GLOBAL ALLIANCE FORMS TO THWART INTERNET ATTACKS

Submitted by: Folliard
Tuesday, 29 March 2005

Arbor Networks achieves global cooperation of telecom companies; British Telecom, MCI, NTT Com work together to fight cyber attacks

London, 29 March 2005

Arbor Networks, a leader in network security, today announced the Fingerprint Sharing Alliance, a first-of-its-kind industry initiative aimed at helping network operators share Internet attack information automatically. The Fingerprint Sharing Alliance marks the first time companies are able to share detailed attack profiles in real-time and block attacks closer to the source. This global alliance marks a significant step forward in the fight against Internet attacks and major infrastructure threats that cross network boundaries, continents and oceans.

Global telecommunications companies participating in the Fingerprint Sharing Alliance include British Telecom, MCI and NTT Communications.

And leading carriers, network providers, hosting companies and educational institutions joining the Alliance include:

Asia Netcom
Broadwing Communications LLC, USA
Cisco Systems, Inc., USA
EarthLink, USA
Energis, UK
Internet2, USA
ITC^DeltaCom, USA
Merit Network, USA
Rackspace, USA
The Planet, USA
University of Pennsylvania, USA
Utah Education Network, USA
Verizon Dominicana, Dominican Republic
WilTel Communications, USA
XO Communications, USA.

As global infrastructure attacks, such as recent domain name server (DNS) attacks and worm outbreaks, become more distributed and diffused, network operators increasingly need to communicate faster and more efficiently with upstream providers and customers to resolve these attacks. Sharing attack information across business and network boundaries today has been a reactive and relationship-driven combination of e-mail and phone calls among colleagues. Before Arbor’s Fingerprint Sharing Alliance, no automated mechanism existed for sharing and receiving threat and attack information.

“We’re seeing more technology-savvy criminals trying to make money through denial of service

extortion schemes," said Senior Yankee Group Analyst Jim Slaby. "Service providers that are cooperating by sharing attack fingerprints are helping mitigate these threats more quickly and closer to the source, thus making the Internet a more secure place."

Arbor Networks has the largest worldwide installed base of service provider customers in the infrastructure security market and is uniquely positioned to enable this industry-wide initiative. Arbor's Peakflow SP – used by the majority of Tier 1 service providers across the globe – has been enhanced to enable the sharing of attack fingerprints automatically – across network boundaries – without revealing competitive information. Sharing real-time attack profiles and blocking closer to the source is a critical step in offering end-to-end security across networks worldwide.

"MCI brings an unparalleled view into Internet security events around the globe," said Mark Sitko, vice president of MCI Security Services Product Management. "As a member of the Fingerprint Sharing Alliance, the Internet community at large will benefit from MCI's robust sources of security information, award-winning expertise and ongoing commitment to securing networks for our customers."

"When an attack hits, time is of the essence. By sharing the attack details providers are better able to protect their customers as the attack is mitigated closer to the point of origin, thus preventing collateral damage," said Tom Schuster, president of Arbor Networks. "Arbor's intent is to have global service providers join together to combat these cyber threats and protect the overall infrastructure of the Internet."

The Fingerprint Sharing Alliance delivers multiple benefits for service providers and their customers including:

• Network operators now have an efficient, automated process for engaging the service provider community in solving significant threats to the Internet
• Service providers' customers – large enterprises, small businesses, and residential customers – benefit from the faster and more effective response to attacks by their providers
• Service providers benefit by being able to communicate attack information more quickly, and will be able to spend less time dealing with attacks, and mitigating attacks closer to the real ingress points
• SLA obligations can be strengthened with a higher rate of fulfillment, and
• Network operators can automatically share attack information across network boundaries in real-time without revealing any competitive information.

(For more information about support for the Fingerprint Sharing Alliance, please see a separate announcement made today entitled, "Leading Organisations Worldwide Join Together to Stop Internet Attacks.")

ABOUT ARBOR NETWORKS
Arbor Networks ensures the security and operational integrity of the world's most critical networks. Arbor's solutions are based on the proven Peakflow platform, intelligent technology for network-wide data collection, analysis, anomaly detection, and threat mitigation. Peakflow provides real-time views of network activity enabling organizations to instantly protect against worms, DDoS attacks, insider misuse, and traffic and routing instability, as well as segment and harden networks from future threats. Peakflow

successfully prevents costly downtime, network cleanup, and loss of customer confidence. Arbor is headquartered in Lexington, MA, with a research and development office in Ann Arbor, MI and overseas headquarters in London and Beijing.

###
Contacts:

Kate Munro
Arbor Networks
+1 781.768.3253
kmunro@arbor.net

Mo Murphy
Folliard
+44 (0)207 686 0625
murphy@folliard.co.uk