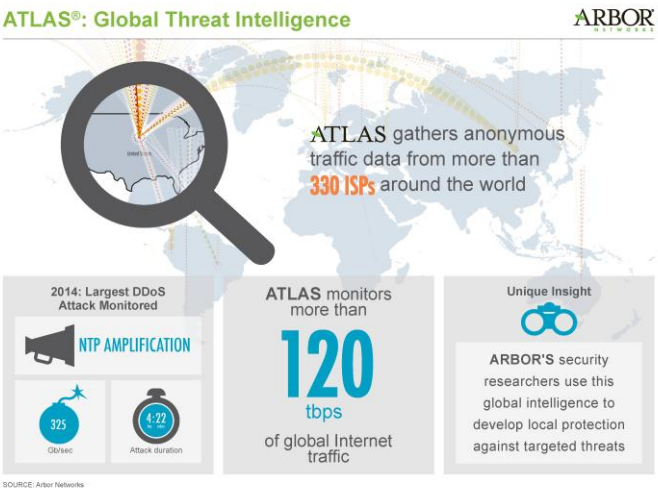
Arbor Networks' ATLAS® Infrastructure Provides Insight into 120Tbps of Global Internet Traffic

Unique Insight into Global Threats Means Better Protections for Customers

BURLINGTON, MA., February 18, 2015 – Arbor Networks Inc., a leading provider of DDoS and advanced threat protection solutions for enterprise and service provider networks, today provided an update on its ATLAS® threat monitoring infrastructure which was launched eight years ago this month. At the time of launch in February 2007, 30 ISPs were participating in the ATLAS program, contributing data representing a total of 3Tbps of global Internet traffic. Today, ATLAS has more than 330 participating network operators around the world who report data representing around 120Tbps of Internet traffic.



"Most security vendors will tell you they can provide great visibility about what is happening on your network. What Arbor has done with ATLAS is leverage their deep penetration in the global service provider community to develop the means for delivering visibility beyond the boundaries of one's own network. This is essential to understanding today's cyber threats. ATLAS is a totally unique and powerful service that provides enormous value to security teams who need to understand what is happening next door, and around the world," said Dr. Yi-Lang Tsai, President of Taiwan's Cloud Security Alliance.

ATLAS collates data from multiple sources, one of which is a collaborative effort with Arbor customers who have agreed to share anonymous DDoS and traffic data on an hourly basis (leveraging the Arbor technology that sits within their networks). ATLAS also utilizes data from Arbor dark address space monitoring probes, BGP routing information from multiple operators and data from ASERT research programs, as well as third-party data feeds. The network and security intelligence delivered via ATLAS gives Arbor customers a considerable competitive advantage, as it allows them to compare and contrast what they are seeing on their own network with a macro view of global Internet traffic and threats.
ATLAS data is the basis for Arbor's collaboration with Google Ideas, which led to the development of the Digital Attack Map, a powerful visualization of global DDoS attack traffic.

"ATLAS gives our customers the ability to see how DDoS threats are evolving not just in their own market, but more broadly around their region and the world, allowing them to better understand the threats and thus ensure the protection of their services and customers," said Darren Anstee, Director of Solutions Architects for Arbor Networks.

Turning ATLAS Data into Actionable Intelligence
For customers, ATLAS data informs decisions in a number of key areas such as network security, service creation, market analysis, capacity planning and application trends. And, the ATLAS Intelligence Feed can help protect Arbor Networks customer's key assets from a variety of the latest threats.

Arbor derives this rich data set from the sources above, and from ongoing research and analysis performed by Arbor's Security Engineering & Response Team (ASERT). ASERT is one of the industry's most respected research organizations, combining security analysts with a diverse set of expertise, from Fortune 25 Computer Emergency Response Teams (CERTs) to former law enforcement, threat mitigation

vendors and well-known malware research organizations. Viewing the global attack landscape, and utilizing custom tools for malware indexing and botnet monitoring, ASERT develops campaign oriented threat intelligence for customers, complete with the context and confidence information required to detect and stop specific threats, and continuously enhance security posture over time.

On a daily basis, ASERT gathers malware samples from ATLAS and other sources, with a focus on seriously malicious and destructive campaigns. This could include Advanced Persistent Threats, geo-political campaigns, financial fraud, point of sale and DDoS. Malware samples are analyzed using a combination of automated and manual techniques, with all relevant data on each unique sample stored in a database with millions of such analyses. Information extracted from each analysis is cross-referenced within the database allowing campaigns, and other common features / infrastructure to be identified.
When a new campaign or DDoS attack vector is detected, an attack policy is created, distributed and installed in Arbor's products via the ATLAS Intelligence Feed.

"ATLAS has not only been a huge asset to Arbor and Arbor's customers, but to the overall community as well. We provide information to over a hundred of the world's national CERT organizations and assist in botnet cleanup and takedown," said Dan Holden, Director of ASERT for Arbor Networks. "The visibility that ATLAS has brought over the years has been a boon for so many, allowing a safe way for ISP's, enterprises, and CERT's to exchange information. ATLAS was threat intelligence and exchange before such buzzwords were cool."

About Arbor Networks
Arbor Networks, Inc. helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor's advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market leading analytics for dynamic incident response, historical analysis, visualization and forensics. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context - so customers can solve problems faster and reduce the risk to their business.

To learn more about Arbor products and services, please visit our website at arbornetworks.com. Arbor's research, analysis and insight, together with data from the ATLAS global threat intelligence system, can be found at the ATLAS Threat Portal.