NETSCOUT

NEWS RELEASE

NETSCOUT's Cyber Threat Horizon Offers Free Real-Time Visibility and Analysis of DDoS Attacks

2020-03-24

New online portal provides advanced insights into global DDoS attack activity backed by data and insights from Arbor ATLAS

Supports need to keep IT networks highly available for increasingly important work-at-home access

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.**, (NASDAQ:NTCT), a leading provider of service assurance, security, and business analytics, today announced the public availability of **Cyber Threat Horizon**, a free threat intelligence portal that offers network and security operators greater visibility into Distributed Denial of Service (DDoS) attacks in real-time. Cyber Threat Horizon collects, analyzes, prioritizes, and disseminates data on past and emerging DDoS threats across the internet. This macro view gives users contextual awareness of the DDoS attacks that could impact their organization and allows them to gain unique insights into DDoS attack trends to provide the situational awareness they need to assess risk and prepare for cyberattacks.

As a result of the current COVID-19 outbreak, organizations around the globe are instituting work/learn from home policies on a massive scale. Now more than ever, critical infrastructure such as internet circuits, routers, VPN gateways, and firewalls must remain available to ensure remote access to internal resources and services. DDoS attacks pose a significant threat to the availability of this critical infrastructure and services. Cyber Threat Horizon gives organizations the ability to gain situational awareness of DDoS attacks and put protection in place before remote access is impacted.

"Our new reality has placed increased demands on network security and IT administrators to ensure remote workers have access to the applications and information they need to be as efficient and productive as possible," stated John Grady, cybersecurity analyst at The Enterprise Strategy Group. "With bad actors escalating their

cyberattacks on our IT infrastructure, global enterprises and service providers should consider not only solutions providing strong mitigation capabilities, but tools that deliver the critical insights necessary to prevent DDoS attacks before they happen."

Backed by the **Arbor Active Threat Level Analysis System (ATLAS™),** which sees approximately one-third of the world's internet traffic, Cyber Threat Horizon collects data from a variety of diverse sources, including anonymized information from **Arbor Smart DDoS Protection by NETSCOUT™** products deployed globally, plus dark web and botnet traffic, to provide a comprehensive understanding of the global threat landscape. Cyber Threat Horizon provides the context needed to understand the threat of DDoS attacks, how they form, evolve, and target businesses. The portal visually displays data by DDoS attack source country, target country, attack size, duration, industry sector, and attack type. The last three most significant DDoS threats scroll across the bottom of the threat map to alert users in real-time.

"For more than 20 years, NETSCOUT has been the leader in DDoS attack research, protection products, and services. With more than 400 worldwide network operators contributing to Arbor ATLAS, no one on the planet has more visibility into global DDoS attack activity. In other words, we see things others can't," stated Hardik Modi, AVP, engineering, threat and mitigation products, NETSCOUT. "When millions of people can be impacted by one DDoS attack, the need for visibility into those attacks across the internet is imperative."

For expanded research and analysis, users can create a free log-in, which provides access to historical data back to 2003. Logging into the portal also offers the ability to establish customized neighborhoods using filters like geography and industry sector, as well as refinements like source country, destination country, and trigger or event types. By leveraging neighborhoods, users can create customized reports across various regions of the world, industry verticals, time increments, and more to understand how DDoS attacks could impact their networks.

"It's this level of threat awareness that enables an organization to determine its DDoS attack risk and put the appropriate level of DDoS attack protection in place," concluded Hardik Modi.

For a global view into how DDoS attack activity could impact your organization, visit **NETSCOUT's Cyber Threat Horizon**, and read more about it on our **blog**. For a deeper understanding, join our webinar on April 9, 2020 at 11:30am EDT, entitled **"How to Use Global DDoS Threat Intelligence for Your Local Situational Awareness."**

For more information on how you can ensure that the services your workforce needs to conduct business are available, reliable, secure and performing at a high level, from any remote location, please visit **www.netscout.com/business-continuity**, and join our webinar on April 2, 2020, at 1:00pm EDT, entitled **"Ensuring Business Continuity for Remote and Home Locations."**

Find us on Facebook, LinkedIn, or Twitter to receive the latest threat intelligence updates.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ:NTCT) helps assure 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 Smart DDoS Protection by NETSCOUT products help protect against 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 on Twitter, Facebook, or LinkedIn.

©2020 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, NETSCOUT Arbor, the NETSCOUT Arbor logo, ATLAS, Cyber Threat Horizon, 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/20200324005104/en/**

Media
Maribel Lopez
Manager, Marketing & Corporate Communications
781-362-4330
Maribel.Lopez@netscout.com

Erica McDonald
Finn Partners for NETSCOUT
+1 646 202 9784
NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC.