NEWS RELEASE

NETSCOUT Reports DDoS Attacks Targeting Critical Infrastructure Play a Dominant Role in Geopolitical Conflicts

2025-04-02

DDoS attacks are precision-guided digital weapons as DDoS-for-hire services, AI and powerful botnets drive onslaught of attacks

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) today released its **2H2024 DDoS Threat Intelligence Report**, revealing how Distributed Denial of Service (DDoS) attacks have become a dominant means of waging cyberwarfare linked to sociopolitical events such as elections, civil protests, and policy disputes. The findings show how attackers exploit moments of national vulnerability to amplify chaos and erode trust in institutions, as they target the critical infrastructure of governments, commercial entities and service providers.

Throughout the year, DDoS attacks were intricately tied to social/political events, including Israel experiencing a 2,844% surge tied to hostage rescues and political conflicts, Georgia enduring a 1,489% increase during the lead-up to the passage of the “Russia Bill,” Mexico having a 218% increase during national elections, and the United Kingdom experiencing a 152% increase on the day the Labour Party resumed session in Parliament.

“DDoS has emerged as the go-to tool for cyberwarfare,” stated Richard Hummel, director, threat intelligence, NETSCOUT. “NoName057(16) continues to be the leading actor for politically motivated DDoS campaigns targeting governments, infrastructure, and organizations. In 2024, they repeatedly targeted government services in the United Kingdom, Belgium, and Spain.”

AI and Automation Drive Scale and Impact

DDoS-for-hire services have become more powerful using AI for CAPTCHA bypassing, with about nine in ten platforms now offering this capability. Additionally, many employ automation to enable dynamic, multi-target campaigns and offer infrastructure exploitation techniques such as carpet bombing, geo-spoofing, and IPv6 to expand attack surfaces. Even the most novice operators can launch significant DDoS attack campaigns causing substantial harm.

Botnets Playing a Bigger Role

Enterprise servers and routers have been exploited to intensify attacks and make remediation more challenging. Overall botnet populations declined by 5% but demonstrated strong resiliency despite concerted takedown efforts. Law enforcement takedown efforts, like Operation PowerOFF, continue to target DDoS-for-hire services but only momentarily disrupt attack platforms as new platforms take their place. The long-term impact is uncertain as attackers adapt and reconstitute their networks, with no significant decline in global attack volume.

DDoS Attacks are Adaptive and Persistent

DDoS attacks are evolving and adapting faster than ever, creating a challenge for defenders and those entrusted with protecting critical infrastructure networks and service availability. Enterprises, government organizations, and service providers are all targets for DDoS attacks. Successful strategies must deploy proactive intelligence-driven methodologies and automation to mitigate modern-day DDoS attacks effectively. Staying ahead of new threats demands that organizations outmaneuver an adversary that can force multiply its strength, speed, intelligence, and persistence like nothing the world has ever seen.

Unparalleled Attack Visibility

NETSCOUT maps the DDoS landscape through passive, active, and reactive vantage points, providing unparalleled visibility into global attack trends. NETSCOUT protects two-thirds of the routed IPv4 space, securing network edges that carried global peak traffic of over 700 Tbps in 2H2024. It monitors tens of thousands of daily DDoS attacks by tracking multiple botnets and DDoS-for-hire services that leverage millions of abused or compromised devices.

Visit our **website** to learn more about NETSCOUT's DDoS Threat Intelligence Report. For real-time DDoS attack stats 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 its 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**.

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