NETSCOUT

NEWS RELEASE

Arbor Networks to Speak at Black Hat Conference on the Next Generation of Cyber Defenders, and for the First Time, at DEF CON, on Iot Botnets

2017-07-19

Visit Arbor Networks at Booth #624 at Black Hat to Learn About Its Network Threat Traffic Analytics Solution for Greater Post-Exploit Visibility

BURLINGTON, Mass.--(BUSINESS WIRE)--Jul. 19, 2017-- **Arbor Networks Inc.**, the security division of NETSCOUT (NASDAQ: NTCT), today announced that it will be exhibiting at Black Hat USA (booth #624) from July 26 – 27 in Las Vegas, Nevada at the Mandalay Bay Convention Center. Arbor will be showcasing its visibility into threats via ATLAS®, the company's global threat intelligence infrastructure, as well as giving product demonstrations for advanced threat investigations and industry leading solutions for protection against distributed denial of service (DDoS) attacks. Additionally, Arbor security experts will be speaking at both Black Hat and, for the first time, at DEF CON.

Black Hat: Connecting Art with Science: The Next Generation Of Cyber Defenders - How do security practitioners change skill-sets and mindsets to defend themselves against adversaries waging campaigns using Techniques, Tactics and Procedures (TTPs) that are subtle and hard to predict or detect using traditional security infrastructure and technical threat intelligence? Created from over 50 in-depth interviews, Arabella will present four detailed profiles of cyber-defense teams and discuss how these teams are structured, staffed, trained and motivated. She will detail case studies of how high-performing teams are benefiting from investments to weave more "art" such as visualization and graphical models, political risk and human intelligence into the workflows of their Security Operations and Cyber Threat functions, and also how this readily applies to understanding and disrupting the plans and attack campaigns of cyber criminals.

Who: Arabella Hallawell, Sr. Director, Arbor Networks
When: Thursday, July 27 | 2:30-3:20 p.m.
Where: Business Hall Theater B, Level 1

DEF CON: **The call is coming from inside the house!** - Are you ready for the next evolution in DDoS attacks? The second half of 2016 saw the rise of a new generation of Internet of Things (IoT) botnets consisting of webcams and other IoT devices. In early 2017, a multi-stage Windows Trojan containing code to scan for vulnerable IoT devices and inject them with Mirai bot code was discovered. The number of IoT devices which were previously safely hidden inside corporate perimeters vastly exceeds those directly accessible from the internet, allowing for the creation of botnets with unprecedented reach and scale. This reveals an evolution in the threat landscape that most organizations are completely unprepared to deal with and will require a fundamental shift in defense against DDoS attacks.

This presentation will include an analysis of the Windows Mirai seeder including its design, history, infection vectors and potential evolution. It will also analyze the DDoS capabilities of typically infected IoT devices including malicious traffic analysis, as well as the consequences of infected IoT devices inside the corporate network. This includes the impact of DDoS attacks, attacks originating from the inside, the targeting corporate assets and external resources, as well as how to detect, classify and mitigate this new threat.

Who: Steinthor Bjarnason, Arbor's Security Engineering & Response Team (ASERT)
When: Sunday July 30 | 12:00 p.m.
Where: Caesars Palace, DEF CON Track 3

About Arbor Networks

Arbor Networks, the security division of **NETSCOUT**, is driven to protect the infrastructure and ecosystem of the internet. It is the principle upon which we were founded in 2000; and remains the common thread that runs through all that we do today. Arbor's approach is rooted in the study of network traffic. Arbor's suite of visibility, DDoS protection and advanced threat solutions provide customers with a micro view of their network enhanced by a macro view of global internet traffic and emerging threats through our ATLAS infrastructure. Sourced from more than 400 service provider customers, ATLAS delivers intelligence based on insight into approximately 1/3 of global internet traffic. Supported by Arbor's Security Engineering & Response Team (ASERT), smart workflows and rich user context, Arbor's network insights help customers see, understand and solve the most complex and consequential security challenges facing their organizations.

To learn more about Arbor products and services, please visit our website at **arbornetworks.com** or follow on

Twitter **@ArborNetworks**. Arbor's research, analysis and insight is shared via the **ASERT blog**. For a global data visualization of DDoS attacks that leverages our ATLAS intelligence, visit the **Digital Attack Map**, a collaboration with Jigsaw, an incubator within Alphabet, Google's parent company (NASDAQ: GOOGL).

Trademark Notice: Arbor Networks, the Arbor Networks logo and ATLAS are all trademarks of Arbor Networks, Inc. All other brands may be the trademarks of their respective owners.

View source version on businesswire.com: **http://www.businesswire.com/news/home/20170719005293/en/**

Source: Arbor Networks Inc.

Arbor Networks
Kevin Whalen, 781-362-4377
kwhalen@arbor.net