NEWS RELEASE

NETSCOUT Highlights Evolution of Internet Scale Threats

2018-08-07

NETSCOUT Threat Intelligence Report—Powered by ATLAS®—Reveals Nation-State Activity and Blending of Internet Scale Threats with Targeted Attack Campaigns

To Learn More, Visit NETSCOUT at Black Hat 2018, Booth 536

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.,** (NASDAQ: NTCT), a leading provider of service assurance, security, and business analytics, today released its 2018 NETSCOUT Threat Intelligence Report, offering globally scoped internet threat intelligence together with the analysis of our security research organization. The report covers the latest trends and activities from nation-state advanced persistent threat (APT) groups, crimeware operations and Distributed Denial of Service (DDoS) attack campaigns. To learn more about the report, visit NETSCOUT at Black Hat 2018, Booth 536.

“ATLAS is a collaborative project with hundreds of service provider customers who have agreed to share anonymous traffic data equaling approximately one-third of all internet traffic. From this unique vantage point, NETSCOUT is ideally positioned to deliver intelligence about DDoS attacks, malware families and botnets that threaten Internet infrastructure and network availability,” said Hardik Modi, senior director, Threat Intelligence, NETSCOUT. “This report makes clear that threat actors are increasingly leveraging internet-scale threats, such as NotPetya, for targeted, highly selective campaigns.”

“NETSCOUT brings unique insights to the global threat landscape through their ATLAS infrastructure. While they’re best known for DDoS defense, the company has built an impressive security research organization that digs deep into malware campaigns and botnets at a global level, providing much needed context to the overall threat environment. By studying the infrastructure, the command and control, they’re gathering much of their intelligence

straight from the source," said Rob Ayoub, research director, Security Products program, IDC.

KEY HIGHLIGHTS:

APT groups expand scope

- State-sponsored activity has developed to the point where campaigns and frameworks are discovered regularly for a broad tier of nations. Nation-state APT groups are also using internet-scale intrusions such as NotPetya, CCleaner, VPNFilter for targeted, highly selective campaigns.

Crimeware actors diversify attack methods

- Inspired by 2017's WannaCry attack, major crimeware groups are adopting self-propagation methods that allows their malware to spread faster and more easily. They are also increasingly focused on cryptocurrency mining.

DDoS attacks grow in volume

- DDoS entered the terabit attack era in 2018, as **NETSCOUT Arbor successfully mitigated** the largest DDoS attack ever recorded at 1.7 Tbps.
- In the first half of 2018, there were 47 DDoS attacks greater than 300Gbps globally, versus only seven during the same period in 2017. Asia Pacific was heavily targeted, with 35 attacks greater than 300Gbps versus only five during the same period in 2017.

Additional Resources

- Download the full report **here**(registration required).
- **Attend a webinar** on key findings with Hardik Modi, Sr. Director of NETSCOUT Threat Intelligence.
- Visit the NETSCOUT Threat Intelligence **blog** for insight on various aspects of the report.
- Find us on Facebook and follow @Netscout on Twitter for more key findings.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) assures digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility, and insights customers need to accelerate and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius service assurance solutions provide real-time,

contextual analysis of service, network, and application performance. Arbor security solutions protect against DDoS attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions, powered by service intelligence can help you move forward with confidence, visit **www.netscout.com** or follow @NETSCOUT and @ArborNetworks on Twitter, Facebook, or LinkedIn.

©2018 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20180807005140/en/**

NETSCOUT
Donna Candelori, +1.408.571.5226
Director, Corporate Communications
Donna.candelori@netscout.com

Source: NETSCOUT SYSTEMS, INC.