NETSCOUT

NEWS RELEASE

Geopolitical Unrest Generates an Onslaught of DDoS Attacks, According to the Latest NETSCOUT Threat Intelligence Report

2024-04-25

Hacktivist Groups Increase Activity Globally While a Rise in DNS Water Torture Contributed to more than 7 Million DDoS Attacks in the Second Half of 2023

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) today released findings from its 2H2023 **DDoS Threat Intelligence Report** that dissects trends and attack methodologies adversaries use against service providers, enterprises, and end-users. The information cited in the report is gathered from NETSCOUT's unparalleled internet visibility at a global scale, collecting, analyzing, prioritizing, and disseminating data on DDoS attacks from 214 countries and territories, 456 vertical industries, and more than 13,000 Autonomous System Numbers (ASNs). Driven by tech-savvy and politically motivated hacktivist groups and an increase in DNS water torture attacks, NETSCOUT observed more than 7 million DDoS attacks in the second half of 2023, representing a 15% increase from the first half.

Hacktivism Increases Ten-Fold

DDoS (Distributed Denial-of-Service) hacktivism transcended geographic borders during the past year, exemplifying a shift in the global security landscape. Groups like NoName057(016) and Anonymous Sudan, as well as lone hackers and small collectives, are increasingly using DDoS to target those ideologically opposed to them, for example:

- Peru experienced a 30% increase in attacks tied to protests of former Peruvian President Fujimori's release from prison on December 6.
- Poland experienced a surge in attacks at the end of 2023 associated with a regime change and statements

reaffirming Poland’s support of Ukraine in the Russia-Ukraine conflict.

- Anonymous Sudan attacked X (formerly Twitter) to influence Elon Musk regarding Starlink service in Sudan, and it attacked Telegram for suspending its main channel.

NoName057(016), Anonymous Sudan, and Killnet have taken credit for DDoS attacks in Ukraine, Russia, Israel, and Palestine targeting communications infrastructure, hospitals, and banks. Daily attacks from hacktivists increased more than ten-fold between the first and second halves of 2023. NoName057(016) topped the list of DDoS adversaries in 2023, targeting 780 websites across 35 countries.

Water Torture Attacks Rise

Targeting critical systems at the heart of the Internet's control plane, DNS (Domain Name System) water torture attacks have been on the rise since the end of 2019. DNS query floods designed to overwhelm authoritative DNS servers experienced a massive 553% increase from 1H2020 to 2H2023. Rather than targeting one website or server, adversaries go after entire systems, resulting in even more damage.

Gaming and Gambling Targeted

NETSCOUT findings point to gaming -- and the gambling associated with gaming – as a primary target for DDoS attacks. Threat actors are drawn to the sector’s substantial financial value and the goal of disrupting competitors, especially during online esports tournaments. Historically, 80-90% of all DDoS attacks are related to gaming and gambling. NETSCOUT assessed attacks on enterprises in these sectors, determining that more than 100,000 DDoS attacks were deployed against those in gaming, and over 20,500 were made against those tied to gambling in 2023.

In addition, based on NETSCOUT’s observations of the DDoS threat landscape, approximately 1% of DDoS attacks are suppressed from originating networks.

“Global adversaries have become more sophisticated in the past year attacking websites and overloading servers to lockout customers and inflict digital chaos to influence geopolitical issues,” stated Richard Hummel, senior threat intelligence lead, NETSCOUT. “The relentless barrage of DDoS threats drives up costs and creates security fatigue for network operators. They cannot safeguard their digital assets without the proper advanced DDoS protection leveraging predictive, real-time threat intelligence.”

Multiple decades of experience working with the world’s largest service providers and enterprises give NETSCOUT far-reaching visibility into the global internet to discern the pulse of the digital world. Our capacity to monitor and respond to DDoS attacks is powered by our ATLAS platform, which enables us to analyze an impressive 500 terabits per second (Tbps) of network traffic.

Visit our **interactive website** for more information on NETSCOUT's DDoS Threat Intelligence Report. For real-time DDoS attack stats, map, and insights, visit **NETSCOUT Cyber Threat Horizon**.

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**, **X**, or **Facebook**.

Editorial:

Chris Lucas

NETSCOUT Systems, Inc.

+1 978-614-4124

chris.lucas@netscout.com

Chris Shattuck

Finn Partners for NETSCOUT

+1 404 502 6755

NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC