NETSCOUT

NEWS RELEASE

Direct-Path Attacks Surge in 2022 Making Up Half of All DDoS Attacks According to Latest NETSCOUT DDoS Threat Intelligence Report

2023-04-04

DDoS traffic reached a high of 436 petabits in a single day, while application-layer attacks increased 487% since 2019

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC**. (NASDAQ: NTCT), a leading provider of performance management, cybersecurity, and DDoS protection solutions, today announced findings from its 5th Anniversary DDoS Threat Intelligence Report that point to a new era of multi-vector attacks focused on taking down victims using application-layer and botnet-based, direct-path attacks. Attack frequency has increased tenfold since NETSCOUT's first report in 2005.

With over one billion websites worldwide, HTTP/HTTPS application-layer attacks have increased by 487% since 2019, with the most significant surge in the second half of 2022. Much of the increase comes from the pro-Russian group Killnet and others that explicitly target websites. Attacks of this nature preceded the Ukraine invasion, knocking out critical financial, government, and media sites.

"DDoS attacks threaten organizations worldwide and challenge their ability to deliver critical services," said Richard Hummel, threat intelligence lead, NETSCOUT. "With multi-terabit-per-second attacks now commonplace, and bad actors' arsenals continuing to grow in sophistication and complexity, organizations need a strategy that can quickly adapt to the dynamic nature of the DDoS threat landscape."

Additional highlights from NETSCOUT's findings include:

- Peak DDoS alert traffic in a single day reached as high as 436 petabits and more than 75 trillion packets.

Service providers rigorously scrubbed a large percentage of this traffic, while enterprises eliminated an additional daily aggregate average of 345 terabytes of unwanted traffic.

- Direct-path attacks have increased by 18% over the past three years, while traditional reflection/amplification attacks decreased by nearly the same, highlighting the need for a hybrid defense approach to weather the fluctuating attack methodology.
- The U.S. national security sector experienced a massive 16,815% increase in attacks related to the pro-Russia Killnet group, including a spike in attacks after President Biden's public remarks at the G7 Summit and another spike the same day the French and U.S. presidents re-affirmed their support for Ukraine.
- NETSCOUT ASERT analysts tracked over 1.35 million bots from malware families like Mirai, Meris, and Dvinis in 2022, with enterprises receiving over 350,000 security-related alerts with botnet involvement. By contrast, service providers received approximately 60,000 alerts where bots were present.
- Carpet-bombing attacks, a technique that simultaneously targets entire IP address ranges, increased by 110% from the first to the second half of 2022, with most attacks against ISP networks.
- A barrage of DDoS attacks hammered EMEA's optical instrument and lens manufacturing sector, resulting in a 14,137% increase, mainly against one major distributor with over 6,000 attacks over four months.
- DDoS attacks on the wireless telecommunications industry have grown 79% since 2020, primarily due to the increase in 5G wireless to the home. It accounts for 20% of all DDoS attacks for a specific industry, second only to wired telecommunications carriers.

NETSCOUT's DDoS Threat Intelligence Report covers the latest trends and activities in the DDoS threat landscape. It incorporates data from NETSCOUT's ATLAS – part of the company's Visibility Without Borders approach – along with expert insights from ASERT, NETSCOUT's security research team. ATLAS was built over two decades through work with more than 500 Internet Service Providers (ISPs) to create a sensor network that provides visibility into more than 400 Tbps of international transit every second of every day. As a result, ATLAS collects DDoS attack statistics from an average of 93 countries daily, encompassing over 50% of the world's internet traffic.

The visibility and insights compiled from the global attack data represented in the DDoS Threat Intelligence Report, and seen in the NETSCOUT **Threat Horizon** portal, fuel the ATLAS Intelligence Feed (AIF). In addition, AIF continuously arms NETSCOUT's security portfolio enabling it to automatically detect, adapt, and block threat activity for enterprises and service providers worldwide.

Visit our **interactive website** for more information on NETSCOUT's semi-annual DDoS 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) protects the connected world from cyberattacks and performance and

availability disruptions through the company's unique visibility platform and solutions powered by its pioneering deep packet inspection at scale technology. NETSCOUT serves the world's largest enterprises, service providers, and public sector organizations. Learn more at **www.netscout.com** or follow @NETSCOUT on LinkedIn, Twitter, or Facebook.

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.