

[Register](#)
[Subscribe](#)



BusinessWeek online

Search

Advanced Search

[BW MAGAZINE](#)
[DAILY BRIEFING](#)
[INVESTING](#)
[GLOBAL BUSINESS](#)
[TECHNOLOGY](#)
[SMALL BUSINESS](#)
[B-SCHOOLS](#)

OCTOBER 30, 2002

OCTOBER

► **TECHNOLOGY**

SECURITY NET

By Alex Salkever

MARKET

[DJIA](#)
[Nasdaq](#)
[S&P 500](#)
[Create / Chk](#)
[Launch Pop](#)

Stock Look

Enter name

[Recent Tech Features](#)
[Tech Special Reports](#)

[E.Biz](#)
[Product Reviews](#)
[Internet Security](#)
[Science & Health](#)

[Tech Columns](#)

LIFESTYLE
COLUMNS
FORUMS & CHATS
NEWSLETTERS
PERSONAL FINANCE
SEARCH & BROWSE
SPECIAL REPORTS
TOOLS & SCOREBOARDS
VIDEO VIEWS

CRM Resource Center
sponsored by:

[Customer Service](#)
[Contact Us](#)
[Advertising](#)
[Media Kit](#)
[Special Ad Sections](#)
[Conferences](#)
[Permissions & Reprints](#)
[Marketplace](#)

The Day the Net Nearly Choked

On Oct. 21 a cyber-attack threatened to overwhelm it. Here's what happened and what's needed to make sure it doesn't happen again

The newsgroups and chat rooms in the computer-security biz are still buzzing about the Oct. 21 distributed denial of service attack (DDOS) that tried to clog the heart of the Internet. That attack used a constellation of hijacked computers to unleash a surging wave of bogus data traffic aimed at the 13 so-called root-level domain name servers (DNS) that function as the authoritative directory assistance for the Internet. Taking down these geographically dispersed servers, three of which are located outside the U.S., in Sweden, Britain, and Japan, would be the digital equivalent of turning off the traffic signals in Manhattan at rush hour.

► [Printer-Friendly Version](#)

► [E-Mail This Story](#)

RELATED ITEMS

[Security Net Archive](#)

• [Find More Stories Like This](#)

TODAY'S HEADLINES

[Tech in 2002: A Time of Tumult](#)

[China Tops Asia's Year in Tech](#)

[CSC: Big Eyes for Uncle Sam's IT Pie](#)

[Return of the Star Wars Fantasy](#)

[A Basket of "January Bounce" Stocks](#)

[John Malone's New Year Resolution](#)

[The Man Who Redefined Management](#)

[Peter Drucker's Search for Community](#)

[Still Eyeless in Gaza](#)

[The Winners and Wipeouts of 2002](#)

[Guangzhou Daily: Rag to Riches](#)

[Yoox: Discounted Luxury](#)

[Hollywood's Digital Love/Hate Story](#)

• [More Headlines](#)

Story Continues Below Ad



Dissatisfied With Your Money Manager?

How dissatisfied are you with your current money manager?

- ☐ Very dissatisfied
☐ Somewhat dissatisfied
☐ Neutral
☐ Somewhat satisfied
☐ Very satisfied

submit

So was it a virtual Armageddon or just worrisome cyber-vandalism? Both of the above. It turned out to be no big

deal because the Internet handled the attack just fine, thank you. Nine of the 13 servers went down at various points during the attack, but disruptions to Web surfing were small, with page-loading delays of a second or two.

On the other hand, it was the worst assault yet because it illustrated more clearly than ever how even unschooled hackers sporting facile strategies could get so close to wreaking serious havoc. "The message here is that it's not that difficult to cause a massive disruption even to root servers. The last time it was done, it was a 13-year-old," says Mark Rasch, an executive senior vice-president at Net security firm Solutionary in Omaha, Neb.

UNKNOWN COMMANDER. To date, no one had tried to take down all 13 root-level DNS servers at once. Even if it was a relatively obvious strategy, the out-of-the-blue nature of this attack proves that more needs to be done to stop DDOS assaults. Luckily, that shouldn't be very hard to do with a little coordination and a some extra work.

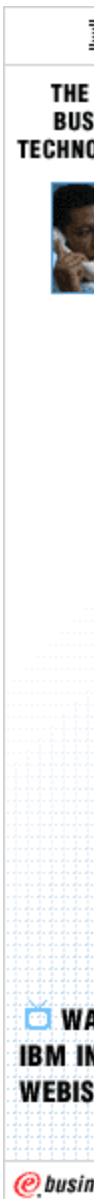
Here's a quick overview of what happened on Oct. 21. Someone (or some group), somewhere -- exactly who remains unknown and at large -- activitated a command that told a still unclear number of computers to start bombarding the 13 root servers with so called ICMP (Internet control message protocol) messages. ICMP messages are data packets that contain information about control, error, and other network minutiae. They're mostly used to confirm that a computer is in fact connected to the Internet and to check how fast the connection is.

When you send an ICMP packet aimed at another computer to find out if it's on a network, that's described as "pinging" the computer. DDOS attacks using ICMP are called "ping floods." They work by overwhelming the big data pipes flowing into the target with bogus ping queries, clogging the pipe and effectively making the target computer inaccessible on the Net.

EASY TO COUNTER. Ping floods are considered unsophisticated. They're generally easy to spot, as the traffic volume of ping queries will quickly soar beyond any normal level. In most cases, ping floods aren't too hard to deal with, given the willingness of the various data carriers and big Internet service providers to open and close ports on their network and filter out large volumes of ICMP queries that may or may not be valid.

However, a ping flood aimed at root servers isn't so simple to defend against. Says Bill Hancock, vice-president for security at Web-hosting giant Exodus, a subsidiary of Cable & Wireless: "Any attack against a DNS of any kind is dangerous because you can't deal with a DDOS attack as you would a DDOS against any other machine."

DDOS attacks typically target one or more servers that are hosting a particular Web site, say BusinessWeek Online. Hackers who surreptitiously take control of hundreds or thousands of PCs use them to



send repeated Web-page requests to businessweek.com's servers until the servers can no longer keep up -- and poof! -- BusinessWeek Online becomes unavailable to real readers.

I NEED YOUR ADDRESS. An attack on a root server, however, is far more dangerous. That's because these DNS servers are the Net's basic traffic directors, sending information to all other servers, say at ISPs or corporate offices, about just which Web sites are available at what specific Internet protocol addresses (the numbers that servers use to identify one another). Many ISPs and Web-hosting companies maintain their own DNS servers to help their customers find Web sites more quickly. Those are considered low-level DNS servers.

When they need to update their DNS listings, or if they receive queries for Web sites they can't find, those low-level DNS servers usually ask higher-level DNS servers for information. Higher-level DNS servers maintain listings for domain names ending in suffixes like .com or .net, or for country listings such as Web addresses ending in .jp for Japan.

At the very top of the DNS hierarchy are the root-level servers. They disseminate changes in DNS information to the rest of the Internet and are the directory assistance of last resort for the entire Net. If the root servers become overwhelmed with false requests for information about other servers on the Internet, the Internet itself would eventually slow to a crawl -- and, worst case, goes offline -- as Web browsers and DNS servers could no longer get the necessary information to connect to Web sites such as businessweek.com.

"ZOMBIES." The importance of root-level DNS servers also makes it harder to use a common strategy in fighting off DDOS attacks, which is simply changing the IP address of the target and letting the offending data traffic fall into a black hole. That's how Bush Administration techies headed off a DDOS assault on WhiteHouse.gov in August, 2001. The upshot? Even a ping flood becomes more serious when it's aimed at root DNS boxes.

So what to do? A number of suggestions are floating around right now. One is mandatory firewalls on any PC attached to a broadband connection and not actively managed by a system administrator. For the most part, that measure would be targeted at consumers using broadband ISPs. Many of today's software firewalls can spot and block DDOS attacks that would originate from a consumer's machine if a hacker had managed to turn it into a so-called "Zombie," or a computer that had been compromised and could be drafted into a digital army to remotely launch a DDOS attack.

Another proposal is mandatory "source authentication" for all ISPs. That means ISPs should check any traffic originating from their users to make sure that their machines' IP addresses, which are included in the header of data packets, matches their machines' actual IP address. It's the equivalent of checking the identity papers of each packet of data to make sure that it

wasn't "spoofed" or faked. Spoofing is a common practice in DDOS attacks, which makes spotting their origin particularly difficult.

BE MORE RESPONSIBLE. "Some ISPs have turned on some source authentication, but no one has made a publicly visible commitment to doing it from stem to stern," says Paul Vixie, chairman of the board of directors of the Internet Software Consortium, a nonprofit that operates one of the 13 root-level servers.

Another suggestion is to force ISPs to install anti-DDOS equipment from companies such as WebScreen, Mazu Networks, Asta Networks, and Arbor Networks. These specialized computers use exotic algorithms to screen out DDOS traffic before it enters a network. This suggestion is meant to force ISPs to use better practices and make them take more responsibility for a phenomenon that causes ISPs little direct pain but can significantly degrade the overall Internet.

Yet another proposal is government intervention. One possibility is a federally funded early-warning system that looks at the whole Internet for signs of trouble. Something like this is already under consideration.

INTERNET FIREMEN? Taking that a step further would be an authoritative office that could coordinate ISP responses to big DDOS attacks. The rationale here is that ISPs will respond in ways to keep their customers happy, but such responses may not contribute to keeping the entire Internet running smoothly. "We're talking about someone who can act as playground coordinator," says Tom Ohlsson, vice-president for marketing at Internet traffic-tracking outfit MatrixNet Systems in Austin, Tex.

A more radical solution would be setting up a dedicated government network designed to step in and pick up key Net functions in case of real emergencies. That would cost billions and require a trained staff that would probably not do much of anything most of the time, sort of like Internet firemen. Still, "How much money would it have been worth to put a Harrier jump jet on the roof of the World Trade Center. The answer is none -- except on September 11," says Rasch.

Each of these possible solutions has a weakness. Firewalls on desktops might prove worthless over time as savvy DDOS hackers work around them. Source authentication works only when someone is directly connected to the Net, so anyone who's on a network that's behind a router -- which is increasingly common these days -- might be hard to authenticate. Forcing ISPs to install these tools doesn't mean they'll get used if they have no direct benefit to customers.

Does that mean those steps don't make sense? Firewalls and mandatory source authentication certainly do. That said, I think government intervention is necessary at some level to coordinate responses. The Internet community is pretty good at blocking DDOS attacks right now, but it might be able to do better if an equivalent of the Federal Emergency Management Agency existed for the Internet. It sure would be more

comforting knowing someone is always watching over the whole thing, ready to coordinate a rescue whenever necessary.

[Salkever](#) is Technology editor for BusinessWeek Online and covers computer security issues weekly in his [Security Net](#)

Click to buy an [e-print or reprint](#) of a *BusinessWeek* or BusinessWeek Online story.

To subscribe online to *BusinessWeek* magazine, please [click here](#).



[BACK TO TOP](#)