NETSCOUT

NEWS RELEASE

Cybercriminal Attacks Accelerate Global Cybersecurity Crisis According to 1H2021 NETSCOUT Threat Intelligence Report

2021-09-21

Approximately 5.4 million DDoS attacks represent an 11% increase over 1H2020 on pace to surpass the previous year's record with far-reaching impact on critical Internet gateways

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC.,** (NASDAQ: NTCT) today announced findings from its bi-annual **Threat Intelligence Report** that underscore the dramatic impact cyberattacks continue to have on private and public organizations and governments worldwide. In the first half of 2021, cybercriminals launched approximately 5.4 million Distributed Denial of Services (DDoS) attacks, increasing 11% over 1H2020 figures. Additionally, data projections from NETSCOUT's Active Level Threat Analysis System (ATLAS™) Security Engineering and Response Team (ASERT) point to 2021 as another record-setting year on track to surpass 11 million global DDoS attacks. ASERT expects this long tail of attacker innovation to last, fueling a growing cybersecurity crisis that will continue to impact public and private organizations.

In the wake of Colonial Pipeline, JBS, Harris Federation, Australian broadcaster Channel Nine, CNA Financial, and several other high-profile attacks, the impact of DDoS and other cybersecurity attacks has been felt worldwide. As a result, leading governments are introducing new programs and policies to defend against attacks, and policing organizations are initiating unprecedented collaborative efforts to address the crisis.

During 1H2021, cybercriminals weaponized and exploited seven newer reflection/amplification DDoS attack vectors putting organizations at greater risk. This attack vector explosion spurred an increase in multivector DDoS attacks with a record-setting 31 attack vectors deployed in a single attack against one organization.

Other key findings from the NETSCOUT 1H2021 Threat Intelligence Report include:

- New adaptive DDoS attack techniques evade traditional defenses. By customizing their strategies, cybercriminals evolved their attack efforts to bypass cloud-based and on-premise static DDoS defenses to target commercial banks and credit card processors.
- Connectivity supply chain increasingly under attack. Bad actors looking to cause the most collateral damage focused their efforts on vital internet components, including DNS servers, virtual private network (VPN) concentrators, services, and internet exchanges, disrupting essential gateways.
- Cybercriminals add DDoS to their toolkit to launch triple extortion campaigns. Ransomware has become big business, with extortionists adding DDoS to their attack regimen to ratchet up the pressure on victims and add stress to security teams. Triple extortion combines file encryption, data theft, and DDoS attacks, increasing the possibility that cyber criminals receive payment.
- The fastest DDoS attack recorded a 16.17% year-over-year increase. A Brazilian wireline broadband internet user launched the attack, which was likely related to online gaming. Using DNS reflection/amplification, TCP ACK flood, TCP RST flood, and TCP SYN/ACK reflection/amplification vectors, the sophisticated attack recorded 675 Mpps.
- The largest DDoS attack, 1.5 Tbps, represented a year-over-year increase of 169%. ASERT data identified this attack against a German ISP, deploying a DNS reflection/amplification vector. This attack represents a dramatic increase in size over any attacks recorded in 1H2020.
- Botnets contribute to major DDoS activity - Tracked botnet clusters and high-density attack-source zones worldwide showcased how malicious adversaries abused these botnets to participate in more than 2.8 million DDoS attacks. In addition, well-known IoT botnets Gafgyt and Mirai continue to pose a severe threat contributing to more than half of the total number of DDoS attacks.

"Cybercriminals are making front-page news launching an unprecedented number of DDoS attacks to take advantage of the pandemic's remote work shift by undermining vital components of the connectivity supply chain," stated Richard Hummel, threat intelligence lead, NETSCOUT. "Ransomware gangs added triple-extortion DDoS tactics to their repertoire. Simultaneously, the Fancy Lazarus DDoS extortion campaign kicked into high gear threatening organizations in multiple industries with a focus on ISPs and specifically their authoritative DNS servers."

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 **Omnis® Threat Horizon** fuel the ATLAS Intelligence Feed used across NETSCOUT's Omnis 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 **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 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/20210921005395/en/**

Editorial Contacts:

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.