they are concerned about the future. For example, David Kennedy, director of research services for ICSA.net, an Internet security service provider, said many networks are being built quickly with speed and functionality but not security in mind. Also, he said, there is a shortage of highly qualified network security personnel who could help cope with the DDoS threat. Moreover, hackers have placed user-friendly DDoS tools on Web sites, where even untrained hackers can find and implement them.

In recognition of these concerns, security experts recommend that organizations and even individuals with Internet connections undertake a number of sig-

nificant and potentially expensive changes to their operations, such as

- implementing new protocols in network equipment to enhance security for Internet communications,
- patching vulnerabilities in Unix systems, and
- regularly updating antivirus and intrusion-detection software.

These measures are critical because security experts are finding evidence that intruders are developing more user-friendly and effective DDoS tools. In addition, hackers will find it easier to access the computers belonging to the millions of consumers who are adopting high-bandwidth, always-on Internet-access technologies, such as DSL (digital subscriber line) and cable modems, than the machines that use temporary dial-up access.

"[The] assaults on some of the most popular Web sites serve as a serious wake-up call to the importance of security in today's Internet economy," added Tom Noonan, president and CEO of Internet Security Systems (ISS), a security-management software and service vendor.

THE ATTACKS

On Monday, 7 February, the first of the high-profile DDoS attacks hit Yahoo, the most popular site on the Web. (Yahoo had more unique visitors in January than any other site, according to Media Metrix, a company that specializes in online traffic measurement.)

The next day, intruders knocked out Buy.com, a large Web-based store celebrating its initial public offering of stock that morning, for 2.5 hours. During the next nine hours, DDoS attacks hammered eBay (15th highest number of unique visitors in January), CNN.com (41st highest), and Amazon.com (10th highest). And the following day, ZDNet (19th highest), E*Trade, and Excite (11th highest) also fell victim. In some cases, the attacks inundated servers with 1 gigabit per second of incoming data, which is much more traffic than they were built to handle. This caused the Web sites to go offline for as long as several hours.

Buy.com CEO Gregory Hawkins said,

“This was clearly an outside, coordinated attack to our network that prevented access to our site.”

Every minute a high-volume e-commerce site like Buy.com is offline, it loses considerable business that, in some cases, may never return. This could threaten confidence in the online economy, just when it stands poised to become an established and significant part of the global economy.

The DDoS assaults also affected the Internet in general. For example, the attacks pumped out so much traffic, and so many people browsed the Web for information about the incidents, that the entire Internet slowed down, said Keynote Systems, a provider of Internet performance-measurement and consulting services to e-commerce sites. As shown in the figure on this page, Keynote found that the Internet’s performance on 9 February, the last day of the attacks, was 26.8 percent worse than a week earlier.

Meanwhile, said ICSCA.net’s Kennedy, daemons may be sitting on unsuspecting zombies now, waiting to launch attacks.

The zombies

Although not all of February’s victims provided details of their attacks, it appears that all or almost all of the machines turned into zombies were Unix- or Linux-based PCs or servers. However, GIAC’s Northcutt said, Windows machines are just as vulnerable. This is scary, he said, because it makes the millions of Windows boxes, including those in private homes, potential zombies.

A number of the zombies in February’s attacks were found on university networks. For example, said Kevin Schmidt, campus network programmer at the University of California, Santa Barbara, one of the 12,000 computers at his school was used to attack CNN.

University networks appeal to DDoS hackers because they frequently have very high-bandwidth Internet connections, said Shawn Hernan, vulnerability-handling team leader with the CERT Coordination Center, a computer-security research and emergency response team based at Carnegie Mellon University’s Software Engineering Institute (SEI). Also, he said, hackers can access university systems rel-

| Date | Internet performance (seconds) | Internet performance a week earlier (seconds) | Change |
|-------------|--------------------------------|---|--------------|
| 7 February | 5.98 | 5.66 | 5.7% slower |
| 8 February | 5.96 | 5.53 | 7.8% slower |
| 9 February | 6.67 | 5.26 | 26.8% slower |
| 10 February | 4.86 | 4.97 | 2.2% faster |

Source: Keynote Systems

During the three days of last February’s denial-of-service attacks, overall Internet traffic slowed, based on performance measurements conducted by Keynote Systems, a provider of Internet performance-measurement and consulting services. Keynote measured Internet performance by determining the average time it took to access and download the home pages of 40 important business Web sites every 15 minutes during business hours from 66 Internet access points in 25 US metropolitan areas.

atively easily because they are very open, providing easy access to research institutions, students, faculty, and others.

The investigation

Law enforcement officials were notified and immediately began their investigation. However, at press time, no arrests had been made.

Because the attacks violated the US Computer Fraud and Abuse Act, which makes it a crime to knowingly transmit a program or command that intentionally damages a computer, the US Federal Bureau of Investigation (FBI) is conducting a criminal investigation. Conviction of this violation carries a sentence of six months to five years and a fine, said FBI spokesperson Debbie Weierman.

According to Weierman, all 56 of the FBI’s field offices are involved in the investigation and are working with the US interagency National Infrastructure Protection Center (NIPC).

Victims of the recent DDoS attacks—including those whose machines were used as zombies—and Internet service providers whose services were used have been turning over system logs and other information to investigators, said FBI Director Louis J. Freeh.

The GIAC’s Northcutt said it can be very hard to catch DDoS hackers, particularly if they’re careful. Frequently, he said, hackers spoof the return IP addresses of the packets they send, making them difficult to trace.

Meanwhile, said CERT’s Hernan,

hackers also frequently run executables with their DDoS traffic that wipe out or alter network and system logs. “You just have to hope that perhaps there was a firewall log they didn’t have access to,” he noted.

Sometimes, said ICSCA.net’s Kennedy, the only way to identify DDoS attackers is to use network-monitoring tools to look at router interfaces all along a transmission path while an attack is occurring. This technique can permit administrators to determine where the DDoS packets originate. However, the process can be difficult and time-consuming.

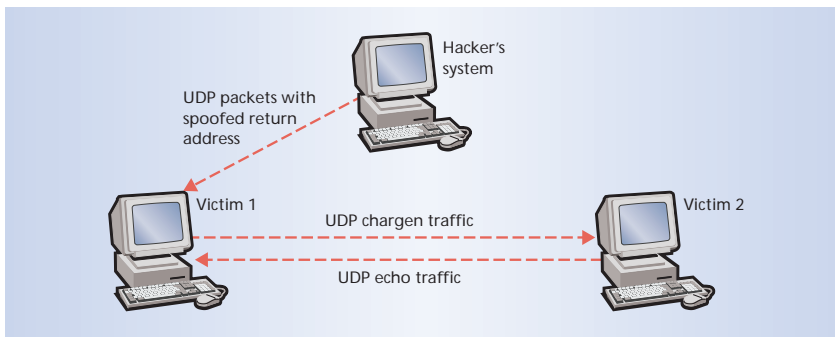
UC Santa Barbara’s Schmidt said he left his network’s compromised machine running for a while after the CNN attack, hoping he could catch intruders using it again. However, he said, this didn’t occur.

In these cases, Hernan said, investigators may have to resort to old-fashioned police work, by, for example, working with informants in the hacker community.

DDOS ATTACKS

Denial-of-service attacks have been around for years. The attacks have used several techniques to crash, hang up, or overwhelm servers with malformed packets or large volumes of traffic. However, said Northcutt, it is the highly distributed aspect of February’s attacks that made them so different and frightening.

In DDoS attacks, hackers may scan millions of machines connected to the Internet and look for unprotected ports,



In a UDP flood attack, a hacker sends UDP packets with spoofed return addresses that link one system's chargen (character-generating) service to another system's UDP echo service. The chargen service begins sending characters to the other system, whose echo service responds. This ongoing flow of UDP traffic ties up both systems.

vulnerable services, and other weaknesses that will let them gain root access, said CERT's Hernan.

Once hackers gain access, they simultaneously install daemons on intermediate machines through batch processes, noted SEI director Stephen Cross.

The daemons then quietly listen to network traffic and wait for commands from the hacker's master machines to launch the DDoS assaults, Hernan explained.

Generally, the only way an organization can stop a DDoS attack once it starts

is to identify the addresses of all zombies sending DDoS packets and shut off traffic from them. This can be a very slow process, as February's victims learned.

University of Minnesota: a prelude

The first reported large-scale DDoS attack via the public Internet occurred in August 1999 on a network used by faculty and students at the University of Minnesota.

The attack, which shut down the network for more than two days, was

launched by 227 zombies, including 114 that were part of the high-speed, high-capacity Internet 2 project. Using Internet 2 made the zombies particularly effective, and is part of a potential future attack scenario that concerns many observers.

Since the University of Minnesota attack, a growing number of DDoS tools began appearing on the Internet. So in December, said FBI Director Freeh, the NIPC issued an alert, and its Special Technologies and Applications Unit created and released a software tool (<http://www.fbi.gov/nipc/trinoo.htm>) that lets system administrators identify major DDoS daemons installed on their computers.

IRC networks: a testing ground

For several years, DDoS attacks have been occurring in Internet Relay Chat (IRC) networks, said Northcutt. The closed networks, which permit anonymous log-ins, have attracted hackers,

I wish I could find a developer.

I wish I could find a developer.

I wish I could find a developer.

I love being a software developer.

I wish I hadn't eaten that corn dog.

Targeted, specific, completely confidential job and people matching. Designed just for software developers. Give your career an upgrade.

Prepare to meet your match. www.careercentral.com/dev

career central
for developers

including members of competing groups in some cases.

According to Northcutt, some hackers have experimented with DDoS attacks in the smaller, more easily controlled IRC environment as part of turf warfare with their rivals. The frequency of these attacks has caused a number of universities and private companies to stop hosting IRC networks.

With February's attacks, Northcutt said, DDoS attacks have definitely expanded beyond the IRC setting. "The genie is out of the bottle now."

Types of attacks

The basic principle for all DDoS attacks is to use multiple intermediate machines to overwhelm other computers with traffic. A few prominent examples show the different types of DDoS techniques that hackers use:

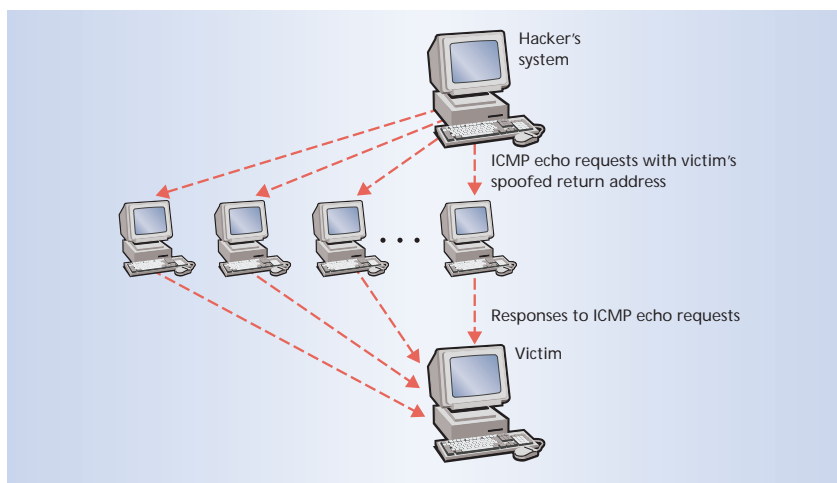
UDP flood. Hackers have used UDP (User Datagram Protocol) technology to launch DDoS attacks. For example, by sending UDP packets with spoofed return addresses, a hacker links one system's UDP character-generating (chargen) service to another system's UDP echo service.

As the chargen service keeps generating and sending characters to the other system, whose echo service keeps responding, UDP traffic bounces back and forth, preventing the systems from providing services, as shown in the figure on the previous page.

Variations of this attack link two systems' chargen and echo services.

SYN flood. In TCP-based communications, an application sends a SYN synchronization packet to a receiving application, which acknowledges receipt of the packet with a SYN-ACK, to which the sending application responds with an ACK. At this point, the applications can begin communicating.

In a SYN flood attack, the hacker sends a large volume of SYN packets to a victim. However, the return addresses in the packets are spoofed with addresses that don't exist or aren't functioning. Therefore, the victim queues up SYN-ACKs but can't continue sending them because it never receives ACKs from the spoofed addresses. The victim then can't provide services because its backlog queue fills up



In a smurf attack, a hacker sends out ICMP echo requests to a large group of hosts on a network but spoofs the packets' return addresses so they show a victim's address. The hosts then send the victim a flood of response traffic, which ties up its system.

and can't receive legitimate SYN requests.

Smurf. In this type of attack, shown in the figure on this page, a hacker broadcasts ICMP (Internet Control Message Protocol) echo (ping) requests, with the return addresses spoofed to show the ultimate victim's address, to a large group of hosts on a network. The hosts send their responses to the ultimate victim, whose system is overwhelmed and cannot provide services.

Tools of the trade

The best known daemon tools used by hackers to launch their DDoS assaults, including some used in February's attacks, include Trinoo, Tribe Flood Network (TFN), Stacheldraht (which means barbed wire in German), and TFN2K, an updated version of TFN.

Hackers frequently post their DDoS tools' source code on the Internet. This permits the hacker community to upgrade the tools in an open-source environment. "It's an arms race," said ICSA.net's Kennedy.

For example, in creating TFN2K, hackers have upgraded TFN by creating a daemon that encrypts its own signals. This keeps the signals from being recognized by intrusion-detection tools that scan for bit strings from known DDoS commands. In addition, TFN2K is harder to detect because it doesn't issue acknowledgments to commands from the hacker's master machines. Instead, the masters send each command multiple times, hoping the daemon gets at least one.

Meanwhile, technically savvy hackers have developed tools that are very easy to use, and they have posted them on the

Internet. This means that even hackers with little experience—called *script kiddies*, *code kiddies*, or *packet monkeys*—can launch complex, dangerous attacks.

DDOS VULNERABILITIES

Several important vulnerabilities make it easier for hackers to successfully implement DDoS attacks.

Planting daemons

Most security experts agree that the key for DDoS hackers is to find zombies, because once they've done so, many of the ultimate victims have virtually no defense against the flood of traffic they will receive.

A principal vulnerability that hackers use is the availability of TCP/IP ports through which they can gain root access to a computer, according to CERT's Hernan. Frequently, firewall or network administrators block only the ports they consider to be particularly dangerous, such as port 23, used for Telnet access, or port 53, used for domain-name server access. To reduce the risk, Hernan said, administrators should block all ports except those they specifically want people to access.

Once into a machine, hackers look for a vulnerability they can exploit to plant a daemon. In fact, said ICSA.net's Kennedy, vulnerabilities in the services behind open ports pose a bigger problem than the open ports themselves.

For example, a principal server vulnerability involves RPC (remote procedure call) services in Solaris, Sun Microsystems' version of the Unix OS. According to Hernan, Solaris can let intruders embed a

metacharacter followed by a command in an RPC command line. This will tell the command processor to execute whatever command follows the metacharacter, even if it is malicious, he said.

According to CERT's Hernan, the Internet also has fundamental weaknesses that make systems vulnerable to DDoS attacks.

For example, he said, "Many of the Internet's older protocols, which are also the most popular, tend to be unauthenticated entirely. For example, SMTP (simple mail transfer protocol) and HTTP are virtually unauthenticated. And the DNS (domain name system) is largely unauthenticated and largely untrustworthy." Lack of authentication makes it easier for hackers to successfully spoof return addresses.

These vulnerabilities exist because, while the Internet was designed to survive external attacks on the physical communications infrastructure, it was also built as an open system not designed

to cope with attacks from within, according to the SEI's Cross. Now that millions of people, including many intruders, are "within," the Internet community must figure out how to cope with such problems as DDoS attacks.

Inexperienced IT workers

A contributing factor to the success of DDoS attacks, according to Kennedy, "is a lack of skilled personnel. The IT explosion has outpaced the ability of anyone to produce enough computer security professionals . . . to secure all these systems."

In many cases, organizations hire people without significant experience or training to work on networks. These employees are not as likely to successfully deal with complex DDoS attacks, Kennedy said, particularly as network and Internet technologies continue to change rapidly.

WHAT THE FUTURE HOLDS

Although users can take steps to minimize the threat posed by DDoS attacks


(see the sidebar, "Denying DDoS Attacks"), there are several reasons for concern about the future.

First, hackers may become more tempted over time to launch the attacks because increasingly fast networks could provide more effective means by which to overwhelm victims with traffic.


In addition, future hacker techniques may bypass such defenses as packet filtering. For example, the stream.c DoS tool uses forged TCP/IP packets, which most routers don't filter.

The GIAC's Northcutt said one of his biggest fears is that hackers will use Windows machines as zombies for DDoS attacks. Many Windows boxes are in residential and small business settings, where there is minimal, if any, security.

Shortly after February's DDoS attacks, James Madison University in Harrisonburg, Virginia, was looking into unusual network activity and discovered that 16 PCs using the school's student-residence network were infected with a Windows

**SMU ENGINEERING**

Take a leadership role in Software Engineering.

**Master of Science in Software Engineering**

Be at the forefront of the next century's most important industry with a Master's degree from SMU. Our core curriculum was developed in consultation with the Software Engineering Institute, which means we offer the very best and latest innovations in the field. You'll be trained in critical software and system design principles as well as practical problems of bringing products to market. Get the competitive advantage in the new millennium.

Available nationwide through videotape distance education.

For information call 214.768.1452
www.seas.smu.edu

SMU will not discriminate on the basis of race, color, religion, national origin, sex, age, disability, or veteran status.

techinsurance.com

Affordable Coverage
In 24 Hours
and 15 Minutes.

Are you a computer consultant paying too much for Professional Liability coverage? If you think you are, check out **Techinsurance.com** and get a free quote. IEEE members receive a 10% discount on the best rates nationally.

Techinsurance.com is your online source for SafetyTek[®] the affordable IT insurance program. Our online quoting service is the fastest in the industry: Just spend 15 minutes completing an application, and you'll get a quote back within 24 hours.

SafetyTek provides the insurance you need – now and as you grow. Get General Liability for as little as \$350 in most states, and Professional Liability for as low as \$1,000. Worker's Compensation, Health and Disability insurance are also available at competitive rates.

Apply online at **www.techinsurance.com**
or call us at **1-800-668-7020**.

SafetyTek[®]
Preferred Provider

Denying DDoS Attacks

Experts have many suggestions as to how users can prevent or cope with distributed denial-of-service (DDoS) attacks.

For example, they say, organizations should conscientiously apply security patches to operating systems and server software; install effective firewalls and update them when necessary; and regularly monitor system logs, network traffic, and system configurations for anomalies. Also, they say, organizations need contingency plans and crisis response strategies in case they become victims.

Organizations should also help keep attacks from driving their Web sites offline by having at least two Internet connections, said Stephen Northcutt, director of the Global Incident Analysis Center (GIAC), which conducts research and education programs on system administration, networking, and security. However, Northcutt said, if the DDoS threat is not eliminated soon, the additional cost of having redundant connections "will price some people out of the [Internet] market."

Some day, DDoS prevention may be a matter of legal prudence, said David Kennedy, director of research services for ICSA.net, an Internet security service provider. He said courts may find the owners of the computers that hackers use to launch attacks liable for damages, if the owners didn't use available security measures.

Meanwhile, Northcutt said, "We need some busts. We need to send some people to jail. Punishment is a deterrence."

Key recommendation: ingress and egress filters

The key recommendation by security experts was that Internet service providers (ISPs), universities, other organizations that provide users with dial-up Internet access, and large companies should install ingress and egress filters in their networks.

These filters are designed largely to stop Internet packets with spoofed return IP addresses (which are frequently used to carry out DDoS attacks) from entering or leaving networks. In some cases, the filters also admit traffic only from authorized sources.

Generally, ICSA.net's Kennedy said, the filters look for packets with addresses that should not be found entering or leaving a particular network. For example, he said, traffic

should not be entering a network with IP addresses that belong only on packets generated within the network or with nonroutable addresses, such as those set aside for use only for transmissions within private networks.

ICSA.net has joined with a group of ISPs and telecommunications companies to form the Alliance for Internet Security. According to Kennedy, the alliance was formed largely to encourage the installation and use of ingress and egress filters, although it will also recommend other measures.

"Buying and installing the filters can be expensive, depending on how big your network is. But it should be considered the cost of doing business on the Internet," he said.

"If only 30 percent of Internet routers and organization firewalls had such filtering, we would achieve a hundredfold reduction of threat from a single attacker," said ICSA.net chief technology officer Peter Tippet. "However, it might slow the equipment or routing somewhat."

Adopt new Internet protocols

Experts recommend that vendors and users accelerate the adoption of IPSec (IP Security Protocol) and DNSSec (Domain Name System Security Protocol), both under development by the Internet Engineering Task Force. IPSec and DNSSec are being designed, in part, to offer authentication services, which would help identify packets with spoofed return IP addresses before they cause problems.

IP version 6 also offers authentication, so as more network equipment vendors support the protocol, users will have more protection against DDoS attacks. "IPv6 will certainly have weaknesses," said the GIAC's Northcutt, "but IPv4 seems to have nothing but weaknesses."

However, said Shawn Hernan, vulnerability-handling team leader with the CERT Coordination Center, a computer-security research and emergency response team based at Carnegie Mellon University's Software Engineering Institute (SEI), "Part of the problem is backward compatibility. Many systems won't have these new measures and will still be vulnerable." Over time, though, he added, "The Internet will slowly evolve and become more secure."

variant of the trinoos DDoS daemon, which the university calls wintrinoos. The university says it checked logs and determined that the computers were not used in any of February's DDoS attacks.

Further investigation showed that hackers had gained access to every infected machine via Back Orifice, a Trojan horse developed in 1998 by a San Francisco-based hacker group called Cult of the Dead Cow. A Trojan horse is a program in which malicious code is hidden inside apparently harmless programming code or data. Back Orifice gives hackers remote-administration privileges over Windows-based machines.

Referring to the discovery of Windows-based DDoS tools on James Madison

University's machines, Northcutt said, "This is big stuff. If this gets successful, it is a formula for disaster. The key to protecting against this is keeping antivirus [and intrusion-detection] signatures up-to-date. The simple fact is that if we don't get a global or national campaign to get people to update their signatures, we are really setting ourselves up for a class of problems that are far bigger than anything we've seen yet."

Organizations must remain ready to respond to the threats posed by potential future DDoS attacks, said ICSA.net's Kennedy. Otherwise, they can count on repeating the ordeal experienced

by the victims of February's attacks.

"There is probably a subset of the hacker community pouring over TCP/IP books right now, learning the intricacies to figure out what can be exploited as a new vulnerability. And as we make changes, they'll be looking for new vulnerabilities." ★

Lee Garber is the news editor for Computer magazine. Contact him at lgarber@computer.org.

Editor: Lee Garber, *Computer*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org