NETSCOUT

NEWS RELEASE

Vital Pandemic Industries Foster Unprecedented DDoS Attack Activity According to 2H2020 NETSCOUT Threat Intelligence Report

2021-04-13

Record-setting 10 million-plus DDoS attacks and 22% increase in attack frequency

WISR survey findings reinforce impact of global DDoS extortion attack campaign

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.**, (NASDAQ: NTCT) today announced findings from its bi-annual **Threat Intelligence Report**, punctuated by a record-setting 10,089,687 Distributed Denial of Service (DDoS) attacks observed during 2020. Cybercriminals exploited vulnerabilities exposed by massive internet usage shifts since many users were no longer protected by enterprise-grade security. Attackers paid particular attention to vital pandemic industries such as e-commerce, streaming services, online learning, and healthcare generating a 20% year-over-year increase in attack frequency over 2019 plus a 22% increase in the last six months of 2020.

In August, a threat actor NETSCOUT dubbed Lazarus Bear Armada (LBA) launched one of the most sustained and extensive DDoS extortion campaigns yet seen, taking down the New Zealand stock exchange and targeting organizations involved in COVID-19 testing and vaccine development.

According to NETSCOUT's Worldwide Infrastructure Security Report® (WISR), which helps inform the Threat Intelligence Report findings, the number of enterprise respondents reporting DDoS extortion attacks increased by 125%. Overloaded firewalls and virtual private network (VPN) concentrators, crucial technologies used during the pandemic lockdown, contributed to the outages in 83% of the enterprises that suffered DDoS attacks. This finding represents a 21% increase over 2019 figures.

"Cybercriminals set multiple records in 2020, taking advantage of the shift towards remote work across the globe,"

stated Richard Hummel, threat intelligence lead, NETSCOUT. "The second half of last year witnessed a huge upsurge in DDoS attacks, brute-forcing of access credentials, and malware targeting internet-connected devices. As the COVID-19 pandemic continues, it will be imperative for security professionals to remain vigilant to protect critical infrastructure."

Other key findings from the NETSCOUT 2H2020 Threat Intelligence Report include:

- Monthly DDoS attack numbers surpassed 800,000. Threat actors increased their DDoS onslaught due to the pandemic lockdown; monthly DDoS attacks exceeded 800,000 in March and never looked back, representing a new normal for DDoS attack activity. On average, there were 839,083 attacks per month in 2020, an increase of nearly 130 thousand attacks over 2019.
- Mirai malware continued to thrive during the pandemic. Adversaries using Mirai malware and its variants took advantage of shifts away from enterprise-grade protection to generate a surge in brute-force attempts on Internet of Things (IoT) consumer-grade devices. Threat actors absorbed more devices into their botnets to further strengthen the frequency, size, and throughput of DDoS attacks worldwide.
- Commonly Used UDP-based DDoS attack vectors fueled attack increases. New reflection/amplification DDoS vectors permitted the abuse of misconfigured Microsoft RDP over UDP, Plex Media SSDP, and DTLS services resulting in an increasingly complex threat landscape.

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 NETSCOUT's **ATLAS Security Engineering & Response Team (ASERT)** insights.

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 visit our **new interactive website**. You can also 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.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20210413005400/en/**

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

Mena Buscetto
Finn Partners for NETSCOUT
+1 860 326 1698
NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC.