NEWS RELEASE

Adversaries Continue Cyberattack Onslaught with Greater Precision and Innovative Attack Methods according to 1H2022 NETSCOUT DDoS Threat Intelligence Report

2022-09-27

TCP-based, DNS water-torture, and carpet-bombing attacks dominate the DDoS threat landscape

Ireland, India, Taiwan, and Finland battered by DDoS attacks resulting from the Russia/Ukraine war

WESTFORD, Mass.--(BUSINESS WIRE)-- NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) today announced findings from its 1H2022 DDoS Threat Intelligence Report. The findings demonstrate how sophisticated cybercriminals have become at bypassing defenses with new DDoS attack vectors and successful methodologies.

"By constantly innovating and adapting, attackers are designing new, more effective DDoS attack vectors or doubling down on existing effective methodologies," said Richard Hummel, threat intelligence lead, NETSCOUT. "In the first half of 2022, attackers conducted more pre-attack reconnaissance, exercised a new attack vector called TP240 PhoneHome, created a tsunami of TCP flooding attacks, and rapidly expanded high-powered botnets to plague network-connected resources. In addition, bad actors have openly embraced online aggression with high-profile DDoS attack campaigns related to geopolitical unrest, which have had global implications."

Deployed in most of the world's ISPs, large data centers, and government and enterprise networks, NETSCOUT Arbor DDoS attack protection solutions send anonymized DDoS attack statistics to NETSCOUT's Active Level Threat Analysis System (ATLAS™). This data, which includes visibility into more than 190 countries, 550 industries, and 50,000 autonomous system numbers (ASNs), is then analyzed and curated by NETSCOUT's ATLAS Security Engineering and Response Team (ASERT) to provide unique insights in the report. No other vendor sees and knows more about DDoS attack activity and best practices in protection than NETSCOUT.

Key findings from the 1H2022 NETSCOUT DDoS Threat Intelligence Report include:

- There were 6,019,888 global DDoS attacks in 1st half of 2022.
- TCP-based flood attacks (SYN, ACK, RST) remain the most used attack vector, with approximately 46% of all attacks continuing a trend that started in early 2021.
- DNS water-torture attacks accelerated into 2022 with a 46% increase primarily using UDP query floods, while carpet-bombing attacks experienced a big comeback toward the end of the second quarter; overall, DNS amplification attacks decreased by 31% from 2H2021 to 1H2022.
- The new TP240 PhoneHome reflection/amplifications DDoS vector was discovered in early 2022 with a record-breaking amplification ratio of 4,293,967,296:1; swift actions eradicated the abusable nature of this service.
- Malware botnet proliferation grew at an alarming rate, with 21,226 nodes tracked in the first quarter to 488,381 nodes in the second, resulting in more direct-path, application-layer attacks.

Geopolitical Unrest Spawns Increased DDoS Attacks

As Russian ground troops entered Ukraine in late February, there was a significant uptick in DDoS attacks targeting governmental departments, online media organizations, financial firms, hosting providers, and cryptocurrency-related firms, as **previously documented**. However, the ripple effect resulting from the war had a dramatic impact on DDoS attacks in other countries too, including:

- Ireland experienced a surge in attacks after providing service to Ukrainian organizations.
- India experienced a measurable increase in DDoS attacks following its abstention from the UN Security Council and General Assembly votes condemning Russia's actions in Ukraine.
- On the same day, Taiwan endured its single-highest number of DDoS attacks after making public statements supporting Ukraine, as with Belize.
- Finland experienced a 258% increase in DDoS attacks year-over-year, coinciding with its announcement to apply for NATO membership.
- Poland, Romania, Lithuania, and Norway were targeted by DDoS attacks linked to Killnet; a group of online attackers aligned with Russia.
- While the frequency and severity of DDoS attacks in North America remained relatively consistent, satellite telecommunications providers experienced an increase in high-impact DDoS attacks, especially after providing support for Ukraine's communications infrastructure.
- Russia experienced a nearly 3X increase in daily DDoS attacks since the conflict with Ukraine began and continued through the end of the reporting period.

Similarly, as tensions between Taiwan, China, and Hong Kong escalated in 1H2022, DDoS attacks against Taiwan regularly occurred in concert with related public events.

NETSCOUT's DDoS Threat Intelligence Report covers the latest trends and activities in the DDoS threat landscape. It covers data captured from NETSCOUT's ATLAS and expert insights from ASERT.

The visibility and insights compiled from the global DDOS attack data, represented in the DDoS Threat Intelligence Report, and seen in the **Omnis Threat Horizon** portal, fuel the ATLAS Intelligence Feed (AIF). In addition, AIF continuously arms NETSCOUT's Omnis and Arbor security portfolio enabling them to automatically detect 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 disruptions through advanced network detection and response and pervasive network visibility. Powered by our pioneering deep packet inspection at scale, we serve 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.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20220927005076/en/**

Editorial Contacts:

Maribel Lopez
Manager, Marketing & Corporate Communications
+1 781 362 4330
maribel.lopez@netscout.com

Chris Shattuck
Finn Partners for NETSCOUT
+1 678 504 6785

NETSCOUT-US@FinnPartners.com

Source: NETSCOUT SYSTEMS, INC.