NETSCOUT

NEWS RELEASE

NETSCOUT's Latest Threat Intelligence Report Uncovers Prime Targets for Cyber Criminals as Attacks Accelerate

2019-08-05

Company Launches Cyber Threat Horizon for Continuous Visibility into the Threat Landscape

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.**, (NASDAQ: NTCT), a leading provider of service assurance and security, today announced the findings of its **Threat Intelligence Report** for the first half of 2019. The report underscores how dramatically the cybercriminal business model has matured into an efficient, global operation and the increasing geographical diversity and proliferation of nation-state Advance Persistent Threats (APT) groups. It reinforces the need for companies to minimize risks by having a better view of the threat landscape.

With the introduction of **NETSCOUT's Cyber Threat Horizon**, users can leverage the platform's visibility and situational awareness capability customized by geography and vertical industries, to gain perspective into emerging threats. These insights in turn allow businesses to identify and address potential risks within their security ecosystem.

"Our latest Threat Intelligence Report underscores how cybercriminals and crimeware have not only gone to business school, but they can now teach classes," said Hardik Modi, NETSCOUT's senior director of threat intelligence. "With the cadence of attacks on the rise, businesses can no longer afford to compromise on security. IoT devices are under attack often within just five minutes of being powered up. The threats are real, and Cyber Threat Horizon gives businesses extensive visibility and clarity into the threat landscape, helping them to make the right security choices."

Key findings from the Threat Intelligence Report include:

- Botmasters are getting smarter. Attackers are increasingly taking advantage of everything from smart home sensors to smartphones, routers, and even Apple software to discover and weaponize new attack vectors.
- Focus on mid-size DDoS attacks. DDoS attack frequency grew 39% in the first half of 2019 from the first half of 2018; a staggering 776% growth occurred in the number of attacks between 100 Gbps and 400 Gbps.
- Firewalls are getting hit. Proof-of-concept malware is targeting IoT devices behind firewalls. This new trend highlights a potentially devastating situation since there are 20 times more IoT devices behind firewalls than directly connected to the internet.
- Geopolitical skirmishes go cyber. Geopolitical adversaries increasingly target one another using cyber tactics ranging from malware and DDoS attacks to social engineering and misinformation.

NETSCOUT's Threat Intelligence Report covers the latest trends and activities, including nation-state, APT groups, IoT vulnerabilities, crimeware operations, and Distributed Denial of Service (DDoS) attack campaigns. It references insights secured from **NETSCOUT's Active Level Threat Analysis System (ATLAS)**, alongside analysis from the company's **ATLAS Security Engineering and Response Team (ASERT)**, to provide a unique view of the growing threat landscape.

Coupled with Cyber Threat Horizon, users gain a continuous view of the threat landscape. They can view cyber threats at a global level and tailor their monitoring capabilities for their organization's specific industry. Insights are available in the Cyber Threat Horizon Portal, which is powered by ATLAS.

Cyber Threat Horizon's analytics and insights are easy to understand and address, thereby reducing the speed to action. Having this level of visibility will be increasingly valuable due to the increasing amount of business being conducted globally.

The visibility and analysis represented in the Threat Intelligence Report and Cyber Threat Horizon both fuel the ATLAS Intelligence Feed, used across NETSCOUT's Arbor security product portfolio to detect and block threat activity for enterprises and service providers worldwide.

For more information on NETSCOUT's bi-annual Threat Intelligence Report, please reference the following resources:

- To download the full report or learn more about the findings from the research, please **click here**.
- To access Cyber Threat Horizon, please **click here**.
- Find us on **Facebook, LinkedIn** or **Twitter** for threat updates and the latest trends and insights.

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.

©2019 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT and the NETSCOUT logo are registered trademarks of NETSCOUT SYSTEMS, INC. and/or its subsidiaries and/or affiliates in the USA and/or other countries.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20190805005181/en/**

Maribel Lopez
Manager, Marketing & Corporate Communications
NETSCOUT
+1 781 362 4330
maribel.lopez@netscout.com

Source: NETSCOUT SYSTEMS, INC.