NETSCOUT

NEWS RELEASE

Arbor Networks Demonstrates High Level of Current Secure Shell / Telnet Scan Activity

2017-02-07

New IoT Device? It Could be Compromised in Seconds

BURLINGTON, Mass.--(BUSINESS WIRE)--Feb. 7, 2017-- **Arbor Networks Inc.**, the security division of NETSCOUT (NASDAQ: NTCT), announced today that it has enhanced its global honeypot network with additional cloud-based infrastructure to monitor scanning activities that could lead to Internet of Things device (IoT) compromises. These instances are present in Northeast Asia Pacific, Southeast Asia Pacific, Central EU, Western EU, Eastern South America, Eastern U.S. and Western U.S. regions.

IoT devices are ideal targets for attackers looking to build Distributed Denial of Service (DDoS) botnets because they have limited or non-existent security features. Some IoT devices utilize hard-coded default passwords. Many devices have unnecessary services running that can be exploited, and others have unprotected management interfaces. Most important for DDoS attackers, IoT devices offer high-speed connections that are always on, which allows for a large, predictable amount of attack traffic volume per compromised device.

Looking at the honeypot data during a two week period, Arbor saw a total of 1,027,543 login attempts, of which 819,198 failed, from a total of 92,317 unique source IP addresses.

- Overall, Arbor witnessed a peak of 18,054 login attempts per hour during the monitoring period.
- Telnet is being targeted more frequently than Secure Shell (SSH). The average rates show the overall trend clearly — 756 versus 2,762 attempts per hour for SSH and Telnet respectively.

Regional Differences

The hardware and software used in a large proportion of current IoT devices comes from a very small number of

manufacturers based in Asia. In 2014, one of the major manufacturers issued a new software release that solved some security issues. However, these fixes were only made available for the English version of the software. A regional breakout of the data showed a variation in the rate of login attempts by geographic area, with the Asia-Pacific (APAC) and South America honeypots seeing higher average and maximum attempt rates, more than one per minute in some cases.

“On a broad regional level, this research from Arbor validates so much of what we have learned over this last year about the expected increase in massive DDoS attacks. It is becoming more and more critical that manufacturers of IoT devices integrate security by design, including update capabilities, into their products to reduce the likelihood of their devices being used in botnets,” said Ari Schwartz, Venable’s Managing Director of Cybersecurity Services and former Special Assistant to the President and Senior Director for Cybersecurity in the Obama administration.

“Arbor’s annual security report is always an authoritative source of data on the state of cybersecurity. The inclusion of a special section on IoT is particularly timely, as it’s coming onto a lot of folks’ radars as a new vector for DDoS and other types of cyberattacks,” said Ovum senior analyst Rik Turner.

To download the full Worldwide Infrastructure Security Report, which includes the special sections on IoT botnet tracking, click **here**.

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 300 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).

View source version on businesswire.com: **http://www.businesswire.com/news/home/20170207005316/en/**

Source: Arbor Networks Inc.

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