NETSCOUT

NEWS RELEASE

Bad Actors Innovate, Extort and Launch 9.7M DDoS Attacks in 2021 According to the Latest NETSCOUT Threat Intelligence Report

2022-03-22

Ransomware Gangs, DDoS-for-Hire Services, and Server-Class Botnet Armies
Make Attacks Easier to Launch with Greater Sophistication

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT SYSTEMS, INC., (NASDAQ: NTCT) today announced findings from its bi-annual **Threat Intelligence Report**. During the second half of 2021, cybercriminals launched approximately 4.4 million Distributed Denial of Service (DDoS) attacks, bringing the total number of DDoS attacks in 2021 to 9.75 million. These attacks represent a 3% decrease from the record number set during the height of the pandemic but continue at a pace that's 14% above pre-pandemic levels.

The report details how the second half of 2021 established high-powered botnet armies and rebalanced the scales between volumetric and direct-path (non-spoofed) attacks, creating more sophisticated operating procedures for attackers and adding new tactics, techniques, and methods to their arsenals.

“While it may be tempting to look at the decrease in overall attacks as threat actors scaling back their efforts, we saw significantly higher activity compared to pre-pandemic levels,” said Richard Hummel, threat intelligence lead, NETSCOUT. “The reality is that attackers are constantly innovating and adapting new techniques, including the use of server-class botnets, DDoS-for-Hire services, and increased used direct-path attacks that continually perpetuate the advancement of the threat landscape.”

Other key findings from the NETSCOUT 2H2021 Threat Intelligence Report include:

- DDoS Extortion and Ransomware Operations are on the rise. Three high-profile DDoS extortion campaigns

simultaneously operating is a new high. Ransomware gangs including Avaddon, REvil, BlackCat, AvosLocker, and Suncrypt were observed using DDoS to extort victims. Because of their success, ransomware groups have DDoS extortion operators masquerading as affiliates like the recent REvil DDoS Extortion campaign.

- VOIP Services were Targets of DDoS Extortion. Worldwide DDoS extortion attack campaigns from the REvil copycat were waged against several VOIP services providers. One VOIP service provider reported $9M-$12M in revenue loss due to DDoS attacks.
- DDoS-for-Hire services made attacks easy to launch. NETSCOUT examined 19 DDoS-for-Hire services and their capabilities that eliminate the technical requirements and cost of launching massive DDoS attacks. When combined, they offer more than 200 different attack types.
- APAC attacks increased by 7% as other regions subsided. Amid ongoing geopolitical tensions in China, Hong Kong, and Taiwan, the Asia-Pacific region saw the most significant increase in attacks year over year compared to other regions.
- Server-class botnet armies arrived. Cybercriminals have not only increased the number of Internet-of-Things (IoT) botnets but have also conscripted high-powered servers and high-capacity network devices, as seen with the GitMirai, Meris, and Dvinis botnets.
- Direct-path attacks are gaining in popularity. Adversaries inundated organizations with TCP- and UDP-based floods, otherwise known as direct-path or non-spoofed attacks. Meanwhile, a decrease in some amplification attacks drove down the number of total attacks.
- Attackers targeted select industries.Those hardest hit include software publishers (606% increase), insurance agencies and brokers (257% increase), computer manufacturers (162% increase), and colleges, universities, and professional schools (102% increase)
- The fastest DDoS attack recorded a 107% year-over-year increase. Using DNS, DNS amplification, ICMP, TCP, ACK, TCP RST, and TCP SYN vectors, the multi-vector attack against a target in Russia recorded 453 Mpps.

NETSCOUT's Threat Intelligence Report covers the latest trends and activities in the DDoS threat landscape. It covers data captured from NETSCOUT's Active Level Threat Analysis System (ATLAS™) coupled with insights from NETSCOUT's ATLAS Security Engineering & Response Team.

The visibility and insights compiled from the global DDOS attack data, which is represented in the Threat Intelligence Report and can be seen in the **Omnis Threat Horizon** portal, fuel the ATLAS Intelligence Feed used across NETSCOUT's Omnis security portfolio to detect and block threat activity for enterprises and service providers worldwide.

Visit our **interactive website** for more information on NETSCOUT's semi-annual Threat Intelligence Report. 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. Omnis® Cyber Intelligence delivers the fastest and most scalable network security solution available on the market. 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.

©2022 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/20220322005111/en/**

Editorial Contacts:

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

Chris Shattuck
Finn Partners for NETSCOUT
+1 404 502 6755
NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC.