NETSCOUT

NEWS RELEASE

Innovative NETSCOUT Solution Protects Customers From Cyberattacks

2023-11-07

Adaptive DDoS Protection for AED Defends Against DNS Water Torture

WESTFORD, Mass.--(BUSINESS WIRE)-- **NETSCOUT SYSTEMS, INC**. (NASDAQ: NTCT), a leading provider of performance management, cybersecurity, and DDoS attack protection solutions, today launched Adaptive DDoS Protection for Arbor Edge Defense (AED) to protect ISPs and enterprises from DNS water torture attacks. According to the **NETSCOUT DDoS Threat Intelligence Report**, Domain Name System (DNS) water torture attacks increased 353% in the first six months of 2023, overwhelming Authoritative DNS server resources and bringing down critical DNS services.

“DNS water torture DDoS attacks have been around since 1997, yet many organizations still struggle to efficiently identify and mitigate them,” said John Grady, principal at Enterprise Strategy Group. “These attacks send invalid requests to an Authoritative DNS server to slow it down and prevent legitimate requests from getting a response. Security teams cannot broadly block this traffic without potentially impacting valid requests due to the pervasiveness of DNS and can easily misdiagnose an attack as a performance issue. NETSCOUT’s Adaptive DDoS Protection auto-learns and adapts to changes in DNS server configuration, enabling AED to identify and mitigate these attacks.”

DNS water torture is one of many attack techniques adversaries can adopt to bring down DNS infrastructure. NETSCOUT’s Adaptive DDoS Protection for AED protects against many DDoS attack techniques at scale by:

- Auto-learning legitimate hostnames for each domain by continually analyzing DNS query and response packets
- Adapting to DNS server configuration changes to prevent blocking legitimate domains and changes to attack

techniques
- Intelligently blocking DNS water torture IP sources on a query-by-query basis

Adaptive DDoS Protection gives SOC teams a scalable, always-on, stateless packet processing solution that uses unmatched visibility into more than 50% of all internet traffic, real-time global DDoS attack threat intelligence, and decades of DDoS mitigation experience to automatically detect, adapt to, and mitigate dynamic DDoS attacks.

“Adaptive DDoS Protection for AED provides customers with a unique hybrid multi-layer DDoS defense architecture,” said Scott Iekel-Johnson, AVP, DDoS and Threat Intelligence at NETSCOUT. “It can learn and filter millions of legitimate hostnames and thousands of domains backed by our ATLAS® Intelligence Feed (AIF) to thwart modern-day attacks and advanced threats.”

To learn more about Adaptive DDoS Protection for AED, visit our **website**.

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.

©2023 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Visibility Without Borders, Adaptive Service Intelligence, Arbor, ATLAS, Cyber Threat Horizon, InfiniStream, nGenius, nGeniusONE, Omnis, and TrueCall 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.

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