



COMPUTERWORLD

[Home](#) [News](#) [Topics](#) [Departments](#) [Services](#) [Subscriptions](#) [Events](#)

You may retrieve this story by entering QuickLink# 28639

► [Return to story](#)

Denial-of-service attacks still a threat

By [JAIKUMAR VIJAYAN](#)
APR 08, 2002

Denial-of-service (DOS) attacks continue to present a significant security threat to corporations two years after a spate of incidents brought down several high-profile sites, including those of Yahoo Inc. and eBay Inc., users and analysts report.

Since then, several technologies have emerged that help users detect and respond to DOS attacks far more quickly and effectively than before. But the increasingly sophisticated attack methods and the growing range of systems targeted in DOS attacks continue to pose a challenge. "In that sense, the tools are always only trying to catch up" with the threat, said Raj Raghavan, a vice president at SiegeWorks Enterprise Security Solutions, a Pleasanton, Calif.-based integrator of security technologies.

DOS attacks make computer systems inaccessible by flooding servers or networks with useless traffic so that legitimate users can no longer gain access to those resources. In distributed DOS (DDOS) attacks, malicious hackers use hundreds and sometimes even thousands of previously compromised computer systems to launch assaults against a network or server.

During a three-week period in mid-2001, researchers from the University of California, San Diego, detected approximately 12,800 DOS attacks against more than 5,000 targets. Recent examples include attacks against the World Economic Forum's Web site in February ([see story](#)) as well as those that drove British Internet service provider CloudNine Communications out of business earlier this year.

Increasing Menace

"The threat is a lot worse today than two years ago," said Harris Miller, president of the Information Technology Association of America (ITAA) in Arlington, Va. "There are lots of indications that since Sept. 11, the number of DOS attacks have greatly increased."

The ITAA is acting as the coordinator of an industry body called the IT Information Sharing and Analysis Center, which was created early last year to share information and find ways of dealing with DOS and other security threats.

Part of the problem with DOS attacks is the sheer number of ways in which they can operate, said Pete Lindstrom, an analyst at Framingham, Mass.-based Hurwitz Group Inc. A DOS attack can be launched to overwhelm a target's Web site, CPU, memory, network bandwidth or routers. It can also work by taking advantage of known flaws in products, Lindstrom said.

Degradation-of-service attacks are another variation. Such assaults, which are more difficult to detect than other DOS attacks, involve short-lived bursts of spurious traffic directed at a target from multiple sources and are aimed at slowing network performance.

"It would be a fairly straightforward issue to handle if such attacks originated and terminated with the same network," said Jeff Ogden, director of high-performance networks at Ann Arbor, Mich.-based Internet service provider Merit Network Inc.

The problem arises because almost all DOS attacks involve multiple networks and attack sources, many of which have spoofed IP addresses to make detection even harder, according to Ogden.

So completely choking off the offending traffic requires network administrators to call upstream service providers, alerting them to the attack and having them shut down the traffic. That process has to be repeated all the way back to every attack source.

Tips to Help Prevent a DOS Attack

- **Regularly review** publicly available information on recent security vulnerabilities and incidents. It helps in configuring and updating your public Web server against new forms of attacks.

- **Regularly update** your DOS detection tools to discover new patterns or events (resulting from new or updated attacks taking advantage of new vulnerabilities).

- **Update** firewall-filtering mechanisms to deny new attacks.

- **Temporarily disable** specific services that might be vulnerable.

- **Augment** your alerting procedures.

- **Work** with your Internet service provider to understand what precautions have been taken to guard against DOS attacks.

- **Get** a configuration that uses multiple connections built from different network backbones. This will help switch public Web servers to another connection in the event of a DDOS attack.

Source: CERT Coordination Center at Carnegie Mellon University, Pittsburgh

Read accompanying story:

- [Cost, Other Priorities Stall Use of DOS Detection/Response Tools](#)

Related stories:

- [Cybersleuthing solves the case](#), Jan. 14, 2002
- [U.S.-China cyberwar a dud, but trouble lingers](#), May 11, 2001

Source: Computerworld

Sponsored Links

Sun and Oracle -- FREE Database Cluster Solutions iSeminar

Sys Admins - Upgrade Your Site to 128 bit SSL Encryption

Avaya's ECLIPS Portfolio Standards-based IP Telephony Solutions

[About Us](#) [Contacts](#) [Editorial Calendar](#) [Help Desk](#) [Advertise](#) [Privacy Policy](#)

Get Smart About E-commerce.

COMPUTERWORLD
Knowledge Centers

Copyright © 2002 Computerworld Inc. All rights reserved. Reproduction in whole or in part in any form or medium without express [written permission](#) of Computerworld Inc. is prohibited. Computerworld and Computerworld.com and the respective logos are trademarks of International Data Group Inc.