NETSCOUT

NEWS RELEASE

NETSCOUT Threat Intelligence Report Shows Dramatic Increase in Multivector DDoS Attacks in First-Half 2020

2020-09-29

4.8 million attacks, combined with a 126% rise in 15-plus vector attacks and a 31% increase in throughput, increases mitigation difficulty

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.,** (NASDAQ: NTCT), today announced the findings of its **1H 2020 Threat Intelligence Report**, which reinforces the dramatic impact cybercriminals have had during the COVID-19 pandemic. Attackers focused on COVID-era lifelines such as healthcare, e-commerce, and educational services with complex, high-throughput attacks designed to overwhelm and quickly take them down.

“The first half of 2020 witnessed a radical change in DDoS attack methodology to shorter, faster, harder-hitting complex multi-vector attacks that we expect to continue,” stated Richard Hummel, threat intelligence lead, NETSCOUT. “Adversaries increased attacks against online platforms and services crucial in an increasingly digital world, such as e-commerce, education, financial services, and healthcare. No matter the target, adversary, or tactic used, it remains imperative that defenders and security professionals remain vigilant in these challenging days to protect the critical infrastructure that connects and enables the modern world.”

Key findings from the NETSCOUT 1H 2020 Threat Intelligence Report include:

- Cybercriminals launched record-breaking attacks at online platforms and services during the pandemic – More than 929,000 DDoS attacks occurred in May, representing the single largest number of attacks ever seen in a month. 4.83 million DDoS attacks occurred in the first half of 2020, a 15% increase. However, DDoS attack frequency jumped 25% during peak pandemic lockdown months (March through June).

- Bad actors focused on shorter, more complex attacks – Super-sized 15-plus vector attacks increased 2,851% since 2017, while the average attack duration dropped 51% from the same period last year. Moreover, single-vector attacks fell 43% while attack throughput increased 31%, topping out at 407 Mpps. The increase in attack complexity and speed, coupled with the decrease in duration, gives security teams less time to defend their organizations from increasingly sophisticated attacks.
- Organizations and individuals bear the cost of cyber attacks – To determine the impact that DDoS attacks have on global Internet traffic, the **NETSCOUT ATLAS Security Engineering and Response Team (ASERT**) developed the DDoS Attack Coefficient (DAC). It represents the amount of DDoS attack traffic traversing the internet in a given region or country during any one-minute period. If no traffic can be attributed to DDoS, the amount would be zero. DAC identified top regional throughput of 877 Mpps in the Asia Pacific region, and top bandwidth of 2.8 Tbps in EMEA. DAC is important since cybercriminals don't pay for bandwidth. It demonstrates the "DDoS tax" that every internet-connected organization and individual pays.

NETSCOUT's Threat Intelligence Report covers the latest trends and activities in the DDoS threat landscape. It covers data secured from **NETSCOUT's Active Level Threat Analysis System (ATLAS)** coupled with insights from the ASERT.

The visibility and analysis represented in the Threat Intelligence Report and **Cyber Threat Horizon** 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 semi-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**
- Find us on **Facebook**, **LinkedIn**, and **Twitter** for threat updates and the latest trends and insights

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, Arbor, ATLAS, Cyber Threat Horizon, InfiniStream, 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/20200929005235/en/**

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

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

Source: NETSCOUT SYSTEMS, INC.