

May 15, 2000

## Hackers Exploit Internet Vulnerabilities

**Sophisticated new attacks lack effective defense, demand vigilant security precautions**

*As society grows ever more dependent upon the Internet, the consequences of hacker attacks become increasingly severe. Last February, a series of attacks crippled major Internet sites for several hours, giving the American public a small taste of the danger that lurks in cyberspace. Doomsayers have bandied about the phrase "information warfare" as a devastating possibility for the future, but the Federal Bureau of Investigation (FBI) has confirmed that entities from several foreign nations are working to transform this concept into a destructive reality. U.S. government officials have already warned of the dire results that would follow a successful attack upon the nation's critical infrastructure systems, yet little progress has been made toward protecting those essential networks. Imagine a terrorist attack upon New York or San Francisco, timed in concert with a blackout of the metropolitan power grid. Envision the results of a simultaneous shutdown of communication systems at several of the nation's largest airports. The recent series of cyberattacks demonstrates the rapid advancement of the day when such scenarios will present viable threats.*

*Experts estimate that the February assaults caused hundreds of millions of dollars in losses and damage, dealing a stunning blow to the heart of electronic commerce. Even though authorities have begun arresting suspected perpetrators, the threat of attack remains, underscoring the need for close cooperation between information technology (IT) and security professionals.*

### Method of attack

The computer vandals who successfully shut down several high-profile web sites last February—including the FBI's—used what is known as a distributed denial-of-service (DDoS) attack. The capability of launching denial-of-service attacks (DoS) has existed for decades, but new tools have transformed this type of electronic assault into a menace with no foolproof defense.

A DoS attack overloads a computer system or network by flooding it with a large amount of traffic. In a normal connection, a computer establishes contact with a server and requests authentication, or verification that the remote computer has permission to access the host. In a DoS attack, the remote system submits several authentication requests at

once, tying up the server. The effect is similar to a person walking into a fast-food restaurant and ordering for an entire football team. Virtually no one else in the restaurant would receive service while employees tried to complete the order, and any attempted service would be significantly slowed. False, or spoofed, Internet addresses can further confuse the server, preventing it from establishing contact with the remote computer to send verification. The host system waits—sometimes as long as one minute—before breaking the connection. Then, the attacking system sends a new set of requests, beginning the process anew.

In the past, these attacks originated from a single computer, making them easy to trace and detect. Such new tools as Trinoo and Tribe Flood Network (TFN), however, distribute the assault among many machines by enabling hackers to plant a time bomb of sorts on vulnerable computer systems. These DoS tools take seconds to install, and they turn the computers into "slave" machines, also known as "daemons" and "zombies," which bombard a target with forged information packets when awakened by a "master" server. Not only are the DDoS assaults more difficult to detect, but they also make it almost impossible to identify the original attacker.

Shortly after the commencement of the February DDoS attacks, an anonymous group of hackers released a new version of Trinoo that could allow assailants to infiltrate a system through an innocent-looking e-mail attachment—a type of Trojan horse virus. Whereas the original tools were largely limited to UNIX and UNIX-like systems, the latest release can penetrate more popular consumer platforms, placing a far greater number of machines in peril of becoming daemons.

### Increasing security awareness

One positive effect from the publicized rash of attacks is the heightened awareness of online dangers. Modern society as a whole has started to realize the grave risks that accompany the

(continued on next page)

---

## Hackers Exploit Internet Vulnerabilities

Sophisticated new attacks lack effective defense, demand vigilant security precautions

(continued from preceding page)

enhanced efficiency and convenience that information systems provide.

In March 1998, the University of Minnesota experienced a type of DoS assault known as a “smurf” attack, which resulted in data loss and slow connections across the state. Only three months before, the Computer Emergency Response Team (CERT) Coordination Center at Carnegie-Mellon University published an advisory warning about such attacks and offering guidelines to protect against them. Similar advisories appeared on the CERT web site in December 1999, cautioning the public about the new distributed denial-of-service attacks, and many computer security teams began gearing up to fight a potential onslaught of DDoS assaults during the holiday season. Still, it required the crippling of Internet giants to gain the public’s attention.

According to a representative for the Software Engineering Institute, the federally funded research and development center that sponsors the CERT/CC and its web site, the site has experienced a significant increase in traffic since the February attacks. “We typically do when there’s a well-publicized event like that. When we released the advisory last March on the Melissa virus, we had about 500,000 downloads of that advisory,” he said. Society’s reactive mode, however, may be changing. “The cumulative effect of some of these stories has been raising people’s awareness of security issues.”

One of the security dangers revealed by the DDoS attacks, for instance, is the heightened security risk associated with high-speed Internet connections, such as digital subscriber lines (DSLs) and cable modems. Some computer vandals routinely target the Internet addresses of DSL and cable providers, searching for machines that they can access. Unlike standard modems, DSLs and cable modems remain connected to the Internet any time the machine is turned on, which provides hackers a greater window of opportuni-

ty to wreak their mischief. Their superior speed also makes these Internet connections a more desirable vehicle to launch an attack.

Two weeks after installing a DSL on his home computer, a scientist at an East Coast-based research firm read a book on network security and decided to check the security of his own system. He was shocked to discover that someone had accessed his computer via the Internet and set it up to accept commands from a remote system. Ultimately, the man had to reinstall all of his computer software, including the operating system.

### Rapid response to the attacks

Initial reports of the attacks led the federal government to launch an immediate investigation. Seven FBI field offices opened cases involving the DDoS assaults, with the remaining FBI offices supporting those seven. This vast network of investigative power tracked down hundreds of leads. Meanwhile, the National Infrastructure Protection Center (NIPC), an interagency center located at the FBI, coordinated the nationwide investigation, analyzing logs from victimized sites and their Internet service providers (ISPs) and offering analytical assistance to field offices. Close cooperation between the FBI, the U.S. Department of Justice and the Royal Canadian Mounted Police (RCMP) led to last month’s arrest of a Canadian teenager in connection with the attacks.

Within days of the highly publicized assaults, several organizations started posting software capable of identifying a DoS attack. News reports alerted the public to a defensive tool available on the NIPC web site since December 1999 and reissued after the start of the February assaults. This tool examines the software on a computer, searching for telltale signs of the attack software—similar to the methods used by anti-virus programs.

Law enforcement agencies are not the only ones who have responded with speed. Less than one week after the initial flurry of DDoS attacks, reports emerged about new versions of attack soft-

---

ware based on Trinoo and TFN, which can elude the defense software publicly posted. Upon identifying an information packet from a particular address as garbage, the target computer blocks incoming correspondence from that address. Hackers circumvent this defense by instructing their zombies to change the address each time, forcing the victim computer to analyze each incoming packet of information. Any computer user who has experienced a problem with junk e-mail has encountered this dilemma; blocking e-mail from “junksender001” does not stop mail from “junksender002.”

This development further illustrates why network security specialists can never become complacent. Just as IT professionals constantly strive to plug security vulnerabilities, hackers—whether out of malice or simply for sport—continue to develop creative methods of causing electronic mayhem.

### **Effects of DoS assaults**

In terms of information security, DoS assaults pose primarily a nuisance to the target system or network. One computer expert describes the attacks as “the equivalent of somebody blockading the entrance to a building.” Someone can prevent entry to a structure without having access to the inside. “The attackers do not have access to your web site, nor do they have access to data, user names or anything else,” he says. Yet, this knowledge often serves as cold comfort for organizations whose web sites are disabled for extended periods of time.

If the crippled web sites deal in electronic commerce, for instance, the annoyance can translate into lost business and, ultimately, decreased market share. Indeed, studies show that the spate of DoS attacks has given many Internet users pause regarding online shopping. A recent Gallup poll reveals that one-third of online adults in the United States are now less likely to make a purchase over the Internet. Among users who had not purchased anything online in the last three months, nearly 47 percent express a reluctance to

shop on the Internet now, and almost 60 percent of respondents report increased privacy concerns. The assaults can also have negative ramifications for victimized companies not involved with Internet commerce in terms of lowered customer confidence; the majority of online consumers feel that electronic industry holds the primary responsibility for preventing such attacks.

The DoS assaults can also cause additional problems. Because the programs used in these attacks randomly generate spoofed addresses, they can inadvertently supply valid addresses. In such cases, the system or network to which the address legitimately belongs will receive information packets that it cannot process, which can result in yet another system disruption. Another negative consequence can arise when the target of the DoS attack screens out “hostile” addresses. If the rightful owner of the spoofed address attempts to connect with the attack victim, the targeted system will block communication from the other machine, identifying it as part of the DoS attack. As more machines gain access to the Internet, the growing congestion among addresses will increase the likelihood of these accidental impostors.

### **Guarding against DoS attacks**

The bad news is that few defenses can thwart a DoS attack. On the other hand, organizations and individuals can decrease the likelihood that their systems will be used in executing such an assault.

According to computer experts, most attackers use automated programs that scan for known vulnerabilities, many of which can be easily fixed. In fact, the author of TFN and its sequel, TFN2K, published a working version of TFN on several security sites shortly after its development; he wanted to make the information public and generate awareness of such programs. Unfortunately, too many organizations do not routinely search for security alerts and patches, thus ignoring valuable assistance in the constant battle for information

**(continued on next page)**

## Hackers Exploit Internet Vulnerabilities

Sophisticated new attacks lack effective defense, demand vigilant security precautions

(continued from preceding page)

security. Intrusion detection systems and firewalls can serve as important elements of a network security program, but organizations cannot rely upon an off-the-shelf product to protect their systems. Commissioning a proprietary firewall or customizing a commercial product, for instance, helps reduce an intruder's ability to capitalize on a well-known vulnerability. Information security managers should sweep the Internet and industry publications continuously to learn about the latest threats so they can plan a defense.

In addition to staying abreast of published threats and solutions, IT departments can protect an organization's networks with continuous vigilance—day to day, week to week and month to month. Important security measures include the following: “sniffing” or searching for suspicious information packets within the network; examining network statistics that reveal unexpected fluctuations in traffic; filtering incoming e-mail for virus attachments; and analyzing system performance statistics in search of anomalies.

Another defensive element entails filtering outgoing information to prevent forged information packets from leaving the network. As mentioned above, many of these attacks involve directing a machine to submit incorrect source addresses, which ties up the target computer as it attempts to respond to the phony address. Network administrators can configure their systems to forward only packets with valid addresses that belong to their network. This task must be executed at every egress point in the network, particularly at the external Internet connections and with the upstream provider. This precaution, however, only prevents transmission of spoofed information packets; it does not prevent the network from sending packets with valid addresses.

Most individuals do not possess this technical expertise, but several measures can reduce the chances of hackers turning their computers into daemons or zombies:

- Disable the file and print sharing features on their computers. Instructions for this task should be available in the operating system manual.
- Visit web sites that post information and tools on Internet security, such as [www.cert.org](http://www.cert.org) and [www.sans.org](http://www.sans.org). Both the CERT/CC and the SANS (System Administration, Networking and Security) Institute are non-profit organizations that educate computer and security professionals about system vulnerabilities and security solutions.
- Use caution when downloading and executing any e-mail attachments. Ensure the attachments come from a reliable source, and scan them with an anti-virus program before opening.
- Disable Internet connections when not in use. If using a cable modem or a DSL, turn off the modem to break the connection.
- Purchase a reliable anti-virus scanner, and update it regularly to ensure that it can identify the latest known virus threats.

*New, sophisticated DDoS attacks have shut down some of the most prominent presences on the Internet. These well-publicized assaults demonstrate the increasing dangers of the electronic Information Age—particularly since no defense can effectively stop them. Modern society's growing dependence on computers and the interconnectivity of the Internet demands a close alliance between security directors and IT professionals. Until organizations recognize the critical need to include security in all technology endeavors, computer criminals will always have the upper hand.*



The Lipman Report Editors