

NETSCOUT Engages With NTT Communications on Threat Intelligence and DDoS Attack Resilience Research

2021-09-27

Initiative Designed to Detect and Mitigate Cyberattacks to Prevent Potential Disruptions in Japan's Network Availability

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.**, (NASDAQ: NTCT), a market leader in cybersecurity, service assurance, and business analytics, today announced that it is working with **NTT Communications Corporation** (NTT Com) to conduct research and resilience testing to detect and mitigate cyberattacks by leveraging the resources of **NETSCOUT's ATLAS Security Engineering & Response Team** (ASERT). NTT Com is taking active measures to ensure its network can support increased traffic and security needs while providing a more resilient network for the future.

Volumetric DDoS attacks overwhelm internal network capacity to consume bandwidth so that genuine users cannot gain access to a network, application, or service.

"We've detected a huge uptick in volumetric DDoS cyberattacks globally, since the release of the Mirai source code, including a 1.7 Tbps reflection/amplification attack in recent years," stated Hardik Modi, Associate Vice President of Engineering, Threat and Mitigation Products, NETSCOUT. "We welcome the opportunity to continue our work with NTT Com through this research initiative to help them discover, analyze, and prevent DDoS and other cyberattacks."

NETSCOUT ASERT will collaborate with NTT Com's technical team to implement this initiative in September 2021 and continue through December 2021. The focus will be to discover and mitigate large DDoS attacks, implement defense measures for application attacks, analyze malware attacks in honeypots, leverage artificial intelligence (AI)

to predict cyberattacks, and identify new attacks before becoming an issue.

About NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) helps assure digital business services against security, availability, and performance disruptions. 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 Omnis® Cybersecurity advanced threat detection and response platform offers comprehensive network visibility, threat detection, highly contextual investigation, and automated mitigation at the network edge. NETSCOUT nGenius® service assurance solutions provide real-time, contextual analysis of service, network, and application performance. And 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 security and performance solutions can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT on Twitter, Facebook, or LinkedIn.

©2021 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor, ATLAS, Cyber Threat Horizon,

InfiniStream, nGenius, nGeniusONE, and Omnis 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/20210927005846/en/): <https://www.businesswire.com/news/home/20210927005846/en/>

Maribel Lopez

Manager, Marketing & Corporate Communications

+1 781 362 4330

maribel.lopez@netscout.com

Mena Buscetta

Finn Partners for NETSCOUT

+1 860 326 1698

NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC.