washingtonpost.com Personalize Your Post | Go to mywashingtonpost.com
Home News OnPolitics Entertainment Live Online Camera Works Marketplace Jobs
TechNews.com DAILY TECH E-LETTER | ARCHIVES SEARCH: News GO Search Options

Technology Home
Washtech
Tech Policy
-Copyright
-Cybercrime
-FCC
-ICANN
-Security
Government IT
Markets
Columnists
Personal Tech
Special Reports
Jobs
washingtonpost.com
More News

CO. POSTINGS:
- Get Quotes
- Tech Almanac

Attack On Internet Called Largest Ever

By David McGuire and Brian Krebs
washingtonpost.com Staff Writers
Tuesday, October 22, 2002; 5:40 PM

The heart of the Internet sustained its largest and most sophisticated attack ever, starting late Monday, according to officials at key online backbone organizations.

Around 5:00 p.m. EDT on Monday, a "distributed denial of service" (DDOS) attack struck the 13 "root servers" that provide the primary roadmap for almost all Internet communications. Despite the scale of the attack, which lasted about an hour, Internet users worldwide were largely unaffected, experts said.

FBI officials would not speculate on who might have planned or carried out the attack.

David Wray, a spokesman for the FBI's National Infrastructure Protection Center (NIPC), said the bureau is "aware of the reports and looking into it."

DDOS attacks overwhelm networks with an onslaught of data until they cannot be used. According to security experts, the incident probably was the result of multiple attacks, in which attackers concentrate the power of many computers against a single network to prevent it from operating.

"This was the largest and most complex DDOS attack ever against the root server system," said a source at one of the organizations responsible for operating the root servers.

Ordinary Internet users experienced no slowdowns or outages because of safeguards built into the Internet's architecture. A longer, more extensive attack could have seriously damaged worldwide electronic communications, the source said.

Internet Software Consortium Inc. Chairman Paul Vixie said that if more servers went down, and if the hackers sustained their hour-long strike a bit longer, Internet users around the world would have begun to see delays

-----Related Coverage-----
- White House Slows Cybersecurity Planning (TechNews.com, Sep 16, 2002)
- White House Officials Debating Rules for Cyberwarfare (The Washington Post, Aug 22, 2002)
- Getting to the Root of All E-Mail (The Washington Post, Mar 29, 2002)
- Internet Vulnerable to Terrorists, Experts Warn (The Washington Post, Sep 28, 2001)

-----Web Special-----
- Cybersecurity and You: Five Tips Every Consumer Should Know (TechNews.com, Sep 18, 2002)
- A Cybersecurity Primer: Links and Resources for Computer Users
- A Short History of Computer Viruses and Attacks (TechNews.com, Sep 18, 2002)
- Key Players in U.S. Government's Cybersecurity Efforts (TechNews.com, Sep 18, 2002)

-----Cybersecurity-----
- SBC Says It Will Test Internet Security Measures (Associated Press, Nov 3, 2002)
- Attacks Exposed Internet's Vulnerabilities (TechNews.com, Oct 31, 2002)
- More Than One Internet Attack Occurred Monday (TechNews.com, Oct 23, 2002)
- More Security News

-----OnPolitics-----
- Today's Political News
- Elections 2002 Coverage
- Daily E-mail Updates

-----TechNews.com-----
- Sign-up for the weekly tech policy e-letter (Delivered every Monday).

-----Full Coverage-----
- More National Security News

and failed connections.

E-Mail This Article
Printer-Friendly Version
Subscribe to print edition

Chris Morrow, network security engineer for UUNET, said "This is probably the most concerted attack against the Internet infrastructure that we've seen." UUNET is the service provider for two of the world's 13 root servers. A unit of WorldCom Inc., it also handles approximately half of the world's Internet traffic.

DDOS attacks are some of the most common and easiest to perpetrate, but the size and scope of Monday's strike set it apart.

Vixie said only four or five of the 13 servers were able to withstand the attack and remain available to legitimate Internet traffic throughout the strike. "It was an attack against all 13 servers, which is a little more rare than an attack against any one of us," he said.

The server Vixie operates was available throughout the attack, he said.

Internet addressing giant VeriSign Inc., which operates the most important server from an undisclosed Northern Virginia location, reported no outages.

"VeriSign expects that these sort of attacks will happen and VeriSign was prepared," company spokesman Brian O'Shaughnessy said.

Vixie said he was unwilling to compare the attack to others he has witnessed in more than two decades of involvement with Internet architecture, but said it was "the largest in recent memory."

The root servers, about 10 of which are located in the United States, serve as a sort of master directory for the Internet.

The Domain Name System (DNS), which converts complex Internet protocol addressing codes into the words and names that form e-mail and Web addresses, relies on the servers to tell computers around the world how to reach key Internet domains.

At the top of the root server hierarchy is the "A" root server, which every 12 hours generates a critical file that tells the other 12 servers what Internet domains exist and where they can be found.

VeriSign manages its servers under contracts with the Commerce Department and the Internet Corporation for Assigned Numbers (ICANN), which manages the DNS.

One rung below the root servers in the Internet hierarchy are the servers that house Internet domains such as dot-com, dot-biz and dot-info.

The DNS is built so that eight or more of the world's 13 root servers must fail before ordinary Internet users start to see slowdowns.

"There are various kinds of attacks all the time on all sorts of infrastructure, and the basic design of the Internet is such that it is designed to withstand those attacks," said ICANN Vice President Louis Touton. "We're not aware of any users that were in any way affected.

"Obviously the prevalence of attacks does make it important to have increased focus on the need for security and stability of the Internet," he added.

Most often, the computers used in the DDOS assaults have been commandeered by hackers either manually or remotely with the help of automated software tools that scan millions of computers for known security holes. These computers often belong to unsuspecting home users.

Little can be done to insulate targets from such attacks, and some of the world's most powerful companies have been targeted in the past. In February 2000, Amazon.com, eBay, Yahoo, and a host of other big-name e-commerce sites came to a grinding halt for several hours due to DDOS attacks.

"Only the richest can defend themselves against this type of attack, and most of them can't withstand a concerted attack," said Alan Paller, research director at the SANS Institute, a nonprofit security research and training group that often works with federal investigators to track computer virus writers. Paller also was the lead expert witness at the trial of "Mafiaboy," the Canadian teenager who was ultimately convicted of the February 2000 attacks.

"The only way to stop such attacks is to fix the vulnerabilities on the machines that ultimately get taken over and used to launch them," Paller said. "There's no defense once the machines are under the attacker's control."

Vixie said he kept the server at Internet Software Consortium operating by "pushing" the flood of data far enough away from his servers that legitimate traffic could flow around the obstruction. Such clogs still affect some Internet users by gumming up Internet communications somewhere else in the network.

UUNET's Morrow said it is too early to tell what the attack bodes for the Internet in coming months. "This could be someone just messing around, but it could also be something much more serious. It's too soon to say," Morrow said.

washingtonpost.com Staff Writer Robert MacMillan contributed to this article. The reporters can be e-mailed at brian.krebs@washingtonpost.com, david.mcguire@washingtonpost.com, robert.macmillan@washingtonpost.com.

TechNews.com Home

Techway Events: Techfast Live | Fast 50
Company Postings: Quick Quotes | Tech Almanac
About TechNews.com | Advertising | Contact TechNews.com | Privacy
My Profile | Reprints | Subscribe to print edition | Syndication

washingtonpost.com Personalize Your Post | Go to mywashingtonpost.com
Home News OnPolitics Entertainment Live Online Camera Works Marketplace Jobs