

Cost, Other Priorities Stall Use of DOS Detection/Response Tools

By JAIKUMAR VIJAYAN
APR 08, 2002

Several vendors offer early-detection and response tools for dealing with DOS attacks. The main focus of such technologies is to quickly give IT managers the information needed to filter out malicious traffic while letting in legitimate users.

Just last week, for instance, Waltham, Mass.-based Arbor Networks Inc. launched an enhanced version of its Peakflow DoS software that uses network information gathered from a user's Cisco Systems Inc. firewall to identify and filter out bad traffic.

Arbor's Peakflow DoS software is just one in a growing list of products available. Other products include the following:

• DDoS Enforcer from Mazu Networks Inc. in Cambridge, Mass.

• Attack Mitigator from Top Layer Networks Inc. in Westboro, Mass.

• Vantage System from Asta Networks Inc. in Seattle.

• CaptIO from Captus Networks Corp. in Woodland, Calif.

Most of these products work by comparing live network traffic against some previously defined baseline and by alerting users if there is a significant divergence from that baseline. The alerts might be based on a comparison of byte or packet rates, traffic that's directed at specific resources, traffic that originates from specific IP addresses or spikes in network traffic.

Despite the early-detection capabilities offered by such technologies, user adoption so far appears to be very slow, said Michael Rasmussen, an analyst at Cambridge, Mass.-based Giga Information Group Inc.

For one thing, the tools aren't cheap. Deploying some of these products can mean shelling out anywhere from $75,000 at the low end to more than $1 million for a large enterprise installation. The tools are most effective only when they are installed not just on the edge of corporate networks, but also in service provider networks as well, analysts said.

Many companies also have their hands full dealing with other security, regulatory and privacy issues and may be giving a lower priority to DOS threats, Rasmussen said.

"The DOS threat is just one of the security issues that users are worried about," agreed Charles Kolodgy, an analyst at Framingham, Mass.-based IDC.

House of Blues Entertainment Inc. in Los Angeles exemplifies that point. Although the company would like to have a DOS tool in place, it has no plans to do so right now because of other priorities, said Steve LaBrie, director of network operations. "I'm concerned about DOS, but it is not fiscally viable to roll out anything now," he said.

Many companies have already beefed up their firewalls, intrusion-detection systems and load-balancing capabilities against DOS threats and therefore may be reluctant to deploy separate anti-DOS technology, analysts said.

Read accompanying story:

- Denial-of-Service Attacks Still a Threat

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

Find IT solutions fast.

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.