



Media and Investors

Michael Doherty
Covad Communications
408-952-7431
mdoherty@covad.com

Media Contact

Christian Pinkston
Pinkston Group
703-994-4235
pinkston@pinkstongroup.com

Covad Enhances Network Protection Against Denial of Service and Bot and Worm Attacks

*Company also serves as active member of Fingerprint Sharing Alliance
to more easily resolve cross-company network threats*

San Jose, Calif. – February 19, 2008 – Covad Communications Group Inc., (AMEX: DVW), a leading national provider of integrated voice and data communications, today announced that it has deployed Arbor Network's Peakflow® SP software solution. This network enhancement is designed to protect Covad's network against distributed denial of service (DDoS) attacks, worms, and other network vulnerabilities and routing instabilities. The latter includes hacker-controlled botnets that can be used to attack a Website or network on command. This network enhancement helps to protect all of Covad's customers at no additional cost to them. In addition to deploying the software solution, Covad also serves as an active member of the Fingerprint Sharing Alliance (FSA), a global coalition of Arbor's telecommunications customers that have joined together to prevent cyber attacks that cross service provider and national boundaries.

"Continuing to ensure the integrity of our nationwide network is of the utmost importance as we deliver innovative and outstanding services to our customers," said Dr. Ron Marquardt, chief technology officer for Covad. "This network enhancement and membership in the FSA improves our traffic monitoring capability and has enabled Covad to save customers and partners thousands of dollars in losses due to security incidents."

"Given the global nature of distributed denial of service attacks, it is critical for service providers to work together and collaborate in order to stop these attacks as close to the source as possible," said Paul Morville, Arbor Networks vice president of product management. "Service providers are increasingly interconnected and the Fingerprint Sharing Alliance has put in place an automated framework that dramatically speeds time to resolution."

Denial of Service and bot and worm attacks are among the most costly security attacks suffered by businesses and other organizations that rely on IP communications. The 2007 Computer Crime and Security Survey released by the Computer Security Institute reported the following:

- 25 percent of respondents reported a denial of service attack, with total respondent losses approaching \$2.9 million;
- 21 percent of respondents reported a Bot attack, with total respondent losses approaching \$2.9 million;
- 52 percent of respondents reported a virus attack (including worm attacks), with total respondent losses of approximately \$8.4 million.



Covad deployed Arbor's Peakflow SP platform solution to analyze its transit, peering and routing traffic. Arbor's Peakflow SP will also assist in proactively detecting, tracing and mitigating network-wide anomalies and attacks. These solutions will help Covad resolve DoS attacks and worms before they affect its network. This proactive response translates to tangible customer benefits including higher network availability and reduced exposure to common Internet threats.

As a member of the FSA, Covad benefits from the sharing of cyber attack profiles, or "fingerprints", to stop attacks more quickly and closer to the source. The FSA is the first effort in which telecommunications companies have been able to share attack profiles automatically, allowing providers to consistently protect one another and their customers from security threats. With the formation of the FSA, a formerly laborious and tedious process has been replaced with an efficient and automated process, and a larger community can be engaged to solve significant threats to the Internet.

For more detail on how Covad is leveraging Arbor Networks' technology in tandem with the Fingerprint Sharing Alliance (FSA), please visit Arbor Networks' website to read the [Solution Brief Case Study](#) or to download the [podcast](#) discussion with Dr. Marquardt.

In addition to these network and industry initiatives Covad also provides enhanced security options directly to its customers. Covad previously announced that it has entered into an agreement that allows Covad to bundle McAfee® Total Protection for Small Business services with Covad's award-winning broadband products to provide small business customers with a simple, affordable solution to meet their security needs. For more information, visit www.covad.com/services/business_essentials/ or call 1-888-GO-COVAD.

###

About Covad

Covad is a leading nationwide provider of integrated voice and data communications. The company offers DSL, Voice Over IP, T1, broadband wireless, Web hosting, managed security, IP and dial-up, and bundled voice and data services directly through Covad's network and through Internet Service Providers, value-added resellers, telecommunications carriers and affinity groups to small and medium-sized businesses and home users. Covad broadband services are currently available across the nation in 44 states and 235 Metropolitan Statistical Areas (MSAs) and can be purchased by more than 57 million homes and businesses, which represent over 50 percent of all US homes and businesses. Corporate headquarters is located at 110 Rio Robles San Jose, CA 95134. Telephone: 1-888-GO-COVAD. Web Site: www.covad.com.

Safe Harbor Statement under the Private Securities Litigation Reform Act of 1995:

The foregoing contains "forward-looking statements" which are based on management's current information and beliefs as well as on a number of assumptions concerning future events made by management. Examples of forward-looking statements include Covad's ability to protect its network from malicious attacks, viruses, worms and bots, as well as Covad's ability to successfully resell



McAfee products. Readers are cautioned not to put undue reliance on such forward-looking statements, which are not a guarantee of performance and are subject to a number of uncertainties and other factors, many of which are outside Covad's control that could cause actual results to differ materially from such statements. These risk factors include our ability to rapidly expand and deploy these services, changes in Granite's strategy and changes in technologies, among other risks. For a more detailed description of the risk factors that could cause such a difference, please see Covad's 10-K, 10-Q, 8-K and other filings with the Securities and Exchange Commission. Covad disclaims any intention or obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise.

###