NETSCOUT

NEWS RELEASE

NETSCOUT Identified Nearly 7.9 Million DDoS Attacks in 1H2023 According to Its Latest DDoS Threat Intelligence Report

2023-09-26

Attacks Grew 31% YOY With a Staggering 44,000 Each Day Fueled by World Events

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT SYSTEMS, INC., (NASDAQ: NTCT) today announced findings from its 1H2023 **DDoS Threat Intelligence Report**. Cybercriminals launched approximately 7.9 million Distributed Denial of Service (DDoS) attacks in the first half of 2023, representing a 31% year-over-year increase.

Global events like the Russia-Ukraine war and **NATO bids** have driven recent DDoS attack growth. Finland was targeted by pro-Russian hacktivists in 2022 during its bid to join NATO. Turkey and Hungary were targeted with DDoS attacks for opposing Finland's bid. In 2023, Sweden experienced a similar onslaught around its NATO bid, culminating with a 500 Gbps DDoS attack in May. Overall, ideologically motivated DDoS attacks have targeted the United States, Ukraine, Finland, Sweden, Russia, and multiple other countries.

During 2H2022, NETSCOUT documented a trend in DDoS attacks against wireless telecommunications providers that incurred a 79% increase globally. That trend continued among APAC wireless providers in 1H2023 with a 294% increase, which correlates to many broadband gaming users shifting their activity to 5G fixed wireless access as providers roll out their networks.

NETSCOUT's insights into the threat landscape come from its ATLAS sensor network built over decades of working with hundreds of Internet Service Providers globally, gleaning trends from an average of 424 Tbps of internet peering traffic, an increase of 5.7% over 2022. The company has observed nearly 500% growth in HTTP/S application layer attacks since 2019 and 17% growth in DNS reflection/amplification volumes during the first half of 2023.

“While world events and 5G network expansion have driven an increase in DDoS attacks, adversaries continue to evolve their approach to be more dynamic by taking advantage of bespoke infrastructure such as bulletproof hosts or proxy networks to launch attacks,” stated Richard Hummel, senior threat intelligence lead, NETSCOUT. “The lifecycle of DDoS attack vectors reveals the persistence of adversaries to find and weaponize new methods of attack, while DNS water torture and carpet-bombing attacks have become more prevalent.”

Other key findings from the NETSCOUT 1H2023 DDoS Threat Intelligence Report include:

- Carpet-Bombing Attacks Rise. A resurgence in carpet-bombing attacks occurred since the beginning of the year, with a 55% increase to more than 724 daily, which NETSCOUT believes is a conservative estimate. These attacks cause significant harm across the global internet, spreading to hundreds and even thousands of hosts simultaneously. This tactic often avoids triggering high bandwidth threshold alerts to begin timely DDoS attack mitigation.
- DNS Water-Torture Attacks Become Commonplace. DNS water-torture attacks rose nearly 353% in daily attacks since the beginning of the year. The top five industries targeted include wired telecom, wireless telecom, data processing hosting, electronic shopping and mail-order companies, and insurance agencies and brokerages.
- Higher Education and Governments Disproportionately Attacked. Adversaries create their own or use different types of abusable infrastructure as platforms to launch attacks. For example, open proxies were consistently leveraged in HTTP/S application-layer DDoS attacks against targets in the higher education and national government sectors. Meanwhile, DDoS botnets featured frequently in attacks against state and local governments.
- DDoS Sources Are Persistent. A relatively small number of nodes are involved in a disproportionate number of DDoS attacks, with an average IP address churn rate of only 10%, as attackers tend to re-use abusable infrastructures. While these nodes are persistent, the impact fluctuates as adversaries rotate through different lists of abusable infrastructure every few days.

Visit our **interactive website** for more information on NETSCOUT's semi-annual DDoS Threat Intelligence Report. For real-time DDoS attack stats, map, and insights, visit **NETSCOUT Cyber Threat Horizon**. You can also find us on **Facebook**, **LinkedIn**, and **Twitter**.

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